EDITORIAL

Editorial Note

Ceyhun Necati Pehlivan*

This issue of the *Global Privacy Law Review* brings together four contributions that, although diverse in subject matter and methodology, converge on a common theme: privacy as part of the basic architecture of legal order. From the historical roots of privacy in Roman law and early modern Europe, through contemporary debates on drone surveillance, to the interplay between competition, data protection and compliance in digital mergers, and the evolving role of pseudonymization and national data protection frameworks, the pieces collected here invite reflection on how law shapes and constrains power over information in a networked world.

The opening article by Camilla Della Giustina and Pierdomenico de Gioia Carabellese, *The Tort (or Scottish Delict) of Privacy from Thomas More's* Utopia *to the 'Tate Gallery' Case via Air Drones*, offers a wide-ranging historical and comparative analysis of privacy in common law systems, with a particular focus on English and Scottish law.[1] Starting from *Utopia* and drawing on Roman law remedies such as the *actio iniuriarum*, the authors show that privacy is not a late-modern by-product of the digital age, but a construct deeply embedded in social practice, architecture and hierarchy. They trace how early Anglo-American doctrine, including Warren and Brandeis's classic formulation and the development of the New York statutory right of privacy, emerged in response to technological change, first the camera and later, as the article emphasizes, drones.

A particular strength of the piece is its insistence on the spatial and physical dimensions of privacy, which have often been overshadowed by information-centred accounts. The authors carefully reconstruct the evolution of English law from *Wainwright* and *Campbell* through *Vidal-Hall v. Google* and *Tchenguiz v. Imerman*, showing how misuse of private information and data protection have functioned as de facto vehicles for privacy protection, even as courts have resisted recognizing a freestanding tort of privacy. The Scottish strand of the analysis, built around the *actio iniuriarum* and cases such as *Martin v. McGuinness* and *C v. Chief Constable of the Police Service of Scotland*, illustrates a distinct legal culture in which dignity and personality interests are central, yet privacy is mediated through broader concepts of unlawful assault on personality. Set against the practical problems posed by drone surveillance, this doctrinal history supports a compelling claim that privacy must be understood both as individual autonomy and as a social practice shaped by expectations of space, visibility and restraint.

The second article, by Kolawole Afuwape, turns from the aerial vantage point of drones to the 'invisible infrastructures' of data integration in digital mergers: *Legal Complexities of Post-Merger Data Integration: Privacy, Antitrust, and Compliance Perspectives in the Tech Sector.*[2] This doctrinal and comparative study starts from a clear premise: in contemporary technology mergers and acquisitions, the core asset is not plant or even code, but data. The article examines how post-merger data integration sits at the junction of competition law, privacy and data protection, and regulatory compliance, and argues that current merger review tools were designed for markets where price and output were primary, rather than for data-driven ecosystems where quality, privacy and control over information are key dimensions of competition.

Through detailed discussion of landmark cases and transactions such as *Facebook/WhatsApp, Google/Fitbit* and *Microsoft/LinkedIn*, and with careful attention to developments under the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and Privacy Rights Act (CPRA), Brazil's *Lei Geral de Proteção de Dados Pessoais* (LGPD), India's DPDP Act, and China's Personal Information Protection Law (PIPL), Afuwape maps the growing convergence and friction between competition authorities and data protection

Notes

* Editor-in-Chief. Email: cpehlivan@faculty.ie.edu.

1 Camilla Della Giustina & Pierdomenico de Gioia Carabellese, *The Tort (or Scottish Delict) of Privacy from Thomas More's Utopia to the 'Tate Gallery' Case via Air Drones* (2026), in this issue at 5.

2 Kolawole Afuwape, *Legal Complexities of Post-Merger Data Integration: Privacy, Antitrust* (2026)*, and Compliance Perspectives in the Tech Sector*, in this issue at 18.

regulators. The article covers both ex ante gatekeeper regulation, notably the European Union's Digital Markets Act, and ex post merger control and conduct remedies that increasingly incorporate privacy-related conditions. A central insight is that post-merger compliance is no longer a purely 'back-end' exercise: the feasibility of integrating datasets in a lawful, ethically robust and technically manageable way now directly affects deal valuation, structure and strategy. In this sense, the paper anticipates a future in which privacy is not only a fundamental right but also a recognized parameter of competition and a constraint on how market power can be built and exercised.

The country report by Ahmed El Sharkawy and Omar Sherif, *Egypt's Personal Data Protection Law: Implementation Challenges and Additional Compliance Requirements*, documents a significant development in the global landscape of privacy and data protection: the entry into force of Egypt's 2020 Personal Data Protection Law through the recent issuance of its executive regulations.[3] Drawing on practitioner insight, the report sets out the key obligations now imposed on organizations, including a mandatory registration and licensing regime for controllers and processors, strict notification duties in the event of personal data breaches, consent-based rules for cross-border transfers and sensitive-data processing, and an extraterritorial provision whose scope remains uncertain. It situates Egypt's framework within wider regional and international trends, reflecting both a desire to align with global standards and a concern with digital sovereignty and control over data flows.

A notable feature of the Egyptian regime, as the report emphasizes, is its departure from the GDPR's model in several respects. Egypt's Personal Data Protection Law combines administrative powers with criminal penalties, requires notification of every personal data breach irrespective of impact, and conditions many forms of processing and cross-border transfer on prior licensing and formal approvals. These design choices create distinctive compliance burdens for organizations operating in or from Egypt and illustrate how states can adopt broadly GDPR-inspired structures while diverging in their approach to enforcement, risk allocation and the supervision of data-driven economic activity.

Completing the issue, the case note by Julie Mannekens, *Case C-413/23 P, European Data Protection Supervisor (EDPS) v. Single Resolution Board (SRB): Reassessing the Role of Pseudonymization in Data Sharing?*, focuses on a more specific but equally significant issue: the notion of personal data in the context of pseudonymized datasets and data sharing.[4] Analysing the judgment of the Court of Justice of the European Union (CJEU) in *EDPS v. SRB*, the note explains how the Court confirms a 'relative' approach to the definition of personal data. Whether pseudonymized information amounts to personal data does not depend on an abstract characterization of the dataset, but on the position of the party in question and the means reasonably likely to be used to (re)identify individuals

Mannekens carefully unpacks the distinction between the position of the transferor, who retains the key enabling re-identification and thus remains subject to full GDPR obligations, and that of a recipient who has neither access to that key nor realistic means of identification. The note proposes a practical framework for those designing compliant data-sharing arrangements: defining 'pseudonymization domains', combining technical measures with contractual and legal safeguards, and limiting the circle of recipients. It also looks ahead to the evolving regulatory context, including the European Commission's Digital Omnibus proposal and forthcoming guidance from the European Data Protection Board on pseudonymization. In doing so, it raises important questions about the potential, and the limits, of pseudonymization as a tool for enabling data use while remaining within, or outside, the GDPR's scope.

Taken together, these four contributions illustrate several overarching themes.

First, they underline the multidimensional nature of privacy. The historical and doctrinal account in the opening article reminds us that privacy is not only about information control but also about physical space, social ritual and dignity. The merger-focused analysis presents privacy as a parameter of competition and an economic quality of digital services. The Egyptian country report demonstrates how privacy functions as a regulatory framework for digital transformation, cross-border commerce and state oversight of data infrastructures. The case note shows how privacy law turns on fine-grained assessments of identifiability and risk.

Secondly, they highlight privacy's social and institutional character. Across common law tort, Scottish delict, EU data protection law and national implementation, privacy is mediated through institutions: courts balancing Articles 8 and 10 of the ECHR; competition and data protection authorities coordinating (or failing to coordinate) over digital mergers; the CJEU defining the reach of the GDPR; and national regulators establishing registration, licensing and oversight systems. The contributions collectively suggest that the protection of privacy depends as much on institutional design, regulatory cooperation and enforcement practice as on the formulation of rights and principles in the abstract.

Thirdly, they confirm that technological change remains a driver of legal development. Drones, messaging

Notes

[3] Ahmed El Sharkawy & Omar Sherif, *Egypt's Personal Data Protection Law: Implementation Challenges and Additional Compliance Requirements* (2026), in this issue at 33.

[4] Julie Mannekens, *Case C-413/23 P, EDPS v. SRB: Reassessing the Role of Pseudonymization in Data Sharing?* (2026), in this issue at 36.

platforms, artificial-intelligence-driven advertising and pseudonymization techniques all operate as stress tests for existing concepts of private life, harm, personality rights and lawful processing. The responses described in this issue are varied: doctrinal adaptations of breach of confidence into misuse of private information; new merger guidelines and gatekeeper regimes; more nuanced interpretations of 'personal data'; and the creation and implementation of comprehensive national frameworks. A common thread is the effort to preserve a meaningful sphere of autonomy and dignity in environments where observation, data collection and profiling are increasingly pervasive and opaque.

Finally, this issue invites reflection on the future direction of global privacy law. The interaction between privacy and competition, the relative concept of personal data, and the spread of comprehensive data protection laws all suggest that privacy will increasingly be shaped in a trans-systemic way. Decisions in Luxembourg, regulatory strategies in Brussels, London, Washington, Beijing or Cairo, and doctrinal developments in Edinburgh or Toronto all feed into an evolving global conversation. That conversation must address not only individual harms, but also the structural implications of concentrated control over data, the risk of 'compliance squeeze' between regimes, and the need to sustain trust in digital infrastructures.

I hope that the contributions in this issue will assist scholars, practitioners, regulators, and policymakers in navigating these challenges, by offering both historical depth and analytical clarity on the multiple roles that privacy plays in contemporary law.