Singapore Journal of Legal Studies
[2009] 290–300

BOOK REVIEWS

Global Privacy Protection: The First Generation BY JAMES B. RULE AND GRAHAM GREENLEAF, eds. [Cheltenham: Edward Elgar, 2008. vii + 318 pp. Hardcover: £75]

An eerie introspection into privacy came to me while I was reviewing the book, *Global Privacy Protection: The First Generation*, edited by Professors James B. Rule and Graham Greenleaf. Coincidentally, I had received a note from the Immigration and Checkpoints Authority, gently chiding and reminding my wife and me to register the birth of our baby girl with the authorities, under the penalty of criminal sanctions for failure to do so, pursuant to the *Registration of Births and Deaths Act* (Cap. 267, 1985 Rev. Ed. Sing.). Barely two weeks had elapsed since mother and child had been discharged from the hospital, but the omniscient authority has already been tracking the whereabouts and identity of this very recent addition to our family! Of course, as a law-abiding academic, the father dutifully complied, but he was left to contemplate if our baby could fend for herself in Singapore without a government-issued identity number.

This brought home to me in a most vivid fashion the pervasiveness of our national identification system and its use, both in the public and in the private sectors. Singapore citizens, residents and recently, even long term visitors, have come to accept the national and foreign identification numbers issued by the authorities. Even legal persons such as companies, societies and charities have been issued all-purpose identification numbers for government and other dealings to simplify corporate and administrative transactions. It may be opined that as a whole, Singapore society has largely accepted and adopted a remarkably tolerant and some may even say, *blasé* view towards privacy, preferring the convenience of a one-stop inter-agency service (such as the Immigration & Checkpoints Authority's One-Stop Change of Address Reporting Service (OSCARS) System) to concerns that their personal information is being shared. This view, which was noted as early as 1990 by a high-level government committee, did not appear to have changed substantially, even though there have been the occasional public indignations regarding incidents of personal information leakage. For instance, it has been reported in April 2009 that schools had inadvertently disclosed the personal data of staff and students from their mis-configured websites. And it is against this background that an inter-ministry committee set up by the Singapore government is conducting a review of data protection issues to develop a data protection model, which the (then) Minister for Information, Communications and the Arts, Dr. Lee Boon Yang, described in Parliament in January this year as one

that "can best address" the issues of privacy concerns, commercial requirements and national interest.

The same Minister had said in Parliament in February 2006 that a government committee would advance recommendations by mid-2006 regarding the protection of personal information in Singapore. In February 2007, the Minister acknowledged in Parliament that it was a "complex issue with extensive impact on businesses and [the] general public" and that the review was "still ongoing and will take some time." In January 2009, the Minister again repeated the statement in Parliament that "data protection is a complex issue with extensive impact on all stakeholders [and that the] review will take some time." All said, this review, which commenced in November 2004, has been ongoing for almost four and a half years. The Minister in his latest speech in Parliament gave no indication as to when this review would be concluded. Perhaps it is now timely that one should inquire into how this review is going.

Actually, the various contributing authors to *Global Privacy Protection* may have offered a socio-political explanation for this delay. As the editors note in the Introduction, they have sought to demonstrate that the adoption of privacy or data protection codes in various jurisdictions is often driven by a combination of social and political chemistry in that jurisdiction. We learn from the various esteemed contributors that privacy sensitivities had arisen and asserted themselves in the United States (arising from information abuses by the Nixon administration stemming from the Watergate scandal), Hungary (arising from the collapse of the Iron Curtain and the Duna-gate scandal) and South Korea (arising from the democratic movement, known as the June Struggle of 1987, that forced the then President Chun to allow a broad liberalisation of the nation and the resurrection of civic groups to serve as a counterweight to the past authoritarian regimes) for political reasons, or had taken the form of triggers of public indignation at government attempts at tracking their citizens in Germany (the proposed German federal census of 1983), France (the proposed French SAFARI system to turn social security numbers into exclusive individual identifiers for aggregation of all information about French residents) and Australia (the proposed Australia Card in 1987 with multiple government uses). It is only in Hong Kong that privacy legislation was shepherded into law by the political elite, in particular, from proposals by the Hong Kong Law Reform Commission. And even then, as Mr. Robin McLeish and Professor Graham Greenleaf, contributors for the Hong Kong chapter had noted, the reason for doing so was primarily commercial, stemming from concerns that the European Union's relatively strong *Data Protection Directive 1995* would forestall transfers of financial data to Hong Kong for data processing purposes. Thus far, none of these operative factors highlighted by the authors have presaged Singapore's data protection review. To borrow the words of Professor Greenleaf, the contributor for the Australia chapter, one would have arguably described Singapore's legal, sociological and political climate as stable but staid, such that it would actually impede the development of public privacy concerns in society.

How should any country bereft of these political and sociological triggers develop a legal framework for the protection of privacy? *Global Privacy Protection* offers some tantalising insights but no clear answers. It is clear from all the chapters that political leadership in this area is very critical, but as Professor Rule observed in the concluding chapter, "all politics is local". In the seven jurisdictions reviewed here, political will has merged with a sharpened social consciousness idiosyncratic to each

jurisdiction to found the requisite privacy legislation. But what about the impact of international instruments? The first chapter by Professor Bygrave opines that the *EU Data Protection Directive*, generally accepted as having set the highest benchmarks for data protection, and its innovative Article 25(1) that proscribes the flow of personal data to states not offering an adequate level of data protection, has the most substantial impact in shaping data protection laws in third countries. Nonetheless, it is depressing to read an affirmation of the corollary that other international instruments such as the non-binding OECD Principles (and even more attenuated APEC Privacy Framework) are unlikely to serve as substantive impetus for privacy protection, as the former, which supports self-regulation, is not legally binding and the latter has substantially diluted the core principles of the OECD Principles.

Here, one can make three additional observations regarding *Global Privacy Protection* from a uniquely Singapore perspective in the area of privacy and data protection. The first is that the editors and contributors have selected and sought to focus on the status of privacy protection in countries where there are privacy laws and codes, as distinct from privacy standards for the industry—for which Singapore was indeed singled out for mention in the book, in the concluding chapter. Privacy standards for the industry were indeed referred to in the U.S. chapter of the book, but there is in no assessment by any contributor regarding its efficacy (or lack thereof) in comparison to laws and codes. There is again a missed opportunity to examine this issue when describing the safe harbour scheme to permit U.S. organisations, particularly those technology companies which are the most aggressive collectors and users of personal information, to qualify as offering adequate protection for personal data flowing from the E.U./E.E.A. Likewise, this invitation was not taken up in the concluding chapter. Industry-driven codes are exceptionally relevant, particularly in the light of the near unanimous conclusion from all contributors that Internet technologies and the commoditisation of Internet users' usage patterns, coupled with an apparent de-sensitisation of privacy concerns among the technologically-savvy younger generation, could lead to a "life-long acquiescence" to privacy-unfriendly practices.

The other observation concerns a lack of an operational definition of "privacy" and "data protection" in the book, terms of which were sometimes used interchangeably in the contributions. Data protection can be seen as an aspect of "informational privacy", but as defined, "information privacy" overlaps with issues such as surveillance, interrogation, identification, exposure, intrusion and interference. Many of the principles discussed in the chapters, such as the formative OECD Principles, pertain to "information privacy" rather than to privacy generally. This has made the discussions in the various chapters regarding the intersection between data protection and the needs of law enforcement and terrorism prevention anachronistic. The discussions about the *U.S. Patriot Act* in the U.S. chapter, the *Interior Security Act* in the French chapter and the legislative changes to legislation to permit warrantless telecommunications interceptions and surveillance in the Australian chapter highlight the severe erosion to privacy in the pursuit of anti-terrorism counter-measures. The only possible exception is the German chapter, with its reference to the German Federal Constitutional Supreme Court's formulation of the principle of "individual self-determination" as an embedded constitutional right and its subsequent application to filter out some forms of police and secret service activities such as screening,

collecting or tapping personal data. Interestingly, in the seminal privacy paper by Warren and Brandeis (published in 1890 in the Harvard Law Review), privacy protection was founded on the idea of an inviolate personality which has Germanic roots. Yet privacy (and data protection) developments have taken diametrically opposed approaches in the U.S. and in Germany.

The final observation takes up a theme identified in the concluding chapter. It notes that the chapters on data protection in the various jurisdictions have seen data protection laws being aligned to a "clearly discernible global consensus" as to "privacy-friendly fair information practices". But its esteemed contributor, Professor Rule, was quick to point out that those widely differing interpretations given to the data protection principles have led to a vast variation in the application of even the key principle—the consensus principle. He noted that the consensus principle has been widely interpreted not to apply to the state's coercive or investigative institutions, fails to resolve the issue of the scope of personal data that institutions can legally appropriate, and does not delimit the circumstances in which a person's consent to his use of information becomes so overbearing as to deprive the term of all meaning, such as through the use of dense and consumer-incomprehensible privacy statements. Likewise, the broad interpretation of the consensus principle has yielded a wide spectrum of "remedies" for aggrieved users, ranging from filing suit to assisted mediation by privacy commissions to fiscal penalties for privacy breaches, but not every such remedy is effective.

These conclusions are undoubtedly correct, and borne out by the observations from the various contributors in the respective chapters. Yet one cannot but feel dissatisfied by the absence of a normative approach towards an understanding of these data protection principles, including the consensus principle. For instance, as some academic authors such as Katrin Schatz Byford, Pamela Samuelson and Daniel J. Solove have observed, founding data protection on one's inviolate personality rights as opposed to characterising it as purely proprietary in nature would have limited the scope and manner in which "consent" could be granted or extracted from the individual. But this would certainly be beyond the avowed scope of the book.

Before ending this review, perhaps some editorial observations about the book are in order. Like all instances, it is often easier to spot errors when texts are in print than when they are in production. For instance, the chapter on Australia is entitled "Privacy in Australia" whereas the other jurisdiction-specific chapters are just designated by the names of the jurisdictions (*e.g.*, "United States", "Hong Kong"). The last chapter does not have a chapter number but the first chapter, which is a review on international agreements, is numbered as Chapter 1 in the table of contents but unnumbered in the text. The first chapter is tagged with footnotes but the other chapters are generally bereft of such footnotes. And while the bibliography table is extensive, it is often very difficult to correlate a case or statute identified in the contribution to its entry in the bibliography more than one hundred pages away at the end of the book. Here, the use of the more precise legal citation style guide for legal texts would have been preferable to a social science citation style guide.

Finally, the closing chapter in the book reaches the conclusion that data protection principles are ultimately based on public support. Unfortunately, this conclusion ostensibly undermines the very basis of the data protection principles that underlie the data protection laws reviewed in the various jurisdictions. It also reinforces my

view that a normative approach would better elucidate and explicate data protection laws worldwide. But if the search for a normative basis forms the basis for the next generation of data protection laws, this must entail educating the public, conducting an informed survey of the laws in the various jurisdictions and engendering a better understanding of the application and limitations of the data protection principles. In this regard, the publication of *Global Privacy Protection: The First Generation* is certainly to be commended.

DANIEL **SENG**
National University of Singapore