Singapore Journal of Legal Studies
[2021] 1–5

PRIVACY, CONFIDENCE & DATA PROTECTION IN THE 21ST CENTURY

DAVID **TAN***

On 5 and 6 December 2019, the Faculty of Law at the National University of Singapore ("NUS Law") hosted about 100 participants at the 8th Asian Privacy Scholars Network ("APSN") Conference at its Bukit Timah Campus, convened by Professor David Tan. The conference was jointly presented by the EW Barker Centre for Law & Business and the Centre for Technology, Robotics, Artificial Intelligence & the Law ("TRAIL")—both research centres at NUS Law. TRAIL was also launched by Mr Edwin Tong, Senior Minister of State for Law and Health, on the first day of the conference.

The theme "Privacy, Confidence & Data Protection in the 21st Century" attracted 40 papers presented by scholars and practitioners from 17 jurisdictions. The kaleidoscope of papers covered a broad range of topics that included an interrogation of conceptual frameworks, practical analyses of personal data protection legislation such as the EU ("European Union") General Data Protection Regulation ("*GDPR*") and other national regulatory regimes, health data management, privacy issues at the Tokyo Olympics, privacy and the Hong Kong protests, and the surveillance economy. Professor Megan Richardson from Melbourne Law School, who delivered the first keynote address on Day One, advanced an account of five disruptive moments in the development of the common law, and the inherent disunity in the judicial conceptions of privacy over the decades. Mr Yeong Zee Kin, who delivered the second keynote address on Day Two, is the Assistant Chief Executive (Data Innovation and Protection Group) of the Infocomm Media Development Authority of Singapore ("IMDA") and Deputy Commissioner of the Personal Data Protection Commission ("PDPC"). He shared how the "regulatory sandbox" had assisted the government in its policy formulations, and mooted the Model AI Governance Framework and the Trusted Data Sharing Framework.

* Professor and Vice Dean (Academic Affairs), Faculty of Law, National University of Singapore; Head (Intellectual Property), EW Barker Centre for Law & Business; Deputy Director, Centre for Technology, Robotics, Artificial Intelligence & the Law; Convenor, 8th Asian Privacy Scholars Network Conference.

At a more philosophical level, scholars like Antoinette Rouvroy and Yves Poullet have theorised that: "Privacy and data protection regimes should thus be understood as 'mere' tools (evolving when required by the new threats that socio-economic, cultural and technological changes impose on individual and democratic self-determination), meant to pursue that one single common goal: sustaining the uniquely human capacity for individual reflexive self-determination and for collective deliberative decision making regarding the rules of social cooperation."[1] More than two decades ago, Lillian BeVier has exasperatingly disparaged privacy as "a chameleon-like word, used denotatively to designate a wide range of wildly disparate interests—from confidentiality of personal information to reproductive autonomy—and connotatively to generate goodwill on behalf of whatever interest is being asserted in its name."[2] A decade later, Daniel Solove argued that it would be a futile endeavour to attempt to define privacy as a unitary concept with a uniform value, and instead proposed a taxonomy "to identify and understand the different kinds of socially recognised privacy violations, one that hopefully will enable courts and policymakers to better balance privacy against countervailing interests."[3] Jon Mills also commented on that it was an "amorphous, global right" and that the "status of our collective privacy is unpredictable, inconsistent, and changing continually—a reflection of a society with changing mores and changing technology."[4]

The theoretical justifications for the protection of personal privacy overlap with those for the protection of personal data, and the protection of these interests are further intertwined with the law of confidence in equity. The Singapore Court of Appeal has noted in *ANB v ANC*[5] that "the protection of privacy under the law of confidence in England in fact materialised *before* the enactment of the HRA[6] pursuant to a *common law right to privacy*" and that in Singapore, "on a policy level, legislative developments in recent years, which included the enactment of the *Protection from Harassment Act*... and the *Personal Data Protection Act 2012*..., also point towards an increasing recognition of the need to protect personal privacy."[7]

As Juliane Kokott and Christoph Sobotta observed, the right to privacy and the right to data protection are distinct rights, and while there are some areas of overlap, there are also "areas where their personal and substantive scope diverge";[8] in particular, they cautioned that although "privacy and the protection of personal data are closely linked in the jurisprudence of the European Court of Human Rights and

---

1 Antoinette Rouvroy & Yves Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy" in Serge Gutwirth *et al*, eds, *Reinventing Data Protection?* (Amsterdam: Springer, 2009) at 76.

2 Lillian R BeVier, "Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection," (1995) 4:2 Wm & Mary Bill Rts J 455 at 458.

3 Daniel J Solove, "A Taxonomy of Privacy" (2006) 154:3 U Pa L Rev 477, at 483, 484. See also Daniel J Solove, *Understanding Privacy* (Cambridge: Harvard University Press, 2008); Daniel J Solove & Paul M Schwartz, *Information Privacy Law*, 6th ed (New York, Wolters Kluwer, 2018).

4 Jon L Mills, *Privacy: The Lost Right*, (New York: Oxford University Press, 2008) at 305.

5 [2015] SGCA 43.

6 *Human Rights Act* (UK), 1998, c 42.

7 *Supra* note 5 at para 22.

8 Juliane Kokott & Christoph Sobotta, "The Distinction Between Privacy and Data Protection In the Jurisprudence of the CJEU and the ECtHR" (2013) 3:4 Intl Data Privacy L 222 at 228.

the Court of Justice of the European Union, but they should not be considered to be identical."[9] Simon Chesterman noted that despite the significant barriers to the general acceptance of a right of privacy, there is considerably more convergence towards a unified approach to data protection.[10] While the digital revolution has transformed our conceptions of privacy, information collection and data sharing, reform of laws may not necessarily be driven by "the desire to defend the rights of data subjects" but is instead premised on "economic considerations", and in the case of Singapore, "the desire to position Singapore as a leader in the region for data storage and processing."[11]

Regarding the privacy-based approach to personal data protection, Benjamin Wong commented: "The premise of the privacy-based approach is the view that data protection rights are parasitic on the right to privacy. In a nutshell, the privacy-based approach assumes that the purpose of data protection law is to protect individual privacy, and that the concept of personal data should be interpreted in accordance with this purpose."[12] However, Wong concluded that "it is quite evident that the new data protection regime under the *GDPR* is not parasitic on the right to privacy" and the "freestanding right to data protection is therefore the sole basis on which the *GDPR* (and the *Data Protection Act 2018*) protect individuals with regard to the processing of personal data."[13]

Indeed, different data protection regimes around the world all impose a panoply of obligations in respect of the collection, management, processing and dissemination of personal data, and they provide a morass of civil remedies and criminal sanctions. Their designs all rest on a pastiche of rights to privacy and to data protection, as well as other extra-legal commercial and political considerations. Many questions are still unanswered. For instance, in the United States, a number of Supreme Court decisions have resulted in confusion about how harms involving personal data should be conceptualised.[14] Daniel Solove and Danielle Citron noted: "To many judges and policymakers, recognizing data-breach harms is akin to attempting to tap dance on quicksand, with the safest approach being to retreat to the safety of the most traditional notions of harm. Unfortunately, public conversation about data-breach harms rarely delves into the muddy conceptual waters. With some noted exceptions, scholarship has not given the issue sufficient attention."[15] Indeed there is much work to be done in this area.

---

9 *Ibid*. See also Orla Lynskey, "Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order" (2014) 63:3 Intl & Comp L Rev 569 at 581 ("despite the jurisprudence of the CJEU, data protection and privacy are distinct, albeit heavily overlapping, rights and that there is adequate justification to treat them as such").

10 Simon Chesterman, "From Privacy to Data Protection" in Simon Chesterman, eds, *Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World*, 2d ed (Singapore: Academy Publishing, 2018) at para 2.28.

11 *Ibid* at para 2.108.

12 Benjamin Wong, "Delimiting the concept of personal data after the *GDPR*" (2019) 39:3 Leg Studies 517 at 519, 520.

13 *Ibid* at 525.

14 See *eg*, *Clapper v Amnesty International* 568 US 398 (2013); *Spokeo, Inc. v Robins* 578 US 330 (2016).

15 Daniel J Solove & Danielle Keats Citron, "Risk and Anxiety: A Theory of Data-Breach Harms" (2018) 96:4 Tex L Rev 737 at 744.

Last but not least, the equitable action for breach of confidence has been struggling to keep pace with digital and technological developments. But in 2020, the Singapore Court of Appeal refined the law in this area and departed from English precedent, pointing to the increasing vulnerability of the wrongful loss interest "against the backdrop of advances in modern technology" that facilitate the accessing, copying and dissemination of confidential information.[16] By removing the requirement for unauthorised use under the third element of the classical test established in *Coco v AN Clark (Engineers) Ltd*[17], the Court had thus opened the doors to claims of breach of confidence in respect of the *access and acquisition* of confidential information which includes data.[18] It is a pity that we could not include a paper on the developments of the equitable breach of confidence action in this issue, but I have no doubt that the academic debate will rage on following this decision.

This special APSN Conference issue curates a selection of refereed papers that advances the academic discussion in these complex and interrelated fields of privacy, confidence and data protection.

In "A Common Law of Privacy?" by Professor Megan Richardson, she highlights in her keynote address that for some time we seem to have been living in a world of legal disunity, rather ironically following the assertion of the right to privacy as a universal human right in the post-War Universal Declaration of Human Rights and International Covenant on Civil and Political Rights. She contends that "the history of privacy law is not just a history of incremental progression along different paths. The paths may often divide but they may also merge together from time to time setting the scene for some (somewhat) more common approaches." Richardson postulates five moments of disruption, that have changed the course of history across the common law world, and have produced albeit, within a limited compass, some common new or renewed privacy traditions. In her conclusion, referring to a number of cases in the United Kingdom ("UK") and European Union, she suggests that "[t]aken together they serve as yet another sign of the possibilities of convergence around legal standards of privacy protection in the future, as in the past and present—for all the legal, social-cultural and political differences that remain and for all the new challenges to privacy that we can expect to see in a post-pandemic world."

In "Enforcement Design for Data Privacy: A Comparative Study", Associate Professor Gehan Gunasekara explores whether the design of enforcement mechanisms in data privacy laws influences the types of privacy harms addressed by them through evaluating evidence of enforcement from four jurisdictions. It employs three of the seven foundational design principles first identified by Ann Cavoukian to examine if each category of data privacy (*eg* data quality, access rights, use, disclosure, security) should be addressed through enforcement tools suited to their characteristics. Gunasekara then evaluates the data privacy regulatory frameworks of four jurisdictions over a six-year period from 2013 until 2018—Australia, New Zealand, Hong Kong and the UK—from the standpoint of how they enforce data privacy rights. He concludes, *inter alia,* that there is a close parallel between regulators being proactive and transparency, and that providing individuals with rights to litigate their

---

16 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] SGCA 32 at para 55.

17 [1969] RPC 41 (HC).

18 Benjamin Wong & David Tan, "A Modern Approach to Breach of Confidence based on an Obligation of Confidence" [2020] 136 Law Q Rev 548 at 551.

data privacy rights tended to be ineffective except where specialist adjudicative fora existed.

In "The Charter of Fundamental Rights, the Aims of EU Competition Law and Data Protection: Time to Level the Playing Field", Divin De Buffalo Irakiza points out that the commodification of personal data has brought data protection issues within the remit of EU competition law and therefore blurring the demarcation between those policy areas. He argues that this has raised questions on the extent to which competition law should be used to safeguard the right to data protection in online markets and contends that data protection should be among the objectives of EU competition law. Drawing on the jurisprudence of the Court of Justice of the European Union on the European Charter of Fundamental Rights (the Charter), he concludes that there is a duty imposed on the EU by the legally binding Charter, to respect and promote fundamental rights, of which data protection is one, by virtue of Article 8 of the Charter.

In "Three Shades of Data: Australia, Philippines, Thailand", Robert Brian Smith, Mark Perry and Nucharee Nuchkoom Smith undertake a comparative analysis of the privacy legislation of Australia, the Philippines and Thailand and through their *Privacy Act 1988*, *Data Privacy Act of 2012*, and *Personal Data Protection Act* 2019 respectively. Their work focuses on the different types of data protected by privacy provisions, methods for investigating breaches and imposing penalties, and whether breaches result in administrative action, civil liability or criminal offences. The findings will no doubt be useful to any policymaker or data privacy scholar seeking to have a quick understanding of how different jurisdictions in the Asia-Pacific region approach the collection, access and use of personal data and information.

Electronic health records are no longer a simple and convenient storage of patient data. Governments, healthcare providers and researchers around the world are clamouring for more data to help them understand and solve the numerous intractable problems in healthcare. In "Whose Health Record? A Comparison of Patient Rights under National Electronic Health Record Regulations in Europe and Asia-Pacific Jurisdictions", James Scheibner, Marcello Ienca and Effy Vayena compare the implementation strategies of National Electronic Health Record ("NEHR") regulations in nine jurisdictions from Europe and the Asia-Pacific, to determine whether there is an international convergence of norms concerning the rights of patients. They argue that NEHR implementations should be neither considered patient property nor a means of outsourcing liability to patients, but instead, NEHRs should be conceived as a public good.

Whether you are an academic scholar, practitioner, policymaker or even a law student, I hope these papers will be of interest and relevance to you.