EDITORIAL

Some Problems of 'Consent' Under Australian Data Privacy Law

This special issue of the Global Privacy Law Review (GPLR) focusses on the role of consent under Australian data privacy law. By addressing a policy issue that is central to the future of data privacy law within the context of a national law with some distinctive features, it offers more general insights into the nature of data privacy regulation and how it might best respond to current and emerging challenges. The authors – Kayleen Manwaring, Katherine Kemp and Rob Nicholls – have together compiled a rich analysis of how consent is treated under Australian data privacy law, which represents the most comprehensive treatment undertaken of this issue under Australian law.

Australian privacy law has followed its own path. While Australia is a signatory to the International Covenant on Civil and Political Rights (ICCPR), it does not have a bill of rights and its legal system fails to recognize a right to privacy. And yet, in the form of the Privacy Act 1988 (Privacy Act), Australia has an omnibus data privacy law that applies general privacy principles to the federal public sector and the private sector, and a federal data privacy regulator, in the form of the Office of the Australian Information Commissioner (OAIC).

As the Privacy Act does not embody a rights-based approach, it is best regarded as a series of pragmatic compromises between the interests of data collectors and processors, on the one hand, and those of data subjects, on the other. An overriding, if incompletely acknowledged, objective has been to deliver a degree of privacy protection while not imposing undue regulatory costs on business. Consequently, there are carve outs from the law – including exceptions for small businesses, employee records and political parties – and the privacy principles, known as the Australian Privacy Principles (APPs), are subject to many complex exceptions.

Australian data privacy law is weak when compared with the law in other jurisdictions. This is evidenced by the ongoing failure of the Australian regime to be deemed 'adequate' by the European Commission. The weaknesses of the substantive law have been exacerbated by a lack of resourcing for the OAIC, which has led to a relatively poor record of enforcement. All of this has meant that the Australian law has been ill-equipped to deal with rapidly evolving data practices, including those of the digital platforms, especially Meta (formerly Facebook) and Google.

The mismatch between the Australian law and contemporary data practices came to a head with an inquiry by the Australian Competition and Consumer Commission (ACCC), Australia's competition and consumer protection regulator, into the practices of digital platforms. The inquiry, known as the Digital Platforms Inquiry (DPI), was established mainly to consider the impact of digital platforms on competition in media and advertising markets, but found that it was impossible to proceed without examining the adequacy (or otherwise) of the Privacy Act in protecting consumer data. The DPI report, released in 2019, made specific recommendations for strengthening the Privacy Act, as well as identifying a range of broader reforms proposed to be subject to further review. The Australian government responded to the ACCC's recommendations by establishing a fundamental review of the Privacy Act to be conducted by the federal Attorney-General's department. In October 2021, the Attorney-General's department released an extensive Discussion Paper (DP), which included significant reform proposals, many of which would more closely align Australian law with the EU's General Data Protection Regulation (GDPR). The fate of the reform process, however, remains uncertain – not merely due to an intervening federal election, but because law reform in this area has been characterized by a lack of political will to take on difficult issues, especially in the face of opposition from business interests.

One issue identified in both the DPI report and the Attorney-General's DP is the adequacy of the consent regime under the Privacy Act. The Privacy Act, like other data privacy regimes, is based on the principle of 'privacy self-management': that individuals should be free to consent to the collection, use and disclosure of personal information. As this special issue explains, however, in line with the generally business-friendly approach underpinning the Australian regime, the Privacy Act defines 'consent' very broadly to include 'implied consent'. This leaves it open for business to argue that, in certain circumstances, a failure to object can amount to consent. The Attorney-General's DP proposed to bring Australian law more into line with the GDPR by requiring consent to be 'voluntary, informed, current, specific and an unambiguous indication through clear action'. The DP also canvassed options for improving informed consent by

requiring standardized consents, such as by means of icons or consent taxonomies.

These proposals raise a regulatory paradox that lies at the heart of the dilemmas facing contemporary data privacy law: 'privacy self-management' is intended to promote the autonomy of data subjects but, as it applies in practice, it often has the effect of undermining autonomy and informational self-determination. As this special issue explains, in the context of contemporary data practices, 'informed consent' is often practically meaningless due to factors such as information asymmetries, cognitive biases and consent fatigue. The 'privacy self-management' paradigm can therefore effectively shift the compliance burden from business to data subjects, who are already over-laden. Moreover, in many cases, consent to data practices is non-negotiable, as it is necessary to gain access to a desired or essential service. This means that it has become generally accepted that, as the 2019 report of the UK Human Rights Committee (HRC) cited in this issue put it, the 'consent model is broken'. In other words, in practice, and in the context of contemporary data practices, the 'notice-and-consent' model simply boils down to an obligation to give notice, with consent being no more than a formality. Merely increasing the threshold for consent, as proposed in the Attorney-General's DP, cannot alone resolve this dilemma.

If we accept that 'privacy self-management' is broken, the question underlying much of the discussion in this special issue is, 'what can replace it'? The UK HRC report echoed a common response to the problem by proposing higher levels of protection by default. The articles in this special issue suggest, correctly in my view, that the response to the challenges posed by contemporary data practices should consist of a two-stage strategy: some immediate 'quick wins' but with further systemic, longer-term reforms. This approach acknowledges the extent to which data privacy regulation is in a state of transition, such that short-term reforms can focus on strengthening the existing framework, while accepting that attention is needed for the difficult task of shifting the paradigm.

As this issue suggests, two important elements of a new regulatory paradigm must be, first, a greater focus on regulating technology design and, secondly, better alignment of laws, regulators, and enforcement bodies. On this last point, one underlying theme that emerges from this issue is the relationship between data privacy and consumer laws, which appear to be increasingly converging, both in principle and in practice. Moreover, as the authors point out, in Australia, privacy law reform has not only been led by the ACCC, a consumer protection agency, but consumer law has often been more effective than the Privacy Act in protecting consumer privacy. There is still much work to be done in exploring the relationship between data privacy and consumer protection law; but my view is that there is a need for general principles that apply to all consumer data, and which should go beyond the existing data privacy principles. An embryonic form of this approach may potentially be found in the privacy safeguards which apply under the Consumer Data Right (CDR) regime, which is introduced in this issue, and which are not confined to 'personal information' (or 'personal data'). Meanwhile, the material assembled in this special issue provides an invaluable resource for anyone with an interest in Australian data privacy law, as well as making an important contribution to debates about the future direction of data privacy and its regulation.

Prof. David Lindsay
University of Technology Sydney