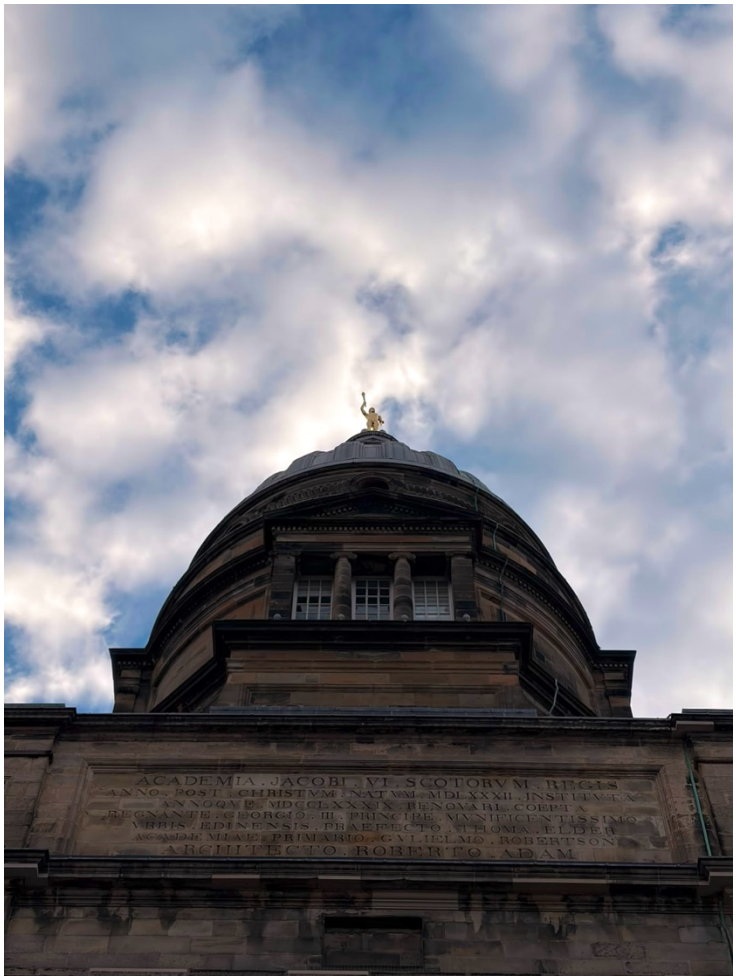
scripted

A Journal of Law, Technology & Society



Issue 23:1

(June 2026)

scripted

Volume 23, Issue 1, June 2026

Editorial Introduction

Rania Djojosugito and Aubrey Wasden***

DOI: 10.2218/scrip.12313

* Editor-in-Chief, SCRIPTed; PhD Candidate, the University of Edinburgh, r.a.djojosugito@sms.ed.ac.uk.
** Managing Editor, SCRIPTed; PhD Candidate, the University of Edinburgh, a.m.wasden@sms.ed.ac.uk.

"Hello World!": A warm welcome back

Long time readers may notice a shift, a proverbial change in the SCRIPTed atmosphere, while new readers may be enticed and curious about what is to come and what is to be expected. We are thrilled to welcome you all to our latest issue of the SCRIPTed journal, introducing a selection of articles, case comments and book reviews that tackle contemporary challenges of law, technology, and society. We are also pleased to share some of the latest developments in the operation of the journal.

New Home and New Faces

SCRIPTed has undergone changes this year, marked by the departure of its outstanding previous Editor-in-Chief, Mihail Dishev, whose baton has been passed to its new Editor-in-Chief, Rania Djojosugito. We would like to extend a heartfelt thank you for Mihail's tireless work and dedication to SCRIPTed. We also express thanks to our Technical Editor, Yiwei Lu, who has recently successfully completed his PhD studies and is moving on to pastures new.

As mentioned in last year's editorial introduction, SCRIPTed has also moved to a new online home. Our new website welcomes you with new centralised means to submit and review pieces thanks to the University of Edinburgh and Edinburgh Diamond. Particular thanks are due to Rebecca Wojturska of Edinburgh Diamond for her support in this transition. We encourage you to take a look at our new website and consider contributing your work here: https://journals.ed.ac.uk/script-ed/index. The Journal has also sustained its online presence via LinkedIn and BlueSky. At this time of transition, making connections to academics and scholars through social media has been an important opportunity and resource to ensure accessibility, opportunity, and

awareness. We appreciate your support and do consider keeping in touch with us via BlueSky: https://bsky.app/profile/scriptedjournal.bsky.social
LinkedIn: https://www.linkedin.com/company/scripted-a-journal-of-law-technology-and-society/?viewAsMember=true

What can you expect from this Issue?

SCRIPTed would not be what it is without the contributions of its authors and generous reviewers. Thank you to the contributors to this latest issue and to the reviewers who have given their time to support the journal. The June 2026 issue contains what we at SCRIPTed value most, a diverse collection of scholarship that tackles different facets of law, technology, and society in action. Specialising in a breadth of disciplines and themes, this issue contains works addressing aviation and data protection and privacy, artificial intelligence, commercial sale of goods, copyright law, and more.

We begin with Arletta Gorecka's article "The Data Landscape of Aviation: Competition, Privacy, and Market Power under EU law". Addressing the digitalisation and competition issue of the European aviation sector, Gorecka highlights an emerging pattern of exploitation where passenger data becomes entangled in unfair market practices such as loyalty schemes, personalised pricing, and mandatory data sharing. Analysing the application of the Treaty on the Functioning of the European Union Article 102, Gorecka concludes that contemporary EU jurisprudence has privacy and competition tied together, wherein securing a passenger's right of privacy is a fundamental legal obligation and competitive factor.

Following a similarly close analysis on the European Union's jurisprudence, the EU Artificial Intelligence Act is put to the test with Fabian Teichmann's article "General-Purpose AI under the EU AI Act: A Conceptual

Allocation of Duties across the Value Chain". By closely dissecting the key actors and components of the Act, Teichmann draws the argument for the Act's enforcement architecture to work in coordination with its supervision of data protection, bringing a focused contrast between the UKs approach against the US. Conclusively, Teichmann shows optimism on the Act's multipurpose and inspiration for further global AI governance as well as recommendations going forward.

Providing the final macro analytical lens of our collection of articles is Dinushi Palawatta's work on "The Limits of Buyer Protection under the CISG: An SME Perspective". Providing a critical evaluation of the United Nations Convention on Contracts for the International Sale of Goods ("CISG"), Palawatta offers a "reality check" on the status and assumptions made in the CISG that disproportionately effect micro and small enterprises. Not only do SMEs have a limited capacity on technical legal expertise, but also on their physical size of employees and turnover. Following a close examination of the CISG, Palawatta contends that SME buyers ought to be treated as distinct actors in international sales law.

Along with this intellectually stimulating collection of original articles, this volume also includes two case comments and a selection of book reviews. In her case comment, Barasha Borthakur provides a welcome update on the treatment of the DABUS patent application in India and Indian Patent Office response on AI inventorship issues. Élodie Migliore also provides a case commentary on the Court of Justice of the European Union judgment in C-590/23, *Pelham II* where she turns to the interpretation of "pastiche" and its consequences for generative AI. Among our book reviews, Qi Jun Kwong starts us off with their review of "Deciphering IP Law and Its Conflict and Complementarity with Competition Law: Global Norms Against Asian Context" by Kung-Chung Liu. Extending conversations of "global" developments to other contexts, Te-Ying

Chen reviews "Chilling Effects: Repression, Conformity, and Power in the Digital Age" by Jonathan W. Penney. Continuing to think about the intersection between law and technology, Guan Yue Wu reviews "Law and Technology: A Methodical Approach" by Ryan Calo. Lastly, rounding out the discussion between law and technology, Jorge Balmaceda Hoyos reviews "Arcana Technicae: El derecho y la inteligencia artificial" (*Arcana Technicae: Law and Artificial Intelligence*) by Carlos Amunátegui Perelló.

A final thank you to our Editorial Team

The existence of this latest volume would not have been made possible without the dedication and tireless work of its editorial team. We would like to extend our gratitude to this year's Assistant Editors: Aaditya Bajpai, Anuj Nakade, Audrey Lepez, Francis Kaiser, Helena Broj, Isabelle Webb, and Tanya Proshak. Furthermore, we would like to thank Amandine Léonard and Jane Cornwell for supporting us during SCRIPTed's transition.

Rania Djojosugito
Editor-in-Chief

Aubrey Wasden
Managing Editor

scripted

Volume 23, Issue 01, June 2026

The Data Landscape of Aviation: Competition, Privacy, and Market Power under EU law

*Arletta Gorecka**

DOI: 10.2218/scrip.12286

Abstract

Competition law has long shaped the European aviation sector, from liberalisation in the 1990s to scrutiny of mergers and alliances. While past enforcement focused on slots, routes, and network structures, digitalisation has shifted competitive dynamics toward control over passenger data. Airlines and intermediaries now rely on vast datasets, raising novel issues under Article 102 TFEU. Data-driven practices, such as loyalty schemes, personalised pricing, and mandatory data sharing, can both entrench market power and undermine transparency, fairness, and privacy. Recent case law confirms that data protection concerns, particularly under the GDPR, may be relevant in competition assessments when dominant firms exploit consumers through unfair terms. In aviation, where choice is often limited and regulatory obligations complex, the intersection of competition, consumer, and privacy law is especially acute.

This article examines exploitative and exclusionary abuses linked to data, arguing that data has become aviation's "new jet fuel" and requires regulatory vigilance.

Keywords

EU competition law; data exploitation; aviation sector; abuse of dominance; consumer privacy

* Lecturer in Law, Glasgow International College, Glasgow, United Kingdom; arlettagorecka1@gmail.com

1. Introduction

Competition law has always played an important role in shaping the European aviation sector. From the liberalisation of airline markets in the 1990s to the scrutiny of major mergers and airline alliances, the European Commission has sought to ensure that consumers benefit from lower fares, greater choice, and fair conditions of access.[1] Traditionally, the focus of EU competition law in aviation has been on slot allocation at congested airports, route monopolies, and the structure of airline networks.[2] However, the rapid digitalisation of the industry means that competitive advantage is increasingly tied not only to physical assets such as fleets and airport slots, but also to control over data.[3]

Airlines and intermediaries such as booking platforms now process vast amounts of personal information, from frequent flyer records to biometric identifiers used at airport gates.[4] These data-driven practices raise important questions under Article 102 TFEU, which prohibits the abuse of a dominant position. In particular, the way passenger data is collected, combined, and used can both shape competition and affect passengers' fundamental rights to privacy. For instance, loyalty programmes can lock passengers into particular airline

[1] Pablo González Casín 'Airline cooperation and competition law: a transatlantic perspective. An analysis of case law and unrealized scenarios' (2025) 16(3) *Journal of European Competition Law & Practice* 151.

[2] Council Regulation (EEC) No 95/93 of 18 January 1993 on common rules for the allocation of slots at Community airports [1993] OJ L 14/1. Case C-127/21 P *American Airlines Inc v European Commission* ECLI:EU:C:2023:209. Case C-95/04 P *British Airways plc v Commission of the European Communities* ECLI:EU:C:2007:166 (*British Airways*). Case T-398/21 *Ryanair DAC and Ryanair Sun SA v European Commission* ECLI:EU:T:2025:222.

[3] Xiangsheng Dou 'Big Data and Smart Aviation Information Management System' (2020) 7(1) *Cogent Business & Management* 1766736.

[4] Haiyue Yuan, Matthew Boakes, Xiao Ma, Dongmei Cao and Shujun L 'Visualising Personal Data Flows: Insights from a Case Study of booking.com' (2023) arXiv <https://arxiv.org/abs/2304.09603> accessed 26 August 2025. Athina Ioannou, Iis Tussyadiah and Yang Lu 'Privacy concerns and disclosure of biometric and behavioral data for travel' (2020) *International Journal of Information Management* 102122. Caitlin Chandler 'Inside the Black Box of Predictive Travel Surveillance' (*Wired* 13 January 2025) <https://www.wired.com/story/inside-the-black-box-of-predictive-travel-surveillance/> accessed 25 August 2025.

groups, while personalised pricing based on behavioural profiling risks undermining transparency and fairness in ticket sales. [5] In each of these situations, the exercise of market power may overlap with concerns about excessive or intrusive data processing.

Recent developments in EU law highlight why this overlap matters. The Court of Justice has recognised that data protection rules, especially the General Data Protection Regulation (GDPR)[6], may be relevant in competition cases when a dominant company uses its position to impose unfair terms on consumers.[7] Although this principle emerged in the context of digital platforms, it has clear implications for aviation, where passengers often face limited choice and where airlines or intermediaries can make data-sharing a condition for accessing essential services. At the same time, aviation is subject to its own complex regulatory framework, including pricing transparency rules, safety requirements, and security-related data transfers, all of which interact with both competition law and privacy law.[8]

This article provides an overview of how Article 102 TFEU might apply to the use of data in aviation markets. It considers how exploitative practices, such as unfair data terms or discriminatory pricing, and exclusionary practices, such as the foreclosure of rivals through control of passenger data, could fall within

---

[5] Philip Georgiadis and Rachel Rees 'The lucrative business of airline loyalty schemes' (*Financial Times* 29 January 2025) <https://www.ft.com/content/85ddff1e-9552-4ff9-ae59-b688e2984d20> accessed 26 August 2025. Marco Alderighi, Consuelo R. Nava, Matteo Calabrese, Jean-Marc Christille and Chiara B. Salvemini 'Consumer perception of price fairness and dynamic pricing: Evidence from booking.com' (2022) 148 *Journal of Business Research* 769. Case C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt* ECLI:EU:C:2023:537 (*Meta Platforms*).

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[7] *Meta Platforms* (n 5).

[8] Francesco Sciaudone, *The Impact of Unfair Commercial Practices on Competition in the EU Passenger Transport Sector* (European Parliament 2020) <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/642381/IPOL_STU(2020)642381_EN.pdf> accessed 10 March 2026.

the scope of abuse of dominance. It also situates these issues within the broader EU regulatory environment, where competition, consumer protection, and privacy are increasingly intertwined. In doing so, the article highlights how data has become aviation's "new jet fuel" and why regulators may need to treat it as a central factor in maintaining both fair competition and passenger rights.

2. Dominance in Aviation Markets

In aviation markets, the concept of dominance has traditionally been grounded in control over infrastructure and route access.[9] Airlines with privileged access to congested airports, such as London Heathrow or Frankfurt, benefit from slot allocation systems that protect incumbents under so-called "grandfather rights." [10] These systems, entrenched in European law through Council Regulation (EEC) No 95/93, give dominant carriers a structural advantage by allowing them to retain slots year after year based on prior use. [11] Such arrangements, combined with strong network effects and economies of scale, have historically made it difficult for new entrants to compete on equal terms. This pattern is evident in merger cases such as *Ryanair/Aer Lingus*, where the European Commission intervened to block repeated acquisition attempts due to concerns over effective competition on Irish and UK routes.[12] In contrast, IAG's acquisition of Aer Lingus was cleared only after the company offered substantial remedies, including slot divestitures and access commitments.[13] These examples

[9] *British Airways* (n 2). EasyJet/GB Airways (Merger) (Commission Decision, Case COMP/M.4439, 18 January 2008). Case T-411/07 *Aer Lingus Group plc v European Commission* ECLI:EU:T:2010:281.

[10] Council Regulation (EEC) No 95/93 (n 2) art 8(2).

[11] *Ibid*.

[12] *Ryanair Holdings plc/Aer Lingus Group plc* (Commission Decision, Case COMP/M.6663, 27 February 2013).

[13] *International Consolidated Airlines Group SA/Aer Lingus Group plc* (Commission Decision, Case COMP/M.7541, 14 July 2015). European Commission 'Mergers: Commission Approves Acquisition of Aer Lingus by IAG, Subject to Conditions' (Press Release IP/15/5371, 14 July

reflect a longstanding regulatory focus on structural indicators of dominance, market shares, route overlaps, and physical access to airports.

However, this view of dominance is increasingly being challenged by the digital transformation of the aviation sector. Airlines today operate not only as transport providers but also as data platforms.[14] Through frequent flyer programs (FFPs), digital booking systems, mobile apps, and even biometric boarding technologies, they accumulate vast volumes of passenger data.[15] This data is used to optimise pricing, segment customers, and personalise offers, creating a deeper form of engagement that can significantly raise the cost of switching carriers.[16] Studies show that passengers approaching elite status in FFPs are more likely to remain loyal, even at the cost of higher fares.[17] Van Ommeren et al. estimated that these switching costs can amount to as much as 41% of the average ticket price for top-tier members.[18] Similarly, Orhun et al. found that proximity to loyalty milestones significantly increases consumer

2015) <https://ec.europa.eu/commission/presscorner/detail/en/IP_15_5371> accessed 17 June 2025.

[14] Ivan Verkalets 'Airline Industry Digital Transformation: Digital Aviation' (Coaxsoft, 19 December 2024) <https://coaxsoft.com/blog/airline-industry-digital-transformation> accessed 20 August 2025. Lucy Budd and Tim Vorley 'Airlines, Apps, and Business Travel: A Critical Examination' (2013) 9 *Research in Transportation Business & Management* 41. Eisquare 'Industry 4.0 Takes Flight: How Big Data, Artificial Intelligence, And The Internet Of Things Are Revolutionising The Aviation Industry' (20 September 2024) <https://www.eisquare.co.uk/blogs/how-bigdata-ai-and-iot-are-revolutionising-the-aviation-industry> accessed 26 July 2025.

[15] OAG 'Redefining Loyalty: The Next Frontier in Traveller Relationship' (20 May 2024) <https://www.oag.com/blog/redefining-loyalty-next-frontier-traveler-relationships> accessed 25 August 2025.

[16] Arkadiusz Tomczyk, Dimitrios Buhalis, Daisy XF Fan and Nigel L Williams 'Price-personalization: Customer Typology Based on Hospitality Business' (2022) 147 *Journal of Business Research* 462.

[17] Hande Şahin, Ali Osman Kuşakcı and Baboucarr Mbowe 'The Effects of Frequent Flyer Programs in the Airline Industry on Customer Loyalty' (2021) 3(2) *Heritage and Sustainable Development* 130.

[18] Jos van Ommeren, Christiaan Behrens and Gerben de Jong, *From Silver to Platinum: The Effect of Frequent Flier Tier Levels on Airline Demand* (Tinbergen Institute Discussion Paper No 21-077/VIII, Tinbergen Institute 2021).

stickiness, as travellers modify their choices to preserve or attain elite status.[19] These forms of behavioural lock-in bear a strong resemblance to the strategies employed by dominant tech platforms.

What makes these developments particularly relevant is that they mirror the shift in how competition law understands dominance more broadly. In the landmark *Intel* case, the Court of Justice clarified that even non-transparent, loyalty-based rebates could amount to abuse under Article 102 TFEU if they had the potential to exclude equally efficient competitors.[20] The focus was not on the price itself, but on how behaviour was being shaped through conditional incentives. A similar logic was applied in *Google Shopping*, where the Commission found that Google had abused its dominance by systematically favouring its own comparison-shopping service in search results.[21] This was not a matter of pricing, but of visibility, data control, and self-preferencing, tools that shaped user behaviour and distorted the competitive process.

These cases are highly instructive when thinking about the aviation sector today. As airlines gain ever more control over the digital travel journey, from search and booking through to in-flight and post-flight interaction, they are increasingly able to guide consumer choices, not through price or availability, but through loyalty incentives, personalised content, and data-driven offers. Marra noted that slot reform efforts are often undermined by these downstream dynamics, as airlines' data advantages allow them to monetise each slot far more effectively than potential rivals.[22] Similarly, Gal and Rubinfeld argued a point in the context of digital markets that in data-driven environments, dominance arises

---

[19] A Yeşim Orhun, Tong Guo and Andreas Hagemann, 'Reaching for Gold: Frequent-Flyer Status Incentives and Moral Hazard' (SSRN, 22 November 2018) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3289321 accessed 15 June 2025.

[20] Case C-413/14 P *Intel Corp Inc v European Commission* ECLI:EU:C:2017:632.

[21] Case T-612/17 Google LLC and Alphabet Inc v European Commission (Google Shopping) ECLI:EU:T:2021:763. (*Google Shopping*).

[22] Marleen Marra 'A Market for Airport Slots' (SSRN, 9 October 2024) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4948006> accessed 26 August 2025.

not only from scale but from the ability to predict and shape consumer preferences.[23] In fact, such stance could indicate that a dominance in aviation is no longer just about who controls the runway, it is also about who controls the relationship with the passenger. As airlines deepen their reliance on data and digital interfaces, traditional competition tools that focus solely on physical infrastructure may overlook the ways in which dominance is being sustained and extended through more subtle, non-price mechanisms. If competition authorities are to keep pace, they will need to consider how informational advantages and behavioural strategies can entrench market power, much like in the digital platform economy.

3. Data and Passenger Loyalty as Market Power

Frequent flyer programs represent one of the most pervasive sources of consumer lock-in.[24] Structurally, they are designed to incentivise continued patronage through tiered status rewards, mileage accrual, and access to benefits which increase in value as a passenger's engagement deepens.[25] Economically, this creates high switching costs: consumers who approach tier upgrades or accumulated benefits are less likely to consider alternative airlines, even when faced with lower fares or more convenient schedules.[26] When embedded within global alliances such as Star Alliance or Oneworld, the exclusionary potential of FFPs is amplified. Smaller, unaffiliated competitors are often unable to match the extended benefits that alliance members offer across routes, lounges, and status recognition. This creates a form of "ecosystemic dominance," wherein the

[23] Michal S Gal and Daniel L Rubinfeld, *Algorithms, AI and Mergers* (NYU Law and Economics Research Paper No 23-36, New York University School of Law 2023).

[24] Christiaan Behrens, Gerben de Jong and Jos van Ommeren 'From Silver to Platinum: The Impact of Frequent Flier Tier Levels on Air Travellers' Behaviour' (2024) 172 *Transportation Research Part B: Methodological* 102986.

[25] *Ibid*. pp. 2-3.

[26] *Ibid*.

competitive playing field is tilted not by price or frequency but by the cumulative reach of integrated loyalty networks.

Further concerns arise regarding data protection and privacy. Participation in loyalty programs typically involves the collection and processing of sensitive personal information, ranging from travel itineraries and purchase behaviours to location data and biometric identifiers.[27] However, consent to such data use is often bundled with general participation in the program, raising concerns under the GDPR. Article 4(11) GDPR requires that consent be freely given, specific, informed, and unambiguous; yet the structure of most airline loyalty schemes provides consumers with limited real control over how their data is used. This bundling effect undermines meaningful choice and may convert data-sharing into a de facto condition for access to competitive pricing or basic service features.[28]

Data advantages extend beyond loyalty systems into increasingly sophisticated pricing mechanisms. Airlines now deploy dynamic pricing models that adjust fares not only based on supply and demand, but also on personalised data such as user location, device type, browser history, and past search behaviour. [29] These practices, while often justified on grounds of revenue management efficiency, raise concerns under Article 102(a) TFEU, which

---

[27] European Parliament, Data Subjects, Digital Surveillance, AI and the Future of Work (European Parliament Research Service 2020) <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656305/EPRS_STU(2020)656305_EN.pdf> accessed 20 April 2025.

[28] Haggai Porat 'Behavior-Based Price Discrimination and Data Protection in the Age of Algorithms' (2026) 55(1) *The Journal of Legal Studies* 129. OECD, *Dark Commercial Patterns* (OECD Digital Economy Paper No 336, OECD Publishing 2022) <https://www.oecd.org/en/publications/dark-commercial-patterns_44f5e846-en.html> accessed 26 August 2025.

[29] OAG, 'Airline Pricing in 2025: How Shopping Data Unlocks Truly Dynamic Offers' (7 April 2025) <https://www.oag.com/airline-pricing-shopping-data> accessed 26 August 2025. Kat George 'When I Booked Flights Online I Noticed the Prices Kept Changing. Is It Legal in Australia? Can I Avoid It?' (*The Guardian*, 21 May 2025) <https://www.theguardian.com/lifeandstyle/2025/may/21/booking-flights-online-dynamic-pricing-ticket-is-it-legal-australia> accessed 20 August 2025.

prohibits the imposition of unfair prices by dominant undertakings. While the legal threshold for establishing exploitative pricing remains high, the opacity of algorithmic pricing systems complicates enforcement, especially where price discrimination is not transparent to consumers. Azzolina et al., in a study of airline e-commerce practices, underscored the difficulty regulators face in identifying systematic discrimination, even where pricing variation is real.[30] Similarly, as Aryal et al., claimed by assessing airline pricing, these data-driven systems allow firms to segment consumers across time and product offerings in ways that systematically extract surplus, particularly from those less able to optimise search or booking behaviour.[31] While such models may enhance short-term efficiency, they can erode long-term consumer welfare and reinforce dominance through informational asymmetries and behavioural conditioning.

4. Privacy as a Competition Parameter

The CJEU's recognition in *Meta Platforms v Bundeskartellamt* that privacy can constitute a dimension of "quality" in EU competition law highlights how exploitative conduct may extend beyond price manipulation or product features. By framing privacy protections as an essential aspect of service quality, the judgment provides a lens for assessing abusive practices in both digital and non-digital markets where consumers' personal data or other qualitative interests are leveraged by dominant firms.[32] In the consideration of the CJEU, privacy in the broader scope could be captured by the anticompetitive rules. In this article, the author would rely on the consideration of the "privacy-as-quality" to discuss competition law and privacy angle.

---

[30] Stefano Azzolina, Manuel Razza, Kevin Sartiano and Emanuel Weitschek 'Price Discrimination in the Online Airline Market: An Empirical Study' (2021) 16(6) *Journal of Theoretical and Applied Electronic Commerce Research* 2282.

[31] Gaurab Aryal, Charles Murry and Jonathan W Williams 'Price Discrimination in International Airline Markets' (2024) 91(2) *The Review of Economic Studies* 641.

[32] *Meta Platforms* (n 5) paras 48-51.

The theory of "privacy-as-quality" highlights that consumer welfare is not solely measured in terms of price, but also encompasses innovation, choice and quality, with privacy emerging as an increasingly salient component of quality in data-driven markets.[33] This theoretical approach acknowledges that in zero-priced services, personal data functions as a form of counter-performance, and excessive data extraction above a competitive level can reduce consumer welfare in a manner equivalent to charging supra-competitive prices. [34] The Bundeskartellamt case exemplifies this reasoning, as the Court recognised that the imposition of excessive data collection as a condition for access to a platform could distort the competitive process and harm consumers by degrading privacy protections.[35]

When transposed into the aviation sector, this reasoning exposes potential risks of exploitative abuse under Article 102 TFEU where dominant airlines or booking platforms leverage their market position to impose intrusive data practices on passengers. Air travel is increasingly digitised, with personal data collection embedded not only in online booking processes but also in ancillary revenue strategies, profiling-based marketing, and biometric boarding systems.[36] If access to essential air transport services is made conditional on consumers accepting excessive data processing, for example, compulsory enrolment in biometric identification systems or the tying of ticket purchases to profiling-

---

[33] Maurice E Stucke and Ariel Ezrachi 'When Competition Fails to Optimise Quality: A Look at Search Engines' (2016) 18 *Yale Journal of Law and Technology* 70. *Anticipated Acquisition by Facebook Inc of Instagram Inc* (Office of Fair Trading, Case ME/5525/12, 14 August 2012).

[34] Eleonora Ocello, Cristina Sjödin and Anatoly Subočs 'What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU Merger Case' (2015) 1 *European Commission Competition Merger Brief* 6. Mauro Luis Gotsch and Marcus Schögel 'Addressing the Privacy Paradox on the Organizational Level: Review and Future Directions' (2023) 73(2) *Management Review Quarterly* 263.

[35] *Meta Platforms* (n 5) paras 48-53, 68, 147-150.

[36] Alexander Grous, *Capitalising on Changing Passenger Behaviour in a Connected World* (London School of Economics and Political Science 2019) <https://www.lse.ac.uk/business/consulting/assets/documents/sky-high-economics-chapter-three.pdf> accessed 26 August 2025.

based ancillary services, passengers are effectively deprived of meaningful choice. In such circumstances, the airline extracts disproportionate value from consumers in the form of their data, thereby degrading the quality of the service offered. This can be characterised as exploitative conduct akin to imposing unfair trading conditions, since the consumer's privacy is diminished not as the result of competition on the merits, but because of the airline's market power.

The concept of "privacy-as-quality" is particularly useful here because it frames the reduction of privacy not as a "standalone" data protection issue, but as a degradation of a recognised parameter of product quality under competition law. The Commission has previously acknowledged in merger control, for instance in *Facebook/WhatsApp* and *Microsoft/LinkedIn*, that privacy protections can constitute an important dimension of competition between undertakings, with stronger privacy protections being seen as an indicator of higher product quality.[37] If this reasoning is extended to exploitative abuse cases, then reductions in privacy standards imposed unilaterally by dominant firms may be treated as a form of harm to consumer welfare.[38] In aviation markets, the imposition of mandatory profiling or biometric boarding systems could be understood in precisely this way: not only does it reduce passengers' ability to exercise control over their data, but it also effectively reduces the quality of the flight service by embedding an intrusive trade-off into an otherwise essential service.

However, significant methodological challenges remain. Competition law analysis has historically been anchored in price-centric tools such as the SSNIP (Small but Significant and Non-Transitory Increase in Price) test, and their direct transposition into zero-priced or hybrid markets such as aviation is problematic.

---

[37] *Facebook Inc/WhatsApp Inc* (Commission Decision, Case M.7217, 3 October 2014). *Microsoft Corp/LinkedIn Corp* (Commission Decision, Case M.8124, C(2016) 8404 final, 6 December 2016).

[38] Arletta Gorecka, *The Interface between Competition Law and Data Privacy Law: Violation of Privacy as an Exploitative Theory of Harm under Article 102 TFEU* (Springer Nature Switzerland AG 2024).

While some commentators propose the SSNDQ (Small but Significant Non-Transitory Decrease in Quality) test as a more appropriate tool, it has not yet been operationalised in case law, and its application to subjective parameters such as privacy is fraught with difficulties, given the heterogeneity of consumer preferences and the presence of information asymmetries.[39] In the aviation context, consumers may accept intrusive data practices not because they do not value privacy, but because air travel is an essential service with limited substitutes, leaving them locked in to privacy-invasive conditions. This structural lack of choice amplifies the exploitative character of excessive data collection and aligns with the rationale in *Meta Platforms*, where the Court underscored that coercive consent mechanisms linked to market power could be anticompetitive.[40]

Accordingly, while EU competition law has not yet explicitly confronted privacy intrusions in the aviation sector, the logic of "privacy-as-quality" provides a coherent framework for doing so. Where dominant airlines or booking platforms compel consumers to trade their data for access to core services, the practice could be framed as a reduction in quality that undermines consumer welfare and thus constitutes an exploitative abuse under Article 102 TFEU. Although the integration of privacy into competition analysis raises both conceptual and practical challenges, the broader trend in EU law recognises that quality-based harms, including privacy degradation, can and should be captured within the competition law framework, particularly in sectors where digitalisation has rendered privacy a central dimension of consumer experience.

---

[39] Aleksandra Gebicka and Andreas Heinemann 'Social Media & Competition Law' (2014) 37(2) *World Competition* 149.

[40] *Meta Platforms* (n 5) paras 147-150.

5. Potential Abuses Under Article 102 TFEU in Aviation

The increasing datafication of the airline industry has created novel avenues for abusive conduct under Article 102 TFEU, shifting the focus of enforcement from traditional capacity- or slot-based dominance towards informational control and behavioural lock-in. In line with the reasoning endorsed by the Court of Justice in *Meta Platforms* which confirmed that excessive data collection imposed as a condition of access can amount to an exploitative abuse, privacy must now be recognised as a parameter of quality in the aviation sector.[41] Airlines are no longer merely transport providers: they operate as data platforms, monetising passenger information through dynamic pricing, biometric processing, and loyalty-driven behavioural conditioning. In such an environment, the abuse of dominance may manifest less through overt price hikes or route foreclosure and more through subtle degradations in privacy and quality that nonetheless impair consumer welfare and distort market structure.

Exploitative abuse under Article 102(a) TFEU arises where a dominant airline imposes unfair trading conditions on passengers. Analogous to the *Meta Platforms* precedent, exploitative practices may include forcing passengers to consent to extensive data harvesting, covering travel history, payment details, geolocation, and biometric identifiers, as a precondition for booking tickets or enrolling in frequent flyer schemes.[42] Such bundled consent, unlikely to satisfy the GDPR's requirement of being "freely given, specific and informed" (Article 4(11) GDPR), acquires competition law relevance once tied to market power. Where personal data is used to fuel algorithmic fare differentiation or priority boarding allocation, consumers risk being subjected to unfair discrimination. Dynamic pricing strategies based on willingness-to-pay proxies, such as device used, browsing behaviour, or past purchasing patterns, may systematically

[41] *Meta Platforms* (n 5) paras 48-53, 68.
[42] *Ibid*.

disadvantage infrequent travellers, low-income passengers, or those less technologically literate. While airlines have long relied on yield management, the move towards opaque, data-driven personalisation blurs the line between commercial innovation and the imposition of unfair conditions, raising the possibility of Article 102(a) TFEU intervention in the same vein as *United Brands v Commission*, where unfair pricing and trading terms were central to the finding of abuse.[43]

Exclusionary abuse under Articles 102(b)–(d) TFEU is equally salient in this data-driven aviation ecosystem. Dominant airlines may refuse to share essential passenger data with rivals, such as loyalty histories, ancillary purchase profiles, or biometric verification data, thereby foreclosing effective competition in ticket distribution and ancillary services. The logic here resonates with *Bronner* [44] and *Microsoft* [45] where access to an input is indispensable for competitors to remain viable, denial without objective justification can amount to abuse. In aviation, the refusal to interoperate booking systems or biometric boarding infrastructure may prevent independent online travel agencies or smaller carriers from offering competitive alternatives, raising rivals' costs and entrenching the incumbent's advantage. This is not hypothetical, the Commission has historically scrutinised exclusionary airline practices, as in *Virgin/BA* [46] concerning travel agent incentive schemes, and in *Ryanair/Aer Lingus*[47] regarding foreclosure effects in minority shareholdings. Extending this logic to the data economy of aviation suggests that informational foreclosure can be as distortive as slot hoarding or predatory pricing.

---

[43] Case 27/76 *United Brands Company and United Brands Continentaal BV v Commission of the European Communities* ECLI:EU:C:1978:22.

[44] Case C-7/97 *Oscar Bronner GmbH & Co KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co KG and Others* ECLI:EU:C:1998:569.

[45] Case T-201/04 *Microsoft Corp v Commission of the European Communities* ECLI:EU:T:2007:289.

[46] *Virgin/British Airways* (Commission Decision 1999/480/EC, Case IV/D-2/34.780, [2000] OJ L 30/1).

[47] Case T-342/07 *Ryanair Holdings plc v European Commission* ECLI:EU:T:2010:280.

A further form of exclusionary abuse lies in the tying of FFPs to alliance ecosystems, effectively constructing "walled gardens" of loyalty.[48] Consumers who accrue points within Star Alliance or Oneworld face prohibitively high switching costs if they wish to fly with unaffiliated carriers. This phenomenon, previously addressed in the Commission's prohibition of SAS's EuroBonus program in Sweden and Norway,[49] is now compounded by the integration of personal data into loyalty systems. By leveraging dominance in one market segment (air transport on hub routes) to condition consumer behaviour in another (loyalty-driven retention), airlines risk infringing Article 102(d) TFEU, consistent with the principles articulated in *Tetra Pak II*.[50] The abusive effect does not derive from overt contractual exclusivity but from the behavioural lock-in generated by cumulative data and benefits, a subtle but powerful barrier to market entry for smaller rivals.

The interplay between exploitative and exclusionary abuses becomes particularly acute in data-driven aviation. Airlines with market power can simultaneously extract value from consumers through intrusive profiling and foreclose competitors by controlling the informational ecosystems necessary for effective rivalry. The strategic combination of personalised fare adjustments, loyalty-induced switching costs, and restricted data interoperability creates a competitive environment where incumbency is protected not by physical assets alone but by informational asymmetries. This dual abuse resembles the Commission's findings in *Google Shopping* [51] where leveraging a dominant platform position distorted competition both vertically and horizontally, albeit

[48] Kan Jie Marcus Ho 'The Faux Pas in Modern Competition Law – Walled Gardens, Data Sharing and Algorithmic Decision Making' (SSRN, 9 February 2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3785141> accessed 26 August 2025.

[49] *GFU – Norwegian Gas Negotiation Committee* (European Commission, Case COMP/36.072, closed by commitments, 17 July 2002).

[50] Case T-83/91 *Tetra Pak International SA v Commission* [1994] ECR II-755.

[51] *Google Shopping* (n 21).

in a non-price dimension. The aviation sector demonstrates how the same logic can migrate from digital platforms into traditional industries.

These dynamics demonstrate that the application of Article 102 TFEU in aviation cannot remain tethered to outdated metrics such as capacity control or slot allocation. Just as the Court in *Meta Platforms* recognised privacy as an element of quality, enforcement in aviation must adapt to account for the non-price parameters of competition increasingly central to consumer welfare. Tools such as a SSNDQ test, though still more conceptual than operational,[52] may offer a framework for analysing whether reductions in privacy protection constitute competitive harm. National authorities have already laid the groundwork: the Bundeskartellamt's willingness to treat privacy as a competition parameter, combined with the Commission's past scrutiny of FFPs and travel agency restrictions, suggests a legal and institutional readiness to extend Article 102 TFEU analysis to privacy-related abuses in aviation. The challenge going forward will be translating this recognition into robust enforcement methodologies capable of quantifying and remedying privacy degradation without collapsing competition law into data protection law. Properly calibrated, such an approach would preserve the integrity of consumer welfare analysis while ensuring that dominance in aviation is not exercised through opaque, exploitative, and exclusionary data practices.

6. Conclusion

Article 102 TFEU provides a powerful framework for addressing emerging forms of dominance in aviation markets driven by data. The EU's evolving jurisprudence demonstrates that privacy is no longer separate from competition:

---

[52] Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, *Competition Policy for the Digital Era* (European Commission 2019) 30 https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf accessed 10 December 2019

excessive data collection and exploitative digital practices can constitute abuses of dominance. In the context of EU aviation, the key challenge is to ensure open, competitive skies while safeguarding passengers' fundamental rights. Recognising privacy as a dimension of service quality underscores that protecting passenger data is not only a legal obligation but also a competitive factor that airlines must integrate into their business practices to maintain fair and effective competition.

scripted

Volume 23, Issue 01, June 2026

General-Purpose AI under the EU AI Act: A Conceptual Allocation of Duties across the Value Chain

Dr. iur. Dr. rer. pol. Fabian Teichmann, LL.M. (London), EMBA (Oxford)[*]

DOI: 10.2218/scrip.12300

Abstract
This article examines how the final version of the EU Artificial Intelligence Act ("AI Act", adopted 2024) allocates obligations across the AI value chain, with a focus on general-purpose AI ("GPAI") or foundation models. It proposes a taxonomy of key actors – foundation model providers, fine-tuners, integrators, and deployers – and analyses the interfaces between them, including documentation tools (model cards, system cards) and logging requirements. Building on principles of control, foreseeability, benefit, and capability, the article argues for a principled distribution of compliance duties: those who design and train foundational AI models should bear upstream transparency and safety obligations, while those who adapt or deploy AI in specific contexts shoulder downstream risk

management and oversight duties. The analysis discusses the EU Act's enforcement model (market surveillance authorities and an EU AI Office) and contrasts it with data protection supervision, highlighting the need for coordination in areas of overlap. A comparative outlook considers the UK's pro-innovation, context-driven approach and the evolving US regulatory landscape. Finally, the article offers recommendations for regulatory guidance and standards development (ISO/IEC, CEN/CENELEC) to support effective implementation, accounting for recent developments including the Digital Omnibus Regulation, the AI Office's emerging guidelines, and the broader debate on EU regulatory competitiveness triggered by the Draghi Report. This approach aims to clarify how the EU AI Act's final provisions on general-purpose AI models can serve as a global benchmark for balanced AI governance.

Keywords
EU AI Act; General-Purpose AI; Value Chain Allocation; Foundation Models; Regulatory Compliance

* Fabian Teichmann, PhD (Zurich), LL.M. (London), EMBA (Oxford) is an attorney-at-law and managing partner at Teichmann International (Switzerland) AG. He holds a graduate degree in Information Management Systems from Harvard University. teichmann@teichmann-law.ch

1 Introduction

The advent of general-purpose AI systems – exemplified by large language models like GPT-4 – has prompted regulators to rethink how AI is governed across its value chain. Unlike narrowly-purposed AI, these foundation models can be adapted to myriad downstream tasks, from writing code and offering medical advice to generating images and driving autonomous vehicles. Their versatility and widespread deployment raise complex questions of accountability: Who should ensure a powerful model is trained responsibly, and who is answerable if its use causes harm? The European Union's answer, in the newly adopted EU AI Act,[1] is to impose tiered obligations on different actors in the AI life cycle. This marks a shift from earlier drafts that focused only on end-use applications – the final Act squarely regulates general-purpose AI model providers (the upstream developers of foundation models) in addition to the providers and users of high-risk AI systems. The Act thereby inaugurates a hybrid governance approach: combining product safety-style market regulation with elements addressing fundamental rights, and extending compliance duties both upstream (at the model level) and downstream (at the application and deployment level).

The rapidly growing body of scholarship on the AI Act has begun to address the allocation of responsibilities across complex AI supply chains as one of the regulation's central challenges. The first article-by-article commentaries – notably the volume edited by Necati Pehlivan, Forgo and Valcke (2024) – provide granular doctrinal analysis of each provision, while Hacker (2024) has offered an influential account of how the Act distributes regulatory burdens between

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 1689/1 ("AI Act").

providers and deployers, identifying residual ambiguities around fine-tuning thresholds and downstream liability.[2] Veale and Zuiderveen Borgesius (2021) laid early groundwork by demystifying the Commission's original proposal and critiquing its product-safety orientation, work that Laux, Wachter and Mittelstadt (2024) extended by examining whether the Act's risk classification genuinely delivers on its promise of "trustworthy" AI.[3] Poncibó (2024) and Noto La Diega and Bezerra (2024) have interrogated the consumer protection and liability dimensions respectively, while Gstrein, Haleem and Zwitter (2024) focused specifically on how the Act's final text handles foundation models – an analysis on which the present article builds and to which it responds.[4] The present contribution differs from this existing literature by developing an integrated conceptual framework grounded in four allocation principles (control, foreseeability, benefit, and capability), by systematically mapping these principles onto the Act's specific provisions, and by offering concrete recommendations for standards development and regulatory guidance that take account of the most recent political and regulatory developments.

---

[2] Ceyhun Necati Pehlivan, Nikolaus Forgo and Peggy Valcke (eds), *The EU Artificial Intelligence (AI) Act: A Commentary* (Wolters Kluwer, 2024); Hacker P, "Comments on the Final Trilogue Version of the AI Act" (2024), available at SSRN: https://ssrn.com/abstract=4757603, 2.

[3] Johann Laux, Sandra Wachter and Brent Mittelstadt, "Trustworthy Artificial Intelligence and the European Union AI Act: On the Conflation of Trustworthiness and Acceptability of Risk" (2024) 18(1) *Regulation and Governance* 3-32, 6; Michael Veale and Frederik Zuiderveen Borgesius, "Demystifying the Draft EU Artificial Intelligence Act – Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach" (2021) 22(4) *Computer Law Review International* 97-112, 112.

[4] Oskar Josef Gstrein, Noman Haleem, and Andrej Zwitter, "General-Purpose AI Regulation and the European Union AI Act" (2024) 13(3) *Internet Policy Review* 1-26, 18–19; Guido Noto La Diega and Leonardo CT Bezerra, "Can There Be Responsible AI Without AI Liability? Incentivizing Generative AI Safety Through Ex-Post Tort Liability Under the EU AI Liability Directive" (2024) 32(1) *International Journal of Law and Information Technology* 1-21, 2–3; Larry DiMatteo, Cristina Poncibó and Geraint Howells, *The Cambridge Handbook of AI and Consumer Law* (Cambridge University Press, 2024), pp. 116–120.

This article proceeds as follows. Section 2 delineates a taxonomy of the relevant roles – foundation model providers, fine-tuners, integrators, and deployers – and the key interfaces between these actors, including documentation and logging mechanisms. Section 3 introduces the four allocation principles and examines how each informs the distribution of obligations between upstream and downstream actors. Section 4 analyses how liability and enforcement are structured under the AI Act's market surveillance model and contrasts this with the General Data Protection Regulation's ("GDPR's") data protection supervision regime,[5] highlighting coordination challenges. Section 5 broadens the perspective with a cross-jurisdictional analysis of the UK and US approaches, updated to reflect recent policy shifts. Section 6 presents recommendations for regulatory guidance and standardisation, taking account of the Digital Omnibus Regulation,[6] the AI Office's emerging guidelines,[7] and the wider debate on EU regulatory competitiveness. Section 7 concludes.

2 Conceptual Taxonomy of Actors and Interfaces

2.1 Actors in the AI Value Chain

Modern AI systems involve a multi-tiered supply chain. In the context of general-

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[6] European Commission, *Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)* COM(2025) 836 final (19 November 2025) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0836 accessed 17 June 2026.

[7] European Commission AI Office, *Guidelines on the Definition of an Artificial Intelligence System Established by Regulation (EU) 2024/1689 (AI Act)* (6 February 2025) <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application> accessed 17 June 2026.

purpose AI ("GPAI"), four main categories of actors can be identified, each bearing distinct obligations under the AI Act.

Foundation Model Providers are the organisations or individuals that develop large-scale GPAI models and place them on the market. Under the Act's definitions (Article 3), a provider of a GPAI model is a person or entity that develops a general-purpose AI model (or has it developed) and makes it available, whether for a fee or free. Examples include AI labs releasing models like GPT-4, Gemini, or open-source large models such as Llama. These actors are subject to Chapter V obligations specific to GPAI model providers, including documenting how the model was developed and tested, disclosing information about training data and model limitations, and implementing appropriate data governance measures (Article 53, Annexes XI-XII). The Act recognises that open-source models warrant differentiated treatment: if a model is released with full access to weights and sufficient documentation, certain documentation obligations may be adjusted (Recital 102). As Hacker (2024) has noted, the provision remains ambiguous on what degree of openness triggers this exception, and the AI Office will need to clarify this boundary through guidance.[8] The stakes are high, since an excessively broad exception could create a regulatory gap for powerful models released under permissive licenses, while an excessively narrow one could deter beneficial open-source development.

Fine-Tuners (Downstream Model Providers) adapt a pre-existing foundation model to create a new model, often for a more specific function or domain. Fine-tuners take a base model and train it further on domain-specific data or with additional objectives. The Act (Recital 97) acknowledges that GPAI models can be "further modified or fine-tuned into new models," and that

[8] Hacker (n 2), 6–7.

downstream entities doing so may themselves become providers with corresponding obligations. Recital 109 attempts to calibrate the burden: a fine-tuner's documentation duties should focus on the changes made, relying on the original model's documentation for the remainder. As Laux, Wachter and Mittelstadt (2024) observe, the threshold for when modification converts a fine-tuner into a "provider" of a new model remains one of the Act's most significant grey areas, with practical implications for the open-source ecosystem and for commercial fine-tuning services.[9] A start-up fine-tuning an open-source language model for legal advice, or a company adapting a general model for medical diagnostics, needs to know whether it has crossed the line into full provider obligations, including conformity assessment for a potentially high-risk system. Further guidance on this threshold – perhaps involving criteria such as the degree to which model behaviour is altered or whether it is repurposed for a high-risk use – is urgently needed.

Integrators (AI System Providers) embed an AI model into a final application or system, potentially combining it with other software or hardware, and determine the system's intended use. A medical device company that takes a pre-trained diagnostic model and embeds it in a clinical decision support tool is an integrator; a software firm that plugs a foundation model into an HR screening system is another. Under the Act, such an entity is the provider of an AI system and, if the system is high-risk under Annex III, it is subject to requirements including conformity assessment, risk management (Article 9), technical documentation (Annex IV), transparency, accuracy, and human oversight measures. The Act requires cooperation between the original GPAI model provider and the integrator: the provider must supply the information

[9] Laux et al (n 3), 26–27.

listed in Annex XII to enable the integrator's compliance (Article 53(1)(b)). As Veale and Zuiderveen Borgesius (2021) anticipated, this creates an information pipeline that depends heavily on the quality and completeness of upstream documentation. In practice, an integrator might receive a model card or technical dossier from the foundation model provider, use it to perform a risk assessment, and then produce system-level documentation covering how the model is used and controlled within the integrated application.[10]

Deployers are the natural or legal persons that use an AI system under their authority in a professional capacity (Article 3(4)). A hospital deploying an AI diagnostic tool, a bank using an AI system for credit scoring, or a public agency employing an AI system for automated decision-making are all deployers. Under the Act, deployers of high-risk AI systems bear their own set of obligations (Article 26): ensuring proper human oversight, providing training to personnel, monitoring the system's performance, maintaining automatically generated logs for at least six months, respecting transparency towards affected individuals, and performing fundamental rights impact assessments in certain use cases. Deployers must also use the AI system in accordance with the provider's instructions and must suspend use if the system is found non-compliant or poses a risk.

These roles can overlap in a single entity or be distributed across many. A large tech company might simultaneously serve as foundation model provider, integrator, and deployer. Conversely, in the open-source ecosystem, distinct independent actors may occupy each layer. The Act uses legal hooks like "placing on the market" and "putting into service" to attach obligations to

[10] Veale and Zuiderveen Borgesius (n 3), 103.

whichever entity effectively controls the AI's introduction into the EU market or usage environment.

2.2 Interfaces and Information Flows

For this chain to function safely, several interfaces – points of exchange of information and control – are critical.

Technical Documentation and Model Cards. The Act requires GPAI model providers to prepare technical documentation containing detailed information about the model's design, testing, and limitations (Annex XI), and to provide transparency information to downstream providers integrating the model (Annex XII, Article 53(1)(b)). This requirement aligns closely with the concept of Model Cards originally proposed by Mitchell et al. (2019) as a transparency measure for AI models.[11] A standardised model card describes the model's architecture, training data characteristics, intended uses, performance benchmarks (including across subgroups), known risks and failure modes, and guidelines for safe use. By standardising this interface, the Act ensures that integrators receive the information needed to perform their own risk management and compliance tasks.

System Documentation. When an integrator builds a high-risk AI system using a GPAI model, it must produce instructions for use and technical documentation (Annex IV) that describe the specific context of use, how the model is integrated, system-level performance metrics, human oversight provisions, and constraints on deployment. There is a clear through-line: the model card feeds into the system documentation. Where gaps remain, the Act's

[11] Margaret Mitchell et al., "Model Cards for Model Reporting" (2019) *Proceedings of the Conference on Fairness, Accountability, and Transparency*, https://doi-org.eux.idm.oclc.org/10.1145/3287560.3287596, 220–222.

cooperation requirement enables integrators to request further information from upstream providers. The emerging industry practice of "system cards" – exemplified by OpenAI's system card for GPT-4 – provides a model for how this information can be structured and communicated to deployers, regulators, and affected persons.

Logging and Record-Keeping. The Act mandates that high-risk AI systems be designed with automatic logging capabilities (Article 12), and deployers must maintain those logs for at least six months to enable tracing of decisions and investigation of incidents. For GPAI models designated as having systemic risk (Article 51), providers must implement post-market monitoring and incident reporting, which implies their own collection of telemetry data. Logging is therefore a two-way interface: it helps deployers supervise AI in operation and provides feedback upstream to model creators and regulators. As commentators have rightly flagged, the Act's logging requirements raise significant data protection questions, particularly regarding the storage of personal data in audit trails – a tension that requires coordinated guidance from AI and data protection authorities (see generally Noto La Diega and Bezerra 2024 on the interplay between AI regulation and liability frameworks).[12]

Contractual and Policy Interfaces. The Act effectively mandates certain contractual terms: GPAI providers must have a policy on compliance with EU data laws in training data (Article 53(1)(c)), and deployers must use AI systems in accordance with the instructions of use provided by the provider (Article 26(1)). These provisions ensure that information and constraints flow downstream in writing: the provider communicates intended use and limitations, and the deployer has a duty to respect them. Any integrator in

[12] Noto La Diega and Bezerra (n 4), 2–3, 7–8.

between must pass these on and potentially add further instructions specific to the integrated system. These contractual interfaces transform the regulatory obligation into a practical governance mechanism operating along the entire supply chain.

3 Allocation Principles: Control, Foreseeability, Benefit, and Capability

Allocating legal duties across different actors in the AI lifecycle should ideally follow principled criteria. The EU AI Act and broader regulatory-theoretical literature on risk governance reflect four interrelated principles – control, foreseeability, benefit, and capability. This section examines how each principle informs the distribution of obligations and applies them to the roles identified in Section 2.

3.1 Control

An overarching tenet is that the more control an actor exercises over the design or functioning of the AI, the greater their responsibility for preventing harm. In product safety law, manufacturers bear primary duties because they control product design. AI model developers exercise substantial control over model architecture, training data curation, and built-in safety mechanisms; accordingly, the Act requires them to implement appropriate data governance and risk mitigation measures before release (Article 53). They also control the upfront allocation of compute resources and know the scale of the model, which the Act leverages in identifying "systemic risk" models (e.g., providers know whether they exceed the 10^25 FLOP training threshold that triggers enhanced obligations under Article 51).

Downstream, deployers control the operational context – who uses the AI, for what tasks, and whether there are human checks – and are obligated to ensure proper use and the ability to intervene (Article 26). They can control input data quality in real-time and must do so (Article 26 requires ensuring input data relevance and integrity for high-risk AI).

The Act's treatment of open-source models exemplifies the alignment of responsibility with control: where model weights are freely released, certain provider obligations are relaxed because direct control over downstream use is relinquished (Recital 102). The rationale is that once control is lost – the model is "in the wild" – holding the original provider to some obligations is impractical; instead, the burden shifts to whoever takes that model and deploys it. As Hacker (2024) argues, the control principle also explains the escalating obligations for systemic-risk providers: the greater the model's capabilities and potential reach, the more consequential the provider's design choices become, justifying heightened regulatory scrutiny.[13]

Human oversight requirements similarly track control. Whichever actor can exert real-time intervention – typically the deployer or the person operating the system – must ensure its effectiveness (Article 14). The foundation model creator cannot directly ensure a human is in the loop during deployment; that responsibility lies with the deployer, who controls the operational environment.

3.2 Foreseeability

The law assigns duties to the party that can reasonably foresee and prevent potential harms. Upstream providers can foresee certain generic risks of their models: a large language model's propensity for generating disinformation or

[13] Hacker (n 2), 12–13.

toxic content, or its potential adaptation for hazardous purposes such as generating malware or lowering barriers to chemical weapon design. Article 53 accordingly requires GPAI providers to document "foreseeable unintended outcomes," and providers of systemic-risk models must "assess and mitigate systemic risks, including novel risks" (Article 55), implying pre-release red-teaming and safety testing to discover foreseeable failure modes.

Downstream actors have a better vantage point for context-specific risks. An integrator or deployer knows the specific application and user population. An HR deployer should foresee the risk that an AI system could discriminate in hiring and must check for relevant biases. A hospital deploying an AI diagnostic tool can foresee that doctors might over-rely on it, necessitating training to avoid automation bias. Article 26 and the fundamental rights impact assessment provisions compel deployers to formally evaluate impacts in their particular setting.

The concept of "reasonably foreseeable misuse" (Article 3(24)) requires providers to consider not only intended use but also how the system could be misused through human behaviour or interaction with other systems. As Laux, Wachter and Mittelstadt (2024) note, this foreseeability mandate places a significant burden on upstream developers to anticipate downstream applications, even where these are inherently difficult to predict.[14] Yet the principle also sets limits: the Act does not classify AI as high-risk in the abstract but by specific use (Annex III), recognising that a foundation model is not "high-risk" until it is deployed in a high-risk domain – at which point the foreseeability of high impacts activates for the integrator or deployer. In summary, foreseeability justifies requiring each actor to conduct risk assessments

[14] Laux et al (n 3), 6, 26–27.

appropriate to their stage: model providers conduct broad hazard analysis (bias, cybersecurity, misuse potential) before release, and deployers conduct context-specific impact assessments and monitoring during use. This prevents a situation where every actor defers responsibility, claiming the harm was not within their purview.

3.3 Benefit

This principle holds that those who derive economic benefit from AI should bear commensurate responsibilities for its impacts, reflecting a "polluter pays" logic. Foundation model providers profit from distributing their models; integrators profit from AI-powered products; deployers gain efficiency from AI deployment. The EU legislature explicitly recognised that the impact of GPAI is too significant to leave to a few powerful players reaping economic benefits without oversight (Recital 105). By extending obligations to GPAI providers – including public disclosure of training data summaries (Article 53(1)(d)) – the Act ensures that companies at the top of the value chain contribute to risk reduction rather than pushing all compliance costs downstream.

Similarly, deployers derive direct value from AI use and are accordingly charged with investing in staff training, performance monitoring, impact assessments, and transparency measures. If using AI saves a bank money through automated credit scoring, some of that saving must be reinvested in compliance measures – a fair allocation of the burden. Had the Act placed all obligations only on providers, deployers might externalise risk by using AI recklessly because "it was certified by the provider."

The benefit principle also underlies liability discussions. The proposed AI Liability Directive reflects the idea that the enterprise benefiting from deployment should bear responsibility for harms, especially where victims would otherwise go uncompensated. This alignment of "pay-off and

accountability" internalises the externalities of AI use, echoing basic fairness principles in regulation.

Benefit ties into power asymmetry as well. Foundation model providers are often major tech companies; deployers may be smaller organisations. The Act tries to be even-handed: obligations are assigned by role, not by size per se. However, Recital 109 and Article 56(5) introduce proportionality based on size and capacity, recognising that a small open-source developer should not bear the same burden as a large commercial AI lab. This tempering by the next principle – capability – ensures regulatory equity.

3.4 Capability

This principle considers the ability and resources of an actor to fulfil obligations. Foundation model developers possess specialised expertise (AI research talent, computing infrastructure) to conduct extensive testing – probing a model for biases, red-teaming for adversarial exploits, evaluating emergent capabilities. Downstream deployers typically lack these capabilities, treating the model as a given component. The Berkeley AI RMF Profile for GPAI explicitly notes that many risk controls – such as addressing emergent behaviours or installing safety mitigations – can only meaningfully be implemented by upstream developers who are "in a better position" than downstream actors.[15] For example, if a language model occasionally produces personal data from its training set (a privacy risk), the model provider is capable of detecting and minimising that through training adjustments or filters far more than an end-user deployer.

---

[15] Anthony Barrett et al, "AI Risk-Management Standards Profile for General-Purpose AI Systems (GPAIS) and Foundation Models" (2023) *CLTC Berkeley* (available at https://cltc.berkeley.edu/wp-content/uploads/2023/11/Berkeley-GPAIS-Foundation-Model-Risk-Management-Standards-Profile-v1.0.pdf) 7–8, 66–67.

Conversely, certain risk mitigations require local knowledge or real-time intervention that only downstream actors can provide. A hospital deploying an AI diagnostic tool is capable of performing clinical validation with its patient data and can impose usage protocols. The model maker cannot do this for every deployment. The Act accordingly requires deployers to monitor outcomes, keep logs, ensure human oversight, and suspend use if needed – tasks that leverage the deployer's on-site capability.

Economic and organisational capacity matters too. Recital 109 calls for codes of conduct to "take due account of the size of the provider and allow simplified compliance for SMEs and start-ups." Article 56(5) provides that reporting obligations for systemic-risk model providers should reflect differences in size and capacity. This capacity-based tailoring ensures that regulation does not inadvertently favour only the biggest players who can absorb high compliance costs. For instance, if a small company fine-tunes an open model for a niche application, it might not be realistic for it to run massive retraining to fix base model issues – instead, its obligation might reasonably be to document the limits and test the narrower use, while the heavy lifting of fundamental model improvements lies with the original provider.

Capability also involves technical access. A deployer using a black-box proprietary model via API cannot realistically explain how the model works internally – only the provider can (hence the Act requires GPAI providers to supply information and even source code to authorities upon request). If the model is open, a deployer might have more capability to inspect it and may then share responsibility for modifications.

3.5 Applying the Principles

In practice, these principles work together. The obligation to ensure "accuracy, robustness, and cybersecurity" of a high-risk AI system (Article 15) is distributed

precisely according to these criteria: the provider trains a robust model and discloses known accuracy limits (capability, control), the integrator validates for the specific application (capability, foreseeability), and the deployer monitors ongoing performance and secures the operational environment (control, capability). Each benefits from the system's accuracy (benefit) and thus has aligned incentives.

By aligning obligations with who holds the levers (control), who can anticipate issues (foreseeability), who gains from the AI (benefit), and who can act to mitigate (capability), the framework aims for both efficiency and fairness. No actor is overburdened with tasks beyond its reach, and none can evade responsibility by pointing fingers. This approach reflects what the regulatory literature calls shared responsibility in complex supply chains – fair precisely because it is grounded in these factors. It also helps interpret grey areas: if a question arises whether a fine-tuner or the original model provider should fix a particular issue, we can ask – who has the control over that aspect of the model and the capability to address it?

4 Liability and Enforcement under Market Surveillance vs. Data Protection Supervision

4.1 The AI Act's Enforcement Architecture

The enforcement of the AI Act is entrusted to national Market Surveillance Authorities ("MSAs"), coordinated at EU level by the European AI Board and the AI Office. This mirrors the New Legislative Framework for traditional product regulation, where each Member State has authorities ensuring that products on the market comply with EU safety rules. MSAs have powers including requiring information from providers, ordering corrective actions, banning or recalling non-compliant AI systems, and issuing administrative fines.

For general-purpose AI models specifically, enforcement is more centralised. The Commission and the AI Office directly enforce the Chapter V provisions (Articles 53-55) in cooperation with Member States. The AI Office can investigate foundation models and, if a provider of a systemic-risk model fails to cooperate, the Commission can impose fines up to 3% of worldwide turnover. This centralisation was a deliberate design choice, recognising that foundation model providers are few, often headquartered outside the EU, and that a unified approach avoids the bottlenecks experienced under GDPR. As Hacker (2024) observes, the EU appears to have learned from the GDPR experience – where Ireland's DPA effectively set the enforcement pace for all of Europe through the one-stop-shop mechanism – by opting for direct Commission involvement for the highest-impact upstream actors.[16]

The Act's penalty regime (Article 99) is tiered by severity: up to 7% of global annual turnover (or EUR 35 million) for prohibited practices, 3% for GPAI provider non-compliance, and lower tiers for other breaches. These thresholds exceed GDPR's 4% ceiling, signalling the EU's intent to make AI rule-breaking potentially more costly.

The European AI Board, comprising Member State representatives and the Commission, will facilitate consistent application and develop guidance. However, unlike the European Data Protection Board's ("EDPB's") binding dispute resolution mechanism under GDPR Article 65, the AI Board has more limited powers – consistency will depend on coordination and Commission oversight. The AI Office itself has begun issuing operational guidance, including on prohibited practices (effective February 2025) and on GPAI model obligations,

[16] Hacker (n 2), 7–8.

though stakeholders have raised concerns that some guidance has been published too close to compliance deadlines.

4.2 Data Protection Supervision and Overlap

The GDPR is enforced by independent Data Protection Authorities ("DPAs") through a cooperation mechanism for cross-border cases. Because AI systems frequently process personal data, both the AI Act and GDPR will often apply simultaneously. A biometric identification system in a public space engages the AI Act (high-risk classification under Annex III) and GDPR (processing of biometric data) in parallel. A company deploying such a system could face scrutiny from an AI MSA checking conformity and accuracy requirements, and from a DPA checking lawfulness of data processing and purpose limitation.

The AI Act states it is "without prejudice to" GDPR and other data protection laws, meaning compliance with both is required simultaneously. Some Member States have signalled that their DPAs will handle certain AI Act aspects – the Netherlands' DPA announced its expectation to be involved in AI Act enforcement, and German data protection commissioners have argued for a role given their experience in algorithmic assessments. Other States will establish separate AI authorities. The resulting institutional landscape requires robust coordination to avoid duplicated enforcement, inconsistent demands, and regulatory arbitrage.

Commentators have highlighted a particularly acute tension: the Act requires deployers to maintain logs for at least six months, while GDPR's data minimisation principle may pull in the opposite direction where logs contain personal data. A related issue arises where the AI Act requires training data transparency summaries but GDPR's storage limitation principle would call for deletion of personal data no longer needed. These conflicts are not irreconcilable – logging for legal compliance can be grounded in GDPR Article 6(1)(c) and data

minimisation can be addressed through pseudonymisation and aggregation – but they require coordinated regulatory guidance.

4.3 Civil Liability

The AI Act's administrative fines do not directly compensate those harmed by AI. The proposed AI Liability Directive ("AILD"),[17] though not yet enacted, would complement the Act by relaxing the burden of proof on causality: if a provider violates an AI Act requirement designed to prevent the kind of harm that occurred, a rebuttable presumption of causality would arise. This essentially binds regulatory obligations to civil accountability: breach of the AI Act eases the victim's path to compensation. The updated Product Liability Directive,[18] which explicitly covers software and AI, further clarifies producers' strict liability for defective AI outputs.

The interplay is designed to close the accountability loop: the AI Act establishes duties (breach constitutes fault or defect), and the liability framework channels that breach into redress for victims. This ensures both deterrence (via administrative fines) and compensation (via civil liability), addressing what scholars including Vasudevan (2023) and Lior (2021) have identified as the critical gap in pre-Act AI governance.[19] The allocation principles discussed in

---

[17] Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) COM(2022) 496 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496 accessed 17 June 2026.

[18] Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC [2024] OJ L, 2024/2853 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024L2853 accessed 17 June 2026.

[19] Anat Lior, "Artificial Intelligence and Tort Law: Who Should Be Held Liable When AI Causes Damages?" available at https://il.boell.org/en/2021/12/24/artificial-intelligence-ai-tort-law-and-network-theory-who-should-be-held-liable-when-ai; Amrita Vasudevan, "Addressing the Liability Gap in AI Accidents" (2023) *Centre for International Governance Innovation Policy Brief No. 177*, available at https://www.cigionline.org/static/documents/PB_no.177.pdf.

Section 3 – control, foreseeability – will inevitably influence courts and the application of the AILD: who controlled the relevant aspect of the AI, and who could have foreseen the harm, will determine where liability falls.

5 Cross-Jurisdictional Perspective

Regulation of AI is a global challenge, with different jurisdictions pursuing markedly different approaches. This section compares the EU's framework with developments in the United Kingdom and United States, focusing on general-purpose AI governance and updated to reflect significant recent policy shifts.

5.1 United Kingdom

The UK, no longer bound by EU regulations post-Brexit, has chosen not to replicate the EU AI Act. Instead, the UK government set out its approach in a White Paper titled "A pro-innovation approach to AI regulation",[20] characterised by non-statutory guidance, reliance on existing regulators and laws, and five cross-cutting principles: safety, transparency, fairness, accountability, and contestability. These principles are to be interpreted and applied by existing sectoral regulators – the Financial Conduct Authority ("FCA"), Medicines and Healthcare products Regulatory Agency ("MHRA"), Information Commissioner's Office ("ICO"), Equality and Human Rights Commission, and others – within their respective domains.

The White Paper acknowledged foundation models as a "novel challenge" for governance, noting that only a "relatively small number of organizations" develop them and that "it can be challenging to identify and allocate

[20] Department for Science, Innovation and Technology, *A Pro-innovation Approach to AI Regulation* (CP 754, March 2023) https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper accessed 17 June 2026

accountability for outcomes" when these models are used widely. However, the UK chose not to impose statutory obligations on foundation model providers, preferring a monitoring-and-evidence approach. Initiatives include the AI Safety Institute (established with GBP 100 million in funding, succeeding the Foundation Model Taskforce) and the Bletchley Declaration on frontier AI safety – cooperative risk governance rather than hard regulation.

The Department for Science, Innovation and Technology's ("DSIT's") voluntary Code of Practice for Foundation Model Developers aligns substantively with many AI Act themes – data transparency, robust testing, information sharing with downstream users – but remains non-binding. [21] The Competition and Markets Authority ("CMA") published draft principles on foundation models addressing competition and consumer protection,[22] while the ICO has issued AI-specific guidance on data protection, bias, and transparency.[23]

The UK's approach distributes accountability through existing legal frameworks: employers deploying AI must comply with the Equality Act,[24] financial institutions with FCA rules, healthcare providers with MHRA medical device regulations. This represents diffuse accountability buttressed by broad duties of responsible use. It lacks the EU's sharp delineation of role-specific

---

[21] Department for Science, Innovation and Technology, *AI Cyber Security Code of Practice* (31 January 2025) https://www.gov.uk/government/publications/ai-cyber-security-code-of-practice accessed 17 June 2026.

[22] Competition and Markets Authority, *AI Foundation Models: Initial Report* (18 September 2023) https://www.gov.uk/government/publications/ai-foundation-models-initial-report accessed 17 June 2026.

[23] Information Commissioner's Office and The Alan Turing Institute, *Explaining Decisions Made with AI* (20 May 2020) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-ai/ accessed 17 June 2026.

[24] Equality Act 2010.

obligations, though individual regulators are beginning to fill the gap with sector-specific guidance. The White Paper itself concedes that foundation models' "wide-reaching impact… means they are unlikely to be directly caught by any single regulator," and the UK has signalled that if voluntary measures prove insufficient, statutory regulation may follow.

5.2 United States

The US regulatory landscape for AI has undergone significant shifts. The Biden Administration's approach centred on the National Institute of Standards and Technology's ("NIST's") voluntary AI Risk Management Framework,[25] which provides a structured approach for identifying, assessing, and managing AI risks through four functions (Govern, Map, Measure, and Manage); the Blueprint for an AI Bill of Rights,[26] outlining five principles for the design and use of automated systems; and Executive Order 14110 on Safe, Secure, and Trustworthy AI,[27] which invoked the Defense Production Act[28] to require developers of very large models to notify the government and share safety test results.

However, the change of administration in January 2025 brought a sharp reversal. President Trump revoked Executive Order 14110 in his first days in office, signalling a clear preference for deregulation and innovation-led growth

---

[25] National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (NIST AI 100-1, US Department of Commerce, January 2023) https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf accessed 17 June 2026. (NIST AI RMF).

[26] White House Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People* (October 2022) https://www.govinfo.gov/app/details/GOVPUB-PREX23-PURL-gpo193638 accessed 17 June 2026.

[27] Executive Order No 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 88 Fed Reg 75191 (1 November 2023) https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence accessed 17 June 2026.

[28] Defense Production Act of 1950, 50 USC §§ 4501–4568.

over prescriptive safety mandates. This revocation removed the mandatory reporting requirements for developers of large models and weakened the executive branch's direct oversight role. The current US approach relies primarily on sectoral enforcement through existing agencies: the Federal Trade Commission ("FTC") enforces against deceptive or unfair AI practices under consumer protection law; the Equal Employment Opportunity Commission ("EEOC") holds employers responsible for discriminatory AI hiring outcomes under Title VII; the Food and Drug Administration ("FDA") reviews AI-based medical devices under existing device regulations; and state-level legislation continues to expand (e.g., the Colorado AI Act,[29] Illinois BIPA,[30] New York City's bias audit law for automated employment decision tools).[31]

NIST's AI RMF remains influential as a voluntary benchmark, including its GPAI Profile[32] which provides detailed guidance for foundation model developers on risk governance, testing, and documentation. However, without the mandatory reporting requirements of the now-revoked Executive Order, the framework's reach is limited to voluntary adoption and market pressure from customers demanding assurance.

The US approach effectively places primary legal responsibility on deployers: employers, banks, and other end-users face liability under anti-

---

[29] Colorado Artificial Intelligence Act, Colo Rev Stat §§ 6-1-1701–6-1-1711 (2024) https://leg.colorado.gov/bills/sb24-205 accessed 17 June 2026.

[30] Illinois Biometric Information Privacy Act, 740 ILCS 14/1–99 (2008) https://law.justia.com/codes/illinois/chapter-740/act-740-ilcs-14/ accessed 17 June 2026.

[31] New York City Local Law No 144 of 2021 (Automated Employment Decision Tools), codified at NYC Administrative Code §§ 20-870–20-874 https://www.nyc.gov/site/dca/about/automated-employment-decision-tools.page accessed 17 June 2026.

[32] National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile* (NIST AI 600-1, US Department of Commerce, July 2024) https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf accessed 17 June 2026.

discrimination, consumer protection, and sector-specific statutes, and in turn pressure AI vendors through contracts to provide bias audits, documentation, and indemnities. This market-driven chain obligation partially mirrors the EU's value-chain allocation but without the statutory granularity of the Act's role-specific duties.

5.3 Convergence Through Standards

Despite divergent regulatory philosophies, convergence is emerging through international standards. ISO/IEC 23894 (risk management), [33] ISO/IEC 42001 (AI management systems),[34] and the work of CEN-CENELEC JTC 21[35] provide a common technical vocabulary. An AI developer following these standards may simultaneously satisfy EU harmonised standard requirements, UK recommended practice, and US NIST guidance. The anticipated "Brussels Effect" – whereby companies preparing for EU AI Act compliance extend those practices globally – is already visible, as it occurred with GDPR. Foundation model providers operating across jurisdictions will find it more efficient to implement a single, EU-Act-aligned governance system than to maintain separate regional processes.

The growing transatlantic divergence following the US deregulatory shift may, however, create pressure on EU policymakers from industry arguing for regulatory "parity." The EU should resist a race to the bottom while remaining

---

[33] International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC 23894:2023 Information Technology—Artificial Intelligence—Guidance on Risk Management* (ISO 2023) https://www.iso.org/standard/77304.html accessed 17 June 2026.

[34] International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC 42001:2023 Information Technology—Artificial Intelligence—Management System* (ISO 2023) https://www.iso.org/standard/81230.html accessed 17 June 2026.

[35] CEN-CENELEC Joint Technical Committee 21, *Artificial Intelligence* https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/ accessed 17 June 2026.

pragmatic about implementation timelines and compliance burdens – a balance explored further in the recommendations below.

6 Recommendations for Guidance and Standardisation

Drawing from the analysis above and accounting for recent regulatory and political developments, this section presents recommendations for clarifying and operationalising the allocation of AI governance duties across the value chain.

6.1 Develop Detailed Guidance on Role-Specific Obligations

Regulators should issue interpretative guidance concretely delineating the obligations of each actor under various scenarios. The AI Office has begun this process: its General-Purpose AI Code of Practice,[36] published in draft form in late 2024, represents an important first step. However, gaps remain. Guidance should clarify what constitutes "sufficiently detailed" documentation for a foundation model, perhaps aligning with the content of model cards (architecture, training data summary, intended uses and limits, known risks) and referencing Annexes XI-XII as checklists. It should clarify when a downstream modifier becomes a "provider" of a new model, providing thresholds or criteria – for instance, if model behaviour is significantly altered or if it is fine-tuned for a high-risk use, the fine-tuner likely assumes provider duties. This could prevent uncertainty that discourages beneficial adaptations. For integrators, guidance should outline how to fulfil system-level requirements using upstream documentation – a blueprint for creating Annex IV technical documentation for a system incorporating a

[36] European Commission AI Office, *First Draft of the General-Purpose AI Code of Practice published, written by independent experts* (14 November 2024) https://digital-strategy.ec.europa.eu/en/library/first-draft-general-purpose-ai-code-practice-published-written-independent-experts accessed 17 June 2026.

GPAI model, including how to perform a gap analysis between the model's Annex XII information and the system's risk assessment needs. For deployers, sector-specific guidelines on implementing Article 26 obligations should be produced in cooperation with industry associations – for instance, how to conduct a Fundamental Rights Impact Assessment in employment contexts, and how to set up logging and human oversight in practice, ideally aligned with existing frameworks (such as Data Protection Impact Assessments ("DPIAs") under GDPR or safety management systems) to avoid duplication.

6.2 Foster Collaborative Interface Mechanisms

To ensure smooth information exchange between upstream and downstream actors, stakeholders should standardise the format and content of key documentation artefacts. Regulators should endorse and potentially mandate a standardised model card format for GPAI providers to use when complying with Article 53(1)(b) and (d). The format should include sections on model overview (architecture, size), intended purposes, training dataset overview, performance benchmarks, limitations and known failure modes, and usage guidelines. The AI Code of Practice (Article 56) can incorporate the requirement for signatories to publish model cards according to this template, enabling semi-automated compliance and ensuring downstream integrators know exactly where to find needed information.

Integrators should be encouraged to produce system cards documenting the specific context of use, how the model is integrated, performance in that context, human oversight and risk mitigations, and constraints on use. Making a summarised system card public could improve transparency and trust for users and affected persons.

Standardisation bodies (CEN-CENELEC JTC 21[37], ISO/IEC JTC1 SC 42[38]) should prioritise developing a technical standard for AI system logging: what events should be logged, format requirements, retention periods, and data protection safeguards. The CEN-CENELEC "AI Trustworthiness Framework"[39] standard under development should be accelerated and designated as a harmonised standard once published. Collaboration with data protection experts is essential to ensure logging does not violate GDPR – for instance, by logging references or hashed values rather than raw personal data.

6.3 Leverage International Standards

The Commission should actively adopt relevant AI standards to confer presumption of conformity. CEN/CENELEC standards on AI Risk Management and Quality Management Systems should be aligned with ISO/IEC 23894:2023[40] and ISO/IEC 42001[41] and cited in the Official Journal as harmonised standards for Article 9 and Article 17 compliance. Standards such as CEN/CLC ISO/IEC/TR 24027:2023 (bias measurement)[42] and CEN/CLC ISO/IEC/TR 24029-1:2023 and EN ISO/IEC 24029-2:2023 (robustness assessment)[43] should be referenced for

---

[37] *Supra* (n 35).

[38] International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC JTC 1/SC 42 – Artificial Intelligence* https://www.iso.org/committee/6794475.html accessed 17 June 2026.

[39] CEN-CENELEC JTC 21 (n 35).

[40] *Supra* (n 33).

[41] *Supra* (n 34).

[42] CEN-CENELEC, *CEN/CLC ISO/IEC/TR 24027:2023 Information Technology—Artificial Intelligence (AI)—Bias in AI Systems and AI Aided Decision Making (ISO/IEC TR 24027:2021)* (CEN-CENELEC 2023).

[43] CEN-CENELEC, *CEN/CLC ISO/IEC/TR 24029-1:2023 Artificial Intelligence (AI)—Assessment of the Robustness of Neural Networks—Part 1: Overview (ISO/IEC TR 24029-1:2021)* (CEN-CENELEC 2023). CEN-CENELEC, *EN ISO/IEC 24029-2:2023 Artificial Intelligence (AI)—Assessment of the Robustness of Neural Networks—Part 2: Methodology for the Use of Formal Methods (ISO/IEC 24029-2:2023)* (CEN-CENELEC 2023).

compliance with the Act's data governance (Article 10) and accuracy/robustness (Article 15) requirements. Standards for AI evaluation methodologies and auditor qualifications should be developed to ensure consistency among notified bodies. These technical recipes reduce ambiguity in the Act's open-textured obligations, giving companies clear methods for demonstrating compliance and enabling a degree of global alignment through dual ISO/CEN adoption.

6.4 Account for the Evolving Political and Regulatory Context

Several developments since the Act's adoption require attention in implementation.

The Digital Omnibus Regulation.[44] The Commission's proposed Simplification Omnibus (November 2025) would amend the AI Act alongside the Cybersecurity Act and Machinery Regulation, seeking to reduce compliance costs, particularly for SMEs. Proposals include extended timelines, simplified conformity procedures for lower-risk applications, and clearer guidance on the interplay between the AI Act and sectoral product legislation. These simplification measures should be welcomed insofar as they genuinely reduce unnecessary burden, but must not hollow out the Act's substantive protections – particularly the transparency and risk management requirements that form the backbone of the value-chain allocation described in this article.

The Draghi Report and Competitiveness Debate. The Draghi Report on European competitiveness (September 2024)[45] identified overregulation as a drag on innovation and urged the EU to shift toward an "innovation principle." While it did not specifically target the AI Act, its broader critique has fuelled calls

---

[44] *Supra* (n 6).

[45] European Commission, *The Draghi Report on EU Competitiveness* https://commission.europa.eu/topics/competitiveness/draghi-report_en accessed 17 June 2026.

from industry associations for a moratorium on AI Act enforcement deadlines. Major groups including BusinessEurope and DigitalEurope have argued that enforcement should be delayed until sufficient guidance, standards, and compliance tools are available.[46] These calls warrant a calibrated response: compliance timelines should be realistic and accompanied by adequate guidance and tooling, but a blanket moratorium would undermine the Act's credibility and the EU's standard-setting position. The better approach is to accelerate the production of harmonised standards, templates, and guidance so that compliance becomes technically feasible before enforcement begins.

AI Office Guidelines.[47] The AI Office has been issuing guidance on prohibited AI practices, GPAI model obligations, and the Code of Practice. These are essential for translating the Act's legal text into operational requirements. Stakeholders have noted that some guidance has arrived late relative to compliance deadlines, creating uncertainty. The AI Office should publish a clear roadmap of forthcoming guidance, with deadlines aligned to enforcement milestones.

The US Deregulatory Shift. The Trump Administration's revocation of Executive Order 14110 creates a growing transatlantic divergence. EU policymakers should be aware that this divergence may intensify pressure from EU-based companies arguing for regulatory "parity." However, the EU's comparative advantage lies in offering a predictable, rights-protective framework that can serve as the global baseline.

---

[46] BusinessEurope, *Joint Industry Statement on the EU Artificial Intelligence (AI) Act* (2025) https://www.businesseurope.eu/publications/joint-industry-statement-on-the-eu-artificial-intelligence-ai-act/ accessed 17 June 2026. DigitalEurope, *Joint Industry Statement on the AI Omnibus: Administrative Clean-up or a Boost for Europe's AI Competitiveness?* (12 March 2026) https://www.digitaleurope.org/news/joint-industry-statement-on-the-ai-omnibus-administrative-clean-up-or-a-boost-for-europes-ai-competitiveness/ accessed 17 June 2026.

[47] *Supra* (n 7).

6.5 Enhance Coordination Between AI and Data Protection Regimes

The EDPB and the European AI Board should produce joint guidance on conducting combined DPIAs and Fundamental Rights Impact Assessments, reconciling logging with data minimisation, and delineating lead authority responsibilities. Memoranda of understanding between national AI authorities and DPAs should be established where they are separate bodies. A streamlined incident notification mechanism should be developed for events implicating both regimes. Joint guidance should also clarify that actions to comply with the AI Act (e.g., collecting sensitive attribute data for bias testing) can be legally grounded under GDPR where done proportionately, and that explanation requirements under both regimes can be aligned so that one disclosure satisfies both.

6.6 Encourage Sector-Specific Implementation

Different industries will apply the Act's requirements in domain-specific contexts. Sectoral guidance for healthcare AI (building on medical device regulations and ISO 81001-1:2021[48]), financial services AI (through EBA/ESMA codes of conduct), and public sector AI (integrating human rights obligations with AI Act requirements) should translate general obligations into domain-appropriate practices. Regulatory sandboxes (Article 57) should be actively used to pilot compliance approaches. SME-friendly templates, checklists, and open-source compliance tools should be funded through the Digital Europe Programme and Horizon Europe.

---

[48] International Organization for Standardization and International Electrotechnical Commission, *ISO 81001-1:2021 Health Software and Health IT Systems Safety, Effectiveness and Security—Part 1: Principles and Concepts* (ISO/IEC 2021) https://www.iso.org/standard/91523.html accessed 17 June 2026.

6.7 Strengthen Upstream-Downstream Communication Through Contracts

The AI Office should publish recommended contractual clauses for agreements between GPAI providers and downstream actors, analogous to GDPR standard contractual clauses. These should cover obligations to supply Annex XII information, notify downstream parties of newly discovered risks, cooperate in remediation, and respect usage instructions. Model providers of systemic-risk GPAI should maintain awareness of significant downstream deployments to enable prompt risk communication, akin to product recalls. Third-party certification schemes and trust marks for GPAI models, leveraging Article 57, can reduce duplicated due diligence while maintaining accountability. An information clearinghouse – an online portal where GPAI providers post model cards, risk analyses, and usage guidelines – could particularly assist SMEs and open-source users.

6.8 Ensure Adaptive Governance

The Commission's mandated review (Article 112) should specifically assess whether the allocation of duties remains appropriate as technology evolves. An expert advisory group should continuously monitor AI developments and recommend adjustments. International regulatory dialogue through the EU-US Trade and Technology Council and the Global Partnership on AI should facilitate convergence. The AI Office should publish regular reports on the state of AI compliance and the risk landscape, flagging systemic implementation challenges and recommending solutions.

7 Conclusion

This article has developed a conceptual framework for understanding how the

EU AI Act allocates governance duties across the AI value chain. Four allocation principles – control, foreseeability, benefit, and capability – provide the normative foundation for the Act's stratified approach: foundation model providers bear upstream transparency and safety obligations because they control model design and possess the capability for extensive testing; fine-tuners inherit and extend those obligations proportionate to their modifications; integrators shoulder system-level risk management and conformity assessment duties as the actors who determine intended use; and deployers assume responsibility for operational oversight, logging, and context-specific risk mitigation.

This allocation represents a significant evolution from the Act's earlier drafts, which overlooked general-purpose AI entirely. It also reflects a broader regulatory maturation: the recognition that complex AI supply chains require shared responsibility, with each actor's obligations calibrated to their actual position in the chain. The comparative analysis confirms that while the UK and US pursue different regulatory strategies – principles-based guidance and sectoral enforcement, respectively – the underlying problem of distributing accountability across the AI lifecycle is universal, and convergence through international standards is already under way.

The Act's success will depend on implementation. The recommendations presented here – from harmonised standards and model documentation templates to regulatory coordination mechanisms and adaptive governance – aim to translate the legal framework into operational reality. Recent developments underscore the need for both rigour and pragmatism. The Digital Omnibus proposals, the AI Office's emerging guidelines, the Draghi Report's competitiveness critique, and industry calls for a moratorium on enforcement deadlines all reflect legitimate concerns about readiness. The appropriate response is not to delay the Act but to accelerate the production of the tools –

standards, guidance, templates, compliance toolkits – that make compliance feasible and proportionate, particularly for SMEs and open-source developers.

The EU AI Act offers a principled and potentially global benchmark for distributing AI governance duties. Its framework of accountable handoffs – where documentation, testing results, and risk assessments flow along the supply chain from upstream to downstream – creates a chain of trust in which each actor knows its role and can verify that others are fulfilling theirs. If effectively implemented, this approach can serve not only Europe but, through the Brussels Effect and international standard-setting, the wider global effort to ensure that the benefits of general-purpose AI are realised in a manner that is innovative, trustworthy, and respectful of fundamental rights.

scripted

Volume 23, Issue 01, June 2026

The Limits of Buyer Protection under the CISG: An SME Perspective

*Dinushi Palawatta**

DOI: 10.2218/scrip.12298

Abstract

This article critically evaluates whether the United Nations Convention on Contracts for the International Sale of Goods (CISG) provides adequate protection for micro and small enterprise (SME) buyers in international business-to-business (B2B) transactions. The CISG is founded on the assumption that commercial parties possess comparable bargaining power, legal expertise, and capacity to safeguard their interests. However, this assumption increasingly diverges from commercial reality, as micro and small enterprises participate more actively in cross-border trade. Focusing on key provisions governing nonconformity and remedies, including Articles 35, 38, 39, 47, and 49, the article demonstrates that the CISG's strict notice requirements, indeterminate legal standards, and reliance on judicial discretion can impose disproportionate procedural and legal burdens on SME buyers.Brief comparative reference to English law illustrates that, although domestic legal frameworks may offer greater doctrinal certainty in some respects, they similarly fail to recognise the structural vulnerability of SME buyers. The article contributes to existing scholarship by shifting focus from abstract doctrinal balance to the

practical impact of CISG rules on vulnerable business participants. The article concludes by proposing recognition of SME buyers as a distinct category in international sales law.

Keywords : CISG, English law, SME protection, international sales, buyer remedies, comparative law

*Lecturer in Law, Faculty of Engineering and Management, The Ocean University of Sri Lanka; dpalawatta@yahoo.com.

1 Introduction

This paper mainly focuses around investigating how the United Nations Convention on Contracts for the International Sale of Goods (CISG)[1] safeguards the interests of (SME) buyers in international Business to Business transactions (B2B). The law treats B2B contracts differently from Business to Consumer contracts (B2C), based on the assumption that the parties involved in B2B agreements possess sufficient commercial knowledge to understand the risks. However, SME buyers may lack the expertise of experienced commercial buyers, a gap that existing legal frameworks often overlook in favour of consumer protection.[2] SME buyers are typically enterprises with fewer than 10 employees and limited turnover.[3] Like consumers, SME buyers usually lack in-house legal expertise, bargaining power, and experience in negotiating complex commercial contracts. This problem is especially prevalent in cross-border transactions. Therefore, they should be awarded heightened protections like those given to consumers because they often share comparable vulnerabilities.

Treating them as commercially sophisticated simply because they operate as businesses overlooks their practical limitations. In international sales governed by frameworks like the CISG, SME buyers face significant challenges such as complying with strict notice requirements[4] and understanding ambiguous legal provisions. These burdens mirror the issues consumers face, yet

---

[1] United Nations Convention on Contracts for the International Sale of Goods (adopted 11 April 1980, entered into force 1 January 1988) 1489 UNTS 3 (CISG).

[2] Neda B Marvasti et al. 'Is This Company a Lead Customer? Estimating Stages of B2B Buying Journey' (2021) 97 *Industrial Marketing Management* 126, 127.

[3] *Cambridge Dictionary*, 'Microbusiness' https://dictionary.cambridge.org/dictionary/english/microbusiness accessed 25 July 2025.

[4] CISG art 39.

consumer protection laws often exclude them solely due to their legal status as "businesses."

The UNIDROIT Principles which shelter all classes of international sales transactions, unlike CISG which exclusively governs international sale of goods transactions, rejects the universal postulation that businessmen are always experienced professionals with equal degree of bargaining power.[5] Since one - shareholder companies qualify within the definition of a business entity,[6] the practical difference between SME buyers and consumers involved in commercial transactions will not be upheld theoretically.

This paper contributes to existing legal scholarship by drawing attention to the overlooked category of SME buyers in international B2B transactions. It challenges the assumption that all business buyers are commercially sophisticated and highlights how e-commerce and simplified incorporation have expanded this category to include vulnerable entities. The paper also identifies judicial discretion (not jurisdiction) as the key cause of inconsistent CISG application, particularly under Articles 38 and 39. By proposing a redefinition of business buyers into micro, SME, and professional categories, the paper offers a novel framework for future legal reform and improved buyer protection mechanisms.

The paper undertakes a brief comparison between English law and the CISG in the final section. Unlike the CISG, English law relies on a domestic framework characterised by greater doctrinal certainty and remains a frequently used benchmark in comparative sales law. The comparison is not intended to determine which system is universally superior. Instead, it seeks to assess

---

[5] Michael Joachim Bonell 'The CISG, European Contract Law and the Development of a World Contract Law' (2008) 56 *The American Journal of Comparative Law* 1, 3.

[6] *Salomon v A Salomon & Co Ltd* [1897] AC 22 (HL).

whether the challenges faced by SME buyers arise from the CISG itself or from a broader failure of commercial sales law which failts to recognise the distinct vulnerabilities of smaller business entities. By comparing the two regimes, the paper evaluates whether greater legal certainty translates into stronger practical protection for SME buyers.

2 Structural vulnerability of SME buyers in international trade

According to the United Nations Commission on International Trade Law, small to medium-sized businesses and traders in developing nations are seen as the primary beneficiaries of the CISG, as they often have limited access to legal services during contract negotiations and are vulnerable to issues arising from a lack of legal knowledge.[7] The United Nations Commission on International Trade Law recognized the potential existence of weaker parties in contracts who might struggle to understand and balance their rights.[8] As such, the commission expected the CISG to serve as a regulatory framework that would balance the interests of both sellers and buyers in international sales agreements. However, existing literature appears to challenge this view.

CISG's boundaries are confined to B2B transactions.[9] B2B transactions are defined as dealings between two enterprises. The term "business" lacks a definition and law finds it undesirable to exhaustively define the term.[10] This

---

[7] United Nations Commission on International Trade Law, *The United Nations Convention on Contracts for the International Sale of Goods* (UNCITRAL 2020).

[8] *Ibid.*

[9] Rouven F Bodenheimer and Axel Benjamin Herzberg 'Commercial CISG'(*Changing Perspectives*) <https://www.changing-perspectives.legal/commercial/types-of-contracts/sale-of-goods/cisg/> accessed 28 February 2026.

[10] *LexisNexis Legal Glossary*, 'Business' <https://www.lexisnexis.co.uk/legal/glossary/business#:~:text=The%20following%2C%20amongst%20other%20thi ngs,role%20of%20an%20investor%3B%20the> accessed 28 February 2026.

lacuna has resulted in the inability to define B2B transactions. Thus, sole traders, single shareholder and multinational companies are considered B2B businesses. Legislation predominantly focuses on protecting consumer buyers, and the presumed sophistication and experience attached to B2B buyers have resulted in lack of protection to B2B buyers coming from unsophisticated backgrounds.

According to the UK Department for Business and Trade, micro-businesses (0 to 9 employees) make up 95.5% of the total UK business population.[11] Hence there are over 5.5 million businesses as of 2023.[12] The Companies Act 2006 was a major legislative reform that simplified company formation to promote entrepreneurship which contributed to this exponential rise. It also expanded the legal category of "business buyers" to include many entities lacking commercial or legal sophistication. In parallel, the OECD (2022) reports that digitalisation in e-commerce has made international trade more accessible to SMEs but also exposed them to higher transactional risks due to limited legal capacity and lack of face-to-face interaction.[13]

Moreover, a 2020 UNCTAD survey on the impact of COVID-19 on e-commerce found that 42% of small firms began or expanded online selling without adequate legal knowledge of cross-border protections.[14] These businesses though classified as "professional" buyers under instruments like the CISG, often mirror consumers through their behaviour and resource limitations. The European Commission has also recognised that SMEs face barriers in cross-

---

[11] Department for Business and Trade, *Business Population Estimates for the UK and Regions: 2023* (2023) <https://www.gov.uk/government/statistics/business-population-estimates-2023> accessed 25 July 2025.

[12] *Ibid*.

[13] OECD, *SME and Entrepreneurship Outlook 2022* (OECD Publishing 2022) <https://www.oecd.org/industry/sme-outlook/> accessed 25 July 2025.

[14] UNCTAD, *COVID-19 and E-commerce: A Global Review* (2021) <https://unctad.org/webflyer/covid-19-and-e-commerce-global-review> accessed 25 July 2025.

border enforcement and suffer from a lack of information on legal rights.[15] These trends collectively demonstrate that the legal definition of "business buyer" no longer aligns with the practical realities of many market participants. Thus, the rise of micro-businesses and digital trade resulted in the dilution of the effectiveness of buyer protections that were originally designed for more sophisticated entities.

The reduced focus on B2B buyers in international sales contracts can be understood in the context of the past, when the internet was still developing, and business startup regulations were stricter. However, today, many economies have simplified these rules to support smaller businesses, highlighting the need for updated considerations in protecting B2B buyers. For example, the introduction of the Companies Act 2006 in England and Wales greatly simplified the process of incorporating a business entity. The Act adopted a "think small first" approach, aiming to create rules that are suited for smaller businesses, while larger corporations could continue to navigate their more complex requirements.[16] This led to the rise of small private entities.

It has become increasingly important to protect the interests of business buyers, particularly those who may be misunderstood or overshadowed by the term "company." These buyers may not fully grasp the negative aspects of operating a business entity through a company, making the need for clearer protections more relevant today.

---

[15] European Commission, *Evaluation of the Small Business Act for Europe* COM(2015) 550 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0550> accessed 25 July 2025.

[16] Jonathan Hardman and Guillem Ramirez Santos 'Empirical Evidence for the Continuing Need to 'Think Small First' in UK Company Law' (2023) 24 *European Business Organization Law Review* 117, 118.

Wolfel and Grosse-Ruyken's article highlights how literature often overlooks the impact of power imbalances on suppliers.[17] This paper argues that this focus is less critical because, if suppliers meet their contractual obligations by delivering quality goods on time, then, buyers typically have no opportunity to act opportunistically. In contrast, sellers have more opportunities to exploit the power imbalance, such as by disguising the true quality of goods. Awarding consumer-style protection would help level the playing field. This is especially critical in the digital economy. Presently, the advancement of technology facilitates microbusinesses to engage in high-risk online transactions without the safeguards afforded to individual consumers. Extending consumer-like protection to SME buyers would not only promote fairness but also encourage entrepreneurship.

This article focuses specifically on buyers because the principal difficulties examined arise from obligations imposed upon buyers under the CISG rather than sellers. Articles 38 and 39 require buyers to inspect goods within a reasonable time and provide timely notice of non-conformity, failing which they may lose access to otherwise available remedies. These provisions place a disproportionate burden on SME buyers, who often lack the legal, technical, and financial resources needed to comply with complex procedural requirements in international transactions. By contrast, sellers are not exposed to equivalent procedural barriers that may result in the forfeiture of substantive rights.

It is worth noting that B2B contracts do not receive the same level of protection as B2C contracts. For instance, certain terms in B2C contracts may be deemed invalid under English Law due to unfairness,[18] but such protections do

[17] Joachim Wölfel and Pan Theo Grosse-Ruyken 'Bilateral Opportunism in Buyer–Supplier Partnerships' (2020) 27(3) *Journal of Business-to-Business Marketing* 247, 248.

[18] Consumer Rights Act 2015 s 62(4).

not apply to B2B contracts. The legal protection for B2B buyers is further reduced in international supply contracts because provisions in the Unfair Contract Terms Act 1977 (UCTA) do not apply to these agreements.[19] For example, in the case of *Phoenix Interior Design Limited v Henley Homes Plc*, an exclusion clause in a B2B contract was deemed ineffective because it failed to meet the reasonableness test under UCTA.[20] The supplier attempted to wholly exclude liability for defects if the customer failed to pay for goods. However, when the customer withheld payment upon discovering that the goods were defective, the supplier was not allowed to invoke the exclusion clause to avoid liability due to the application of UCTA. If this had been an international sales contract, the buyer would have had no legal recourse, as UCTA 1977 would not apply.

In B2C contracts, sellers are often legally prohibited from limiting their liability for certain breaches, whereas similar clauses in B2B contracts may still be valid. Laws in many jurisdictions, including those in England and international conventions like the CISG, provide some protection for B2B buyers from seller abuses. However, the question arises whether such protections are adequate in today's digital economy, where businesses are no longer limited to larger companies.

Some B2B buyers, particularly smaller entities, may require broader protection from sellers who often have greater bargaining power. Consumers typically lack negotiating power when entering contracts,[21] but B2B buyers could negotiate specific terms. For instance, it is legally possible to include contractual terms that are not explicitly written in the contract. Despite this negotiating

---

[19] Unfair Contract Terms Act 1977 s 26.

[20] *Phoenix Interior Design Ltd v Henley Homes plc* [2021] EWHC 1573(QB).

[21] Thomas C Kaiser 'Negotiating with a Customer You Can't Afford to Lose' (*Harvard Business Review*, November 1988) < https://hbr.org/1988/11/negotiating-with-a-customer-you-cant-afford-to-lose > accessed 14 June 2025.

capacity, SMEs operating as B2B buyers, often lack the knowledge to fully leverage this opportunity to protect their interests. In B2B contracts, the rights and liabilities of each party are often more heavily negotiated than in consumer contracts, which can be complex and difficult for small business owners to navigate. While consumer contracts often use standard templates,[22] B2B contracts are more tailored. Therefore, concerns of B2B buyers, particularly small businesses, need to be carefully reviewed and addressed, with particular attention to the size of the business.

3 CISG provisions and their effect on SME buyers

3.1 Doctrinal Balance vs Commercial Reality: Where Do SME Buyers Stand?

Luiz Moser's global survey assessing parties perceptions prior to choosing a governing law identified lawyers perceiving CISG as a choice which is needlessly benevolent towards buyers as a reason for excluding it from sales contracts.[23] Schwenser and Hachem in their research discovered German legal practitioners viewing CISG as extremely buyer-oriented owing to its employment of Anglo-American concepts such as strict liability and the notice requirement.[24] These conflicting ideas represent the current debate surrounding whether the CISG is buyer-friendly or seller-friendly but do not engage with the question of how the CISG impacts SME buyers.

---

[22] *Ibid.*

[23] Luiz Gustavo Meira Moser 'Parties' Preferences in International Sales Contracts: An Empirical Analysis of the Choice of Law' (2015) 20 *Uniform Law Review* 19, 20.

[24] Ingeborg Schwenzer and Pascal Hachem 'The CISG – Successes and Pitfalls' (2009) 57 *The American Journal of Comparative Law* 457, 471.

Uniform laws like the CISG are designed to balance the duties and obligations of buyers and sellers in international sales contracts.[25] However, parties to these contracts often resist applying national law, as it could provide an advantage to the party domiciled in that jurisdiction, enabling them to access legal advice and act strategically, even potentially masking breaches of contract. Spagnolo state that unfamiliarity with the CISG is a reason many counsels opt out of its provisions.[26]

Article 30 of the CISG outlines the seller's obligation to deliver goods, relevant documents, and transfer property in the goods as per the contract or the convention.[27] Similarly, Article 53 mandates the buyer to pay the agreed price and take delivery of the goods.[28] These provisions seem to balance the rights of both parties at the beginning and end of a contractual agreement. If the seller fulfils their obligations and the buyer accepts and pays for the goods, both parties' rights will be protected, and the effectiveness of the CISG in balancing their rights may not be questioned.

However, these initial provisions assume that business parties are equally knowledgeable and fair, which is not always the case. CISG's provisions related to buyers' rights against nonconforming goods or breach of contract by the seller provide an opportunity to assess how well it protects SME buyers from potential abuse. Articles 35 to 44 focus on nonconforming goods, and Articles 45 to 52

---

[25] Herbert Lazerow 'Uniform Interpretation of CISG' (2019) 52(3) *The International Lawyer* 369, 387.

[26] Lisa Spagnolo 'Green Eggs and Ham: CISG, Path Dependence, and the Behavioural Economics of Lawyers' Choice of Law in International Sales Contracts' (2010) 6(2) *Journal of Private International Law* 417, 422.

[27] CISG art 30.

[28] *Ibid* art 53.

address remedies available to buyers when facing issues like non-delivery or lack of conformity.[29]

3.2 Article 38 and the "Short Period" Dilemma: Efficiency or SME Risk?

Article 35 specifies that the seller must deliver goods that match the contract's quantity, quality, and description, and that are packaged as agreed. Goods are considered nonconforming if they do not meet these standards or are not fit for the intended purpose.[30] Further, goods are considered nonconforming if they are not fit for their ordinary or intended purpose, fail to match the quality of a sample, or are improperly packaged.[31] However, if the buyer agrees to receive nonconforming goods or is aware of the nonconformity when the contract is made, the seller is not liable for the actual nonconformity.[32] While the CISG includes implied terms like satisfactory quality and description, it also respects party autonomy by allowing deviations from these terms if agreed upon by both parties.[33] If a buyer knowingly consents to nonconforming goods, it can be argued that this exclusion of liability is not a violation of the buyer's interests, as it reflects the buyer's agreement. SME buyers are often in a weaker negotiating position in this situation. They may feel pressured to accept nonconforming goods clauses to secure supply relationships, especially when dealing with dominant suppliers. Although party autonomy allows buyers to agree to such terms, SMEs are more likely to agree without fully appreciating the commercial and legal risks involved.

---

[29] *Ibid* art 35 to 52.
[30] *Ibid* art 35.
[31] *Ibid*.
[32] *Ibid* art 35(3).
[33] *Ibid* art 6.

The issue arises when a buyer receives nonconforming goods that they neither consented to nor were aware of at the time of the contract. Article 36(1) of the CISG holds the seller liable for delivering nonconforming goods that exist at the time the risk is transferred to the buyer.[34] However, Articles 38 and 39 impose practical requirements that the buyer must meet to hold the seller liable for nonconformity.[35] In practice, many CISG-related litigations revolve around non-conforming goods,[36] revealing that commercial transactions often deviate from the ideal scenario where both parties fulfil their obligations.

Article 38, mandates that buyers must examine the goods upon receipt to retain their right to remedies for nonconformity.[37] This requirement ensures that nonconformity is identified at the point of risk transfer from the seller to the buyer, preventing sellers from being held liable for issues that arise after delivery. This provision can be a balanced mechanism, as it provides protection for both parties since buyers are able to confirm the seller's breach, and sellers are shielded from unjust claims.

However, the time constraints set by Article 38 are problematic for buyers. Article 38 specifies that buyers must examine the goods with/in a "short period" and notify the seller of any nonconformity.[38] While this provision facilitates the swift resolution of disputes, it creates a potential injustice for buyers, especially when the goods are complex or require extensive inspection. For example, inspecting sophisticated goods like airplanes may require significantly more time than inspecting simpler goods. The narrow time frame for examination may

---

[34] *Ibid* art 36(1).
[35] *Ibid* arts 38, 39.
[36] Amy H. Kennedy 'Recent Developments: Non-Conforming Goods under the CISG – What's a Buyer to Do' (1998) 16 *Dickinson Journal of International law* 319, 323.
[37] CISG art 38.
[38] *Ibid*.

prevent buyers from thoroughly assessing the goods and, if they fail to notify the seller within the specified period, they may lose their right to any remedy. Overall, Article 38 of the CISG can be both beneficial and challenging for SME buyers, but it is generally riskier for SMEs than advantageous in practical terms.

On the positive side, Article 38 helps SME buyers by requiring prompt inspection of goods, which can protect them from long-term disputes and ensure that sellers are held accountable for nonconformity discovered at the point of delivery. This can be useful for small businesses that need quick resolution of quality issues to maintain smooth business operations. However, the strict time requirement can be particularly harmful to SME buyers. Small businesses often lack specialised technical staff and advanced inspection facilities to properly examine complex goods within a short period. Unlike large commercial buyers, SMEs may struggle with detailed testing or quality verification, especially for technically complex products. If SMEs fail to notify sellers within the required timeframe, they risk losing legal remedies even if the goods are defective.

The critical issue here is whether the "short period" for examination, as prescribed in Article 38, should be flexible based on the nature of the goods. According to Ferrari, Article 38 should require immediate examination, which would ensure that any defects present at the point of delivery are identified.39 However, the uniformity of this short period fails to account for practical differences between types of goods. The time allowed to inspect sophisticated goods should arguably be more generous than for basic goods, as the complexity of the goods may require more time for an accurate inspection.

Case decisions on this matter would be essential to determine whether courts have recognized the need to adapt the time required for inspection to the

---

[39] Franco Ferrari 'Divergence in the Application of CISG's Rules on Nonconformity of Goods' (2004) 68(3) *Rabels Zeitschrift für ausländisches und internationales Privatrecht* 473, 478.

nature of the goods involved. While the provisions of the CISG, particularly those related to examination and notification of nonconformity, seem to balance the interests of both parties, a strict application of the "short period" for inspection creates potential disadvantages for all forms of buyers, including SMEs, especially those dealing with complex goods.

In the case of *M SpA v N*, the buyer was allowed to claim damages for nonconformity despite not inspecting the goods immediately.[40] The court ruled that the buyer could only discover the defect after using the cooling installations for a sufficient period, emphasizing the need to consider the practical realities of the situation. The court's interpretation was not strictly formalistic; it recognized that the buyer should have had time to use the goods before uncovering the defect, thus considering the surrounding circumstances. Therefore, the court took a more flexible approach, recognizing that a "short period" for inspection should be adapted to the specific circumstances of the case.

Contrastingly, in the case of *Roelants B.V v Beltronic Engineering*,[41] a Belgian buyer received defective rolls and refused to pay after complaints from clients. The court held that the buyer failed to examine the goods as soon as possible and did not give timely notice of the nonconformity. The defects, such as bad printing and perforations, were easily discoverable, so the court concluded that the buyer should have inspected the goods promptly. The court's reasoning also considered the surrounding circumstances, such as the buyer's uncertainty about the quality of previous deliveries. Given these facts, the court found it reasonable to expect the buyer to inspect the goods more promptly and notify the seller of any defects.

---

[40] *M SpA v N* (Rechtbank van Koophandel Ieper (Belgium), 29 January 2001) (*M SpA*).

[41] *Roelants Eurosprint BV v Beltronic Engineering International BVBA (*Rechtbank van Koophandel Hasselt (Belgium), 6 March 2002, AR 01/2703).

These two cases show a contrast in the application of Article 38, highlighting that the CISG provides flexibility for courts interpreting the "short period" for inspection based on the specific circumstances of each case. The *M SpA* case[42] demonstrates a buyer-friendly, flexible approach, while *Roelants B.V* illustrates a stricter,[43] more formal interpretation that aligns with the convention's requirement for timely inspection and notification. The differing judicial interpretations of Article 38 highlight the complexity of balancing buyer and seller interests under the CISG, and the importance of contextual factors in determining the rights and responsibilities of parties.

The interpretation of Article 38 of the CISG has sparked considerable debate regarding its fairness, particularly in balancing the interests of buyers and sellers. The case law highlights that a strict interpretation of the Article can sometimes lead to outcomes that disadvantage buyers, particularly in situations where the goods are complex or technical. For example, in a German case, the buyer discovered that two engines were non-conforming and sent them to a university for confirmation.[44] However, the court imposed a duty on the buyer to inspect the goods within a few working days, ignoring the fact that the engines were highly technical and required more time for proper inspection. This strict adherence to a short inspection period did not consider the complexity of the goods, which highlights a flaw in how Article 38 is often applied in certain jurisdictions, especially in Germany.

[42] *M SpA* (n 40).
[43] *Roelants Eurosprint* (n 41).
[44] *LG Düsseldorf* 31 O 231/94 (23 June 1994, Germany).

This case contrasts with the more lenient approach taken by courts in France[45] and Belgium,[46] where judges consider the practical circumstances surrounding the inspection of goods.

Kennedy argues that courts should be more lenient towards buyers by granting them a longer period to inspect goods if they can demonstrate diligence in doing so.[47] This perspective holds merit, especially considering the complex nature of some goods, such as highly technical machinery. While Kennedy's suggestion to extend the inspection period may appear fair, it must be noted that Article 38 already mandates courts to consider practical circumstances when determining the time frame for examination. The cases from Germany, however, demonstrate a strict and formalistic approach that does not account for the nature of the goods or the buyer's ability to conduct a thorough inspection in a short time frame.

The conflict between jurisdictions that interpret Article 38 strictly (like Germany) and those that prioritize practical considerations (like France and Belgium) shows a divergence in how the CISG's provisions are applied. Thus, the debate surrounding CISG Article 38's interpretation underscores the tension between legal formality and the need for flexibility to accommodate the complexities of international commerce, particularly when it comes to safeguarding the interests of business buyers, especially those dealing with sophisticated or technical goods.

3.3 Timely and Adequate Notice under the CISG

Under Article 39 of the CISG, buyers are required to give notice of any

---

[45] *Roger Caiato v Société Française de Factoring International Factor France* (Cour d'appel de Grenoble (France) Chambre Commerciale, 13 September 1995, no 48992) (*Roger Caiato*).
[46] *M SpA* (n 40).
[47] Kennedy (n 36) 326.

nonconformity within a "reasonable time" after discovering the defect.[48] Failure to do so results in the buyer losing the right to claim nonconformity and may lead to an obligation to pay the purchase price with interest.[49] Like Article 38, which requires buyers to examine goods within a "short period,"[50] the definition of "reasonable time" in CISG Article 39[51] is ambiguous, and determining what constitutes too late for providing notice is contentious

The notice requirement of CISG is viewed by some as a heavy burden placed on the buyer,[52] whereas others, especially German practitioners view it as a buyer friendly provision.[53] However, the question of how this may affect SME buyers has not been previously assessed. Kennedy views the notice requirement as a heavy burden placed on buyers.[54] If the seller intentionally delivers nonconforming goods to the buyer, he is precluded from benefiting from the notice requirement.[55] Therefore, Schwenzer and Hachem are of the view that both criticisms cancel each other out, suggesting that the CISG achieves reasonable results for both parties.[56] However, this debate results in a stalemate situation. Despite the heavy criticism placed on CISG's notice requirement, academics such as Treitel criticise English law for not incorporating a similar provision because he views the lack of notice as giving an opportunity for buyers to terminate the contract based on trivial nonconformities whilst opportunistically benefiting from the easy termination afforded by the English law regime.[57]

---

[48] CISG art 39.
[49] *Ibid*.
[50] *Ibid* art 38.
[51] *Ibid* art 39.
[52] Kennedy (n 36) 323.
[53] Schwenzer and Hachem (n 24) 476.
[54] Kennedy (n 36) 323.
[55] Schwenzer and Hachem (n 24) 473.
[56] *Ibid*.
[57] G H Treitel and Edwin Peel, *Treitel on Law of Contract* (13th edn, Sweet & Maxwell 2011) 257.

In *Chicago Prime Packers v Northam Food Trading*, the United States District court addressed the issue of what constitutes a "reasonable time" under Article 39 of the CISG for providing notice of nonconformity.[58] The court emphasized that determining reasonable time is a factual matter, requiring consideration of various factors like customs and past practices. Since neither party provided sufficient evidence to clarify what "reasonable time" meant in this case, the court dismissed the motions for summary judgment, highlighting the importance of these factors in determining the appropriate timeframe.

In contrast, in a *LG München*, 10 HK 2375/94 (Germany),[59] the court ruled that a buyer's delay of twenty days in appointing an expert was unreasonable, even though the buyer may have needed additional time to assess the goods. This decision illustrates a stricter approach to interpreting the "reasonable time" requirement, focusing on the timeliness of notice without considering the buyer's need for additional time to evaluate the nonconformity. This judgment did not adequately consider the practical challenges faced by the buyer, such as the need to defrost the goods and find an expert during the busy Christmas period.

The court's strict interpretation of "timely notice" left little room for flexibility based on the circumstances, which could be particularly detrimental to SME buyers. These businesses may not fully understand the technicalities of notice requirements under CISG, putting them at a disadvantage if they are held to strict time limits that do not account for the complexities of the goods or market conditions.

This issue highlights the different ways courts interpret the concept of "reasonable time" for inspection and notice under the CISG. Some jurisdictions apply a strict approach, where any delay beyond a few days is considered

---

[58] *Chicago Prime Packers Inc v Northam Food Trading Co* 408 F 3d 894 (7th Cir 2005).
[59] *LG München*, 10 HK 2375/94 (20 March 1995, Germany).

unreasonable, while others adopt a more lenient view.[60] In *Caiato*, the court ruled that a notice given one-month after discovering defects was reasonable, acknowledging the practical realities involved in inspecting goods like cheese.

If the judges in *Caiato* had decided the German case, they may have ruled in favour of the buyer, as they were willing to allow up to a month for the discovery of defects in a perishable good. This highlights the inconsistency across jurisdictions in interpreting what constitutes a "reasonable time" under Article 39,[61] and the potential disadvantage to buyers, particularly small businesses, in jurisdictions with a more rigid approach.

The key protective mechanism for buyers under the CISG is the requirement to provide effective notice of nonconformity. As demonstrated in previous analyses, the interpretation of Articles 38[62] and 39 of the CISG[63] varies significantly across different jurisdictions and individual judges. If a buyer fails to provide an adequate notice, they lose critical rights, such as the right to claim damages,[64] request performance of the contract,[65] demand avoidance,[66] and seek a reduction in the purchase price.[67] Additionally, Article 39(2) limits the time a buyer can raise the issue of nonconformity to two years from receiving the goods, though it allows courts to extend this period based on specific circumstances.[68]

This variability in the interpretation of CISG provisions creates uncertainty for buyers, as the drafters intentionally designed flexible language to accommodate different legal systems while allowing them to maintain their

---

[60] *Roger Caiato* (n 45).
[61] *Ibid*.
[62] CISG art 38.
[63] *Ibid* art 39.
[64] *Ibid* art 74.
[65] *Ibid* art 46.
[66] *Ibid* art 49.
[67] *Ibid* art 50.
[68] *Ibid* art 39(2).

sovereignty. In this context, whether the CISG adequately protects buyers depends on the courts' approach to interpreting these provisions.

The situation is further complicated by the significant burden placed on the buyer regarding the content of the notice. Article 39 only requires the notice to specify the nature of the defect, but it offers no clear guidance on the specifics of what should be included.[69] While large corporations or multinational buyers with access to legal expertise can navigate this, SME buyers may struggle with just the CISG text, potentially leading to misunderstandings. In the *Namur v Wesco* case, a buyer of cotton fabrics lost the right to rely on nonconformity because their notice simply mentioned "bad quality" without detailing the nature of the defect, which the court deemed insufficient.[70] This highlights the challenges faced by buyers, especially SMEs in complying with CISG requirements.

As highlighted, even if a buyer provides timely notice, courts may still require more detailed information about the defect than what the buyer might reasonably expect. This is especially challenging for buyers who do not have professional legal advice and may assume that a simple description, such as "bad quality," would suffice. In contrast, courts, as seen in the German case, expect more specific details like the type of goods, delivery date, and serial number, which adds complexity to the notice process.[71]

The drafters of the CISG did not intend to impose such a heavy burden on buyers, as evidenced by a commentary stating that buyers are not expected to

---

[69] *Ibid* art 39.

[70] *Namur Kredietverzekering v Wesco* (Rechtbank van Koophandel Kortrijk (Belgium), 16 December 1996, No 8336). (*Namur v Wesco*).

[71] *Landgericht Stuttgart*, 3 KfH O 97/89 (31 August 1989, Germany). (*Landgericht Stuttgart*).

conduct exhaustive inspections that would uncover every possible defect.[72] However, courts have often interpreted the notice requirement more strictly, leaving buyers with less protection than the convention might have intended. To address this, scholars like Honnold suggest that courts should consider various factors when determining the reasonableness of the notice, including the nature of the goods, whether independent inspection is required, the seller's ability to cure the defect, the ease of examining the goods, and the remedy the buyer is seeking.[73]

While the CISG provides mechanisms to protect buyers, the practical application of these provisions, especially concerning timely and adequate notice, depends heavily on jurisdiction and judicial interpretation. This inconsistency can place an undue burden on buyers, particularly small businesses, who may struggle to meet the strict notice requirements set by courts.

In *Sport D'Hiver v Ets. Louys et Fils*, the court ruled that the buyer's 23-day delay in notifying the seller of the defect was unreasonable, given the defect was easily discoverable (wrong sizes).[74] However, in *Caiato v Societe Francaise*, the court allowed a one-month delay to identify the defect in perished cheese, despite both cases involving easily noticeable issues.[75] These contrasting rulings show that interpretations of CISG provisions can vary significantly, making it unpredictable for both parties. Some courts use an equitable approach, considering various factors, while others strictly adhere to formal interpretations.

---

[72] CISG Advisory Council 'Examination of the Goods and Notice of Nonconformity Articles 38 and 39' (Opinion No 2, 7 June 2004) < https://cisgac.com/opinions/cisgac-opinion-no-2/> accessed 17 June 2026.

[73] John O Honnold, *Uniform Law for International Sales under the 1980 United Nations Convention* (Kluwer Law International) <https://iicl.law.pace.edu/sites/default/files/cisg_files/honnold.html> accessed 1 March 2026.

[74] *Sport d'Hiver di Geneviève Culet v Ets Louys et Fils* (Tribunale Civile di Cuneo (Italy), 31 January 1996) No 45/96).

[75] *Roger Caiato* (n 45).

In general, the above suggests that CISG Articles 38 and 39 both protect and disadvantage SME buyers, but the overall effect tends to be riskier for SMEs than for large commercial buyers. On the protective side, the CISG provides flexibility by allowing courts to consider the nature of the goods and commercial circumstances when determining what constitutes a "short period" for inspection or a "reasonable time" for notice. Cases such as the Belgian decisions[76] show a buyer-friendly, pragmatic approach, which can benefit SMEs dealing with complex or technical goods.

However, the provisions can also disadvantage SME buyers. The ambiguity of terms like "short period" and "reasonable time" creates legal uncertainty. SMEs often lack resources, making it easier for them to lose their right to remedies due to procedural technicalities rather than substantive defects in goods. The notice requirements can also be particularly burdensome for SMEs. Courts sometimes demand detailed technical descriptions of defects, which may be difficult for small businesses without legal or technical support. As shown in the German cases,[77] strict interpretations can bar claims even where buyers acted in good faith but failed to meet strict formal standards.

Overall, while the CISG aims to balance interests, its practical application can create disproportionate risks for SME buyers compared to large commercial buyers, particularly in jurisdictions that adopt strict interpretations.

It must be highlighted that Articles 38 and 39 promote efficiency by requiring prompt inspection and notice. However, this trade-off operates differently across market participants. Large commercial buyers are well equipped to comply with these requirements, whereas SME buyers are more likely to lose their rights due to procedural non-compliance.

---

[76] *Namur v Wesco* (n 70).
[77] *Landgericht Stuttgart* (n 71).

3.4 Balancing Remedies or Shifting Risk? The CISG from an SME Perspective

CISG offers a range of remedies to buyers, with specific performance being the most prominent.[78] This remedy is based on the idea that sellers should be compelled to fulfil their contractual obligations. Zahraa and Ghith's article highlights how UNCITRAL and scholars support specific performance, emphasizing its benefits like holding the seller accountable, easing the buyer's search for similar goods, and reducing litigation costs.[79] However, there is an opposing view that specific performance can be burdensome to the buyer, as it may be as costly and time-consuming as litigation itself.[80]

In *Styles v Movie Star*[81], the buyer paid for a vintage car, but the seller refused to deliver it. Despite the contract being governed by the CISG, the court considered Florida law to determine the appropriate remedy. The court ultimately granted specific performance under both CISG and Florida law. While specific performance is discretionary under Florida law, it is considered a primary remedy under the CISG. Although Articles 46 and 62 of the CISG formally recognise specific performance as a primary remedy, this principle is qualified by Article 28. Article 28 provides that a court is not bound to order specific performance unless it would do so under its own domestic law in respect of similar sales contracts. Consequently, the practical availability of specific performance under the CISG depends largely on the law of the forum. Therefore, the case demonstrates that specific performance under the CISG is not an

[78] CISG art 46.

[79] M Zahraa and A Ghith 'Specific Performance in the Light of CISG, the UNIDROIT Principles and Libyan Law' (2002) 7(3) *Uniform Law Review* 753.

[80] Pontian Okoli 'A Case for Reviewing the System of Remedies under CISG' (2011) 22(6) *International Company and Commercial Law Review* 245.

[81] *Styles v Movie Star Musclecars Inc* 2017 Fla Cir LEXIS 9983 (Fla Cir Ct 2017).

absolute buyer remedy but one whose effectiveness depends upon the extent to which domestic law recognises and enforces it.

This shows that CISG does not automatically enforce specific performance without regard for the buyer's interests. Instead, the combination of CISG and local law provides a balanced approach to determining the most suitable remedy, a point that is often overlooked in scholarly analysis of the interaction between Articles 28 and 46 of the CISG.

This case supports the use of specific performance, particularly because of the unique nature of the antique car. Enforcing the seller's obligations helped the buyer avoid the impossible task of finding a similar vintage car, thereby safeguarding the buyer's rights. The judgment in *Styles v Movie Star*[82] may benefit SME buyers because it reinforces the strength of specific performance as a remedy under the CISG.

For SME buyers, this is particularly significant. Small businesses often lack market access to easily replace unique or scarce goods. In *Styles v Movie Star*, the vintage car was a unique item.[83] By granting specific performance, the court ensured that the buyer was not left with mere damage, which may be inadequate where substitute goods are unavailable or prohibitively expensive. Instead, the seller was compelled to deliver the exact goods contracted for.

In *Magellan v Salzgitter*, the court ruled that a buyer's request for specific performance could only be granted if the buyer proved it was difficult to obtain similar goods on the market.[84] Okoli examining the viability of CISG remedies commented negatively of all CISG remedies in the standpoint of buyers.[85] He specifically levels criticism against Article 47 of CISG, under which a seller who

---

[82] *Ibid*.
[83] *Ibid.*
[84] *Magellan International v Salzgitter Handel GmbH* 76 F Supp 2d 919 (ND Ill 1999).
[85] Okoli (n 80).

doesn't execute his obligations within the timeframe can be given additional time to the detriment of the buyer. According to Torsello, seller is prohibited from using this provision for his fragmented performance,[86] but Okoli cite Article 51(1) to prove the ability of a partially performing seller to benefit from this Article.[87] Schwenzer and Fantoulakis are critical of s51(1) for providing the possibility to separate delivered goods into parts.[88] Under English law, if the seller fails to perform his side within the agreed period, nothing in this world could prevent him from being punished for his fault. Formulating confidence among sellers to extend the period of performance will create uncertainty amongst buyers to the extent of jeopardizing their smooth trade.

This position negatively affects SME buyers more than large commercial buyers because small enterprises usually depend on timely performance for maintaining cash flow and operational stability. Under CISG Article 47, allowing sellers to request additional time to perform their obligations may place small buyers in a vulnerable position, as they often lack the financial reserves to tolerate delayed deliveries. Okoli's reliance on Article 51(1), which allows partial performance to be treated separately, may further weaken buyer protection by enabling sellers to deliver goods in stages, prolonging contractual uncertainty.[89] While larger commercial buyers may have greater capacity to manage delayed or fragmented performance, small businesses are more likely to suffer

[86] Marco Torsello 'Sales Law Beyond Sales Contracts: Applicability and Applications of the CISG to Non-Sales Transactions (The Case of Countertrade and Barter Transactions)' (2019–20) 38 *Journal of Law and Commerce* 286.

[87] Okoli (n 80).

[88] Ingeborg Schwenzer and Christiana Fountoulakis, *International Sales Law: A Guide to the CISG* (Hart Publishing 2014) <https://dokumen.pub/international-sales-law-a-guide-to-the-cisg-9781509919628-9781509919659-9781509919635.html> accessed 1 March 2026.

[89] Okoli (n 80).

operational disruption and increased transaction costs when seeking remedies for non-performance.

Schwenzer negatively comments on CISG provisions for allowing the seller an ability to remedy his breach within a reasonable time without causing unreasonable inconvenience to buyer.[90] The term "unreasonableness" has no clear definition. Same can be said about the concept of "fundamental breach". Peacock denominates the recourse to fundamental breach as the most controversial remedy of CISG.[91] Treitel condemned CISG terms for being indeterminate and imprecise.[92] The existing literature cites terms such as "fundamental breach", "good faith", "reasonableness" as such vague terms which makes CISG unsuitable for contracts, especially commodity transactions.[93]

Aforesaid vague terms used in CISG are not present in Sale of Goods Act 1979, which could be a reason why Aldershot and Ashgate[94] mention the disuse of CISG concepts of fundamental breach and good faith in English law as a reason for its certainty. Schlechtriem commented positively on CISG Article 49 for facilitating the buyer with an option to choose between avoidance or specific performance when seller's non delivery constituted a fundamental breach of contract,[95] however, Okoli denominate the cooperation of Article 47 and 49(1)(b) as creating a helpless buyer who is coerced to hold-up till seller make good his fault.[96] Though Schlechtriem and Okoli bear opposing views about Article 49,

---

[90] Peter Schlechtriem and Ingeborg H Schwenzer (eds.), *Commentary on the UN Convention on the International Sale of Goods (CISG*) (4th edn, Oxford University Press 2010) 56.

[91] Darren Peacock 'Avoidance and the Notion of Fundamental Breach under the CISG' (2003) 8 *International Trade and Business Law Review* 95, 106 <https://cisg-online.org/files/commentFiles/Peacock_8_ITBLA_2003_95.pdf> accessed 1 March 2026.

[92] Treitel (n 57).

[93] Schwenzer and Hachem (n 24).

[94] John M Rojers, 'International Law and the United States Law' (1999) 93(3) *American Journal of International law* 531.

[95] Schlechtriem and Schwenzer (n 90).

[96] Okoli (n 80).

both perceive Article 47 as negative towards buyers, especially within fluctuating markets. Contrary to what Schlechtriem remarks, practically Article 49 do not give the buyer discretion to select the desired remedies, because if the avoidance amount to fundamental breach, buyer will not only suffer from sellers' nonconformity but will be guilty of breach of contract.

The language used in CISG can be viewed critically, but Zahraa commenting on the specific enforceability of English law governed international contracts, accused the test used to determine the "enforceability" for being vague.[97] Thus, both CISG and English law is tainted with language issues. Effort made by academics to bring precision to these terms often ended with a list of conditions which is far from a solution. SME buyers are less able to manage legal and commercial uncertainty. The vague terminology in the CISG, such as "unreasonableness", "fundamental breach" and "good faith", creates unpredictability in determining when buyers can successfully claim remedies or terminate contracts. Small businesses typically lack legal teams to interpret and litigate ambiguous legal standards, making them more vulnerable when disputes arise.

Additionally, provisions allowing sellers to remedy breaches within a reasonable time may specifically disadvantage SME buyers who rely on strict delivery schedules for inventory management. Larger commercial buyers are usually better equipped to absorb delays and negotiate contractual protections, whereas SME buyers may suffer.

Okoli criticizes the CISG remedy of price reduction, which allows a buyer to accept defective goods in exchange for a reduced price.[98] He argues that this

[97] Mahdi Zahraa and Aburima Abdullah Ghith 'Specific Performance under the Vienna Sales Convention, English Law and Libyan Law' (2000) 15 *Arab Law Quarterly* 304.
[98] Okoli (n 80).

remedy is unfavourable to the buyer because it assumes the buyer will still find the goods useful. This perspective is supported by a Belgian case in which a buyer of tomatoes refused to pay, claiming the tomatoes were too ripe for resale.[99] The court declared the tomatoes fit for resale and confined the buyer to the price reduction remedy, despite the tomatoes being unusable for the buyer's purpose. Okoli argues that this judgment overlooks commercial and practical realities, as the perishable nature of tomatoes meant the buyer was forced to pay at least a partial amount for goods that were already spoiled.[100] The criticism directed at the CISG's price reduction remedy (Article 50 of CISG) has significant implications for SME buyers.

Price reduction allows a buyer to retain non-conforming goods and reduce the price proportionately. In theory, this is a flexible and efficient remedy. However, as Okoli argues, it assumes that the buyer can still derive some commercial value from the defective goods.[101] This assumption can disadvantage SME buyers.

The Belgian tomato case illustrates the problem.[102] The buyer argued that the tomatoes were too ripe for resale, but the court found them objectively fit for resale and limited the buyer to price reduction. From a strict legal perspective, the goods retained some value. However, commercially, perishable goods lose value rapidly. For a small or medium-sized enterprise, particularly one operating on thin margins, the inability to resell the goods immediately may mean total loss, even if the goods are technically "usable."

---

[99] *Rechtbank van Koophandel Mechelen* (18 January 2002) (Belgium).
[100] Okoli (n 80).
[101] *Ibid.*
[102] *Rechtbank van Koophandel Mechelen* (n 99).

Okoli further criticizes the CISG remedy that forces the buyer to give the seller additional time to fulfil their contractual obligations.[103] He argues that this puts the buyer in a vulnerable position, as they are left waiting without certainty, while the seller attempts to remedy the breach. This remedy can be problematic for the buyer, as there is no guarantee of success in the seller's efforts to fix the issue. Okoli sees this as an unfair burden on the buyer, who may end up in a prolonged situation with no assurance of a satisfactory resolution.[104] This can be particularly harmful to SME buyers because it leaves them in a state of uncertainty while the seller attempts to cure the breach. During this extended period, the buyer remains bound by the contract and may be unable to secure alternative goods, even though there is no guarantee that the seller will successfully perform. For SMEs operating with tight delivery schedules, such delays can result in lost commercial opportunities. Consequently, the mechanism may shift disproportionate risk onto SME buyers, who are less able to absorb prolonged uncertainty.

In a German case[105] involving a buyer of women's shoes, the buyer sought to avoid the contract due to delayed delivery and nonconformity of goods. The court ruled that the buyer must give the seller additional time to perform under Article 47 of the CISG. The court ordered the seller to pay the balance and interest. This judgment can be deemed reasonable because the short delay (two days) was negligible, and fixing an additional time for performance allowed the buyer to receive what was contracted for without significant loss.

In non-perishable goods cases, granting additional time helps both parties avoid costly litigation and provides a legal compromise, making the contract

---

[103] *Ibid.*
[104] *Ibid.*
[105] *Oberlandesgericht Frankfurt am Main*, 5 U 15/93 (18 January 1994, Germany).

workable. While Okoli's concerns about the remedy are valid, in practice, if the seller fails to perform during the extended period, the buyer can still claim damages based on the difference in price between the contract and market value at the time of avoidance.[106] Thus, the additional time does not harm the buyer's rights materially. SME buyers are more harmed because they typically operate with narrower profit margins and less diversified supply chains than larger commercial buyers. Prolonged uncertainty during the additional performance period can disrupt operations and damage customer relationships.

The CISG limits the remedy of avoidance to cases of fundamental breach,[107] but as noted earlier, the term "fundamental breach" remains undefined, leading to ambiguity in determining when it applies. Okoli argues that a breach is not fundamental if the violation is remediable.[108] Case law supports this view, indicating that if the buyer can resell the goods at a lower price[109] or use them reasonably,[110] it would not be considered a fundamental breach.

Okoli criticizes the strict interpretation of "fundamental breach" in the CISG, viewing it as an unnecessary burden on buyers.[111] He argues that this approach makes contract termination almost impossible, particularly since reselling defective goods, even at a discount, is always a possibility.[112] Okoli believes that the unsettled nature of what constitutes a fundamental breach further complicates the situation for buyers.[113] The restriction of avoidance to

---

[106] CISG art 74.
[107] *Ibid* art 25.
[108] Okoli (n 80).
[109] *Cobalt Sulphate* (Bundesgerichtshof, 3 April 1996, Germany) (*Cobalt Sulphate*).
[110] *Rotorex Corp v Delchi Carrier SpA* 71 F3d 1024 (2d Cir 1995).
[111] Okoli (n 80).
[112] *Ibid*.
[113] *Ibid.*

cases of "fundamental breach" under Article 25 of the CISG can significantly disadvantage SME buyers.

Because "fundamental breach" is narrowly interpreted and often excludes remediable breaches, SME buyers may be unable to terminate the contract even when the goods are commercially unsatisfactory. If a court finds that the goods can still be resold at a discount or put to some reasonable use, avoidance will likely be denied. For a small business , being forced to resell defective goods at a reduced price may eliminate profit entirely or even cause loss.

The ambiguity surrounding what constitutes a fundamental breach further increases legal uncertainty. SMEs generally lack the financial resources to engage in prolonged litigation to clarify their rights. As a result, they may feel compelled to accept defective performance rather than risk costly disputes. In practice, the strict threshold for avoidance may shift commercial risk onto SME buyers.

In *Lamina System v Coelin*, a Spanish buyer successfully sued for breach of contract when an industrial machine failed to function as specified in the agreement.[114] The court found this failure to be a fundamental breach, even though the buyer had the option to resell the machine. This contrasts with the *Cobalt Sulphate* case, which Okoli criticizes, where the court ruled that the buyer could not terminate the contract because they could resell the goods at a discount, thus preventing the breach from being considered fundamental.[115]

Okoli argues that forcing buyers to maintain business relations with a breaching seller is the consequence of the strict interpretation of "fundamental breach".[116] The analysis indicates that while the CISG generally aims to provide

---

[114] *Lamina System AB v Coelian Asesoramiento SA* (Audiencia Provincial de Madrid (Spain), 22 March 2007) No 244/2007).

[115] *Cobalt Sulphate* (n 109).

[116] Okoli (n 80).

equitable remedies for both parties in international sales agreements, its provisions, such as those concerning the duration to examine goods and notice requirements, are sometimes interpreted in ways that bring justice, but in other instances, result in manifest injustice to the buyer. There is no inherent flaw within the CISG text itself, as it offers comprehensive rules to address issues in international sales. However, the uncertainty surrounding the interpretation of its provisions remains a significant concern that needs to be addressed.

Some academics argue that the CISG's rules on nonconformity and remedies favour the seller, though the real issue may be the individual judge's approach to interpreting the contract.[117] Sastry attributes the detest of the CISG to its ambiguities,[118] while these gaps were intentionally included by the drafters to allow judges to make more equitable decisions while respecting state sovereignty.

Where courts adopt a broader approach, as in *Lamina System v Coelin*,[119] SME buyers benefit because they can terminate the contract when goods fail to perform their essential purpose. For a small enterprise that purchases an industrial machine central to its operations, non-functioning equipment may halt production entirely. Termination allows the SME to seek an alternative supplier quickly and avoid ongoing operational losses. However, under the stricter approach reflected in the *Cobalt Sulphate* decision,[120] if the goods can technically be resold at a discount, the breach may not be considered fundamental. This disproportionately harms SME buyers. Being forced to resell defective goods at a reduced price may wipe out their profit margin or create cash-flow instability.

---

[117] *Ibid*.

[118] D R V VL N Sastry, *English Sales Law v Vienna Convention on CISG* (1st edn, Blue Diamond Publishing 2020) 23.

[119] *Lamina System v Coelin* (n 114).

[120] *Cobalt Sulphate* (n 109).

Additionally, being compelled to maintain business relations with a breaching seller may expose SMEs to further risks, whereas large corporations are better equipped to renegotiate terms, or litigate.

The broader issue of interpretative uncertainty also impacts SMEs more severely. Large commercial entities can manage legal ambiguity through in-house counsel and risk allocation strategies. Thus, inconsistent case law on "fundamental breach" creates a heavier burden on SME buyers than on well-resourced commercial actors. Because outcomes depend heavily on individual judicial interpretation rather than clear, predictable standards, SMEs face greater legal uncertainty. SMEs could be more vulnerable since they often rely on the CISG as a default system because negotiating detailed contracts require in-house legal support which they may lack. The CISG is supposed to help SMEs by providing a uniform set of rules and reducing the need to understand foreign laws. However, challenges arise when interpretations given to CISG provisions conflict.

4 SME Buyers in International Sales: CISG versus English Law

With the rise of online shopping, the risk of encountering abusive sellers and nonconforming products has significantly increased. Long before the said types of e-commerce related problems, English law has introduced several buyer protection mechanisms that address issues such as receiving damaged goods, undelivered orders, and data theft. These protections are vital in fostering a safe and secure trading environment for buyers.

Historically, general buyer protection predated consumer protection. The Sale of Goods Act 1979 offered general protection for all types of buyers including consumers and business buyers, whereas Unfair Contract Terms Act 1977 offered

specific protection to business buyers. The "consumer" is defined as individual purchasing goods for personal use under Section 2(3) of the Consumer Rights Act 2015. The Act was specifically designed to protect consumers. Unfortunately, this focus on consumer protection has often overlooked the needs of SME buyers who purchase goods for resale or other non-consumer purposes, leaving a gap in protection for such buyers.

Long before the Consumer Rights Act 2015, English law introduced the Unfair Contract Terms Act (UCTA) 1977 to safeguard business buyers. The UCTA prevents sellers from exploiting a buyer's lack of expertise by limiting the ability to exclude liability for legal obligations unless the exclusion meets a test of reasonableness.[121] While UCTA offers significant protection to business buyers, it does not extend to international sales of goods contracts, though it still applies to international service contracts.[122]

Accordingly, SME buyers are not granted special protections under English law. The only protections available to such buyers are those embedded in the Sale of Goods Act 1979 and common law, since UCTA 1977 does not apply to international contracts despite offering protection for business buyers. The following analysis will briefly compare the CISG with English law to assess which framework better safeguards the interests of SME buyers.

Regardless of whether the contract is governed by CISG or English law, the rights and obligations of each party can be outlined through express terms. Article 35 of the CISG[123] and the Sale of Goods Act 1979 both impose additional rights and obligations in a contract to protect buyers, allowing them to claim damages for breaches of both express and implied terms. Under both

---

[121] Unfair Contract Terms Act 1977 s 11.

[122] *Trident Turboprop (Dublin) Ltd v First Flight Couriters* [2008] 2 Lloyd's Rep 581. Unfair Contract Terms Act 1977 s 26.

[123] CISG art 35.

frameworks, the seller is required to deliver goods that conform to the contract's specified quantity, quality, and description.[124] In English law, there is an additional requirement that the seller has the right to sell the goods, which is an implied term under the Sale of Goods Act 1979.[125] This right ensures that the buyer is not subject to any legal claims from third parties. While the CISG does not explicitly require the seller to have the right to sell the goods, this requirement is reflected in Article 41 of the CISG, which mandates that the seller delivers goods that are free from any third-party rights or claims.[126] This ensures the buyer is protected from potential legal issues related to ownership and title.

For SME buyers, this clearer and stricter protection under English law is significant as they are less able to absorb the financial consequences of purchasing goods subject to third-party claims (for example, retention of title disputes or intellectual property claims). The explicit statutory guarantee reduces uncertainty and strengthens the buyer's right to immediate remedies, providing greater legal security for SMEs operating with limited risk tolerance.

Under Article 35(2) of the CISG, if the buyer consents to the delivery of non-conforming goods or cannot be unaware of the nonconformity, the seller is exempt from liability for any alleged nonconformities.[127] This provision essentially limits the buyer's ability to claim for nonconformity once they accept the goods, particularly if they were aware of the issue. In contrast, under English law, a buyer loses the right to reject non-conforming goods if they accept them. However, Section 35 of the Sale of Goods Act 1979 still allows the buyer to claim damages even if they negligently accepted nonconforming goods.[128] This

[124] Sale of Goods Act 1979 scts 13 and 14 (SGA).
[125] SGA s 12.
[126] CISG art 41.
[127] CISG art 35(2).
[128] Sale of Goods Act 1979 s 35.

provides buyers with more protection, as English law rewards them with damages even when they fail to notice the nonconformity at the time of acceptance. Article 35(2) of CISG can disproportionately disadvantage SME buyers because it relieves the seller of liability where the buyer knew or could not have been unaware of the nonconformity at the time of contracting. In practice, this may bar SMEs from claiming remedies if they accept goods despite visible defects or fail to identify problems due to limited technical expertise.

Large commercial buyers are generally less affected because they typically have technical capacity to detect defects early. They can also negotiate contractual safeguards. This provision can undermine the protection of the buyer's interests, particularly in situations where the buyer might have acted negligently but was still expected to accept the goods.

In *Oberlandesgericht Köln*, 22 U 4/96 (Germany), the court ruled against the general interpretation of Article 35, deciding that a seller would not be exempt from liability if the buyer should have been aware of the nonconformity.[129] This decision was based on broader principles embedded in Articles 40 and 7 of the CISG, which prioritize the protection of a negligent buyer over a fraudulent seller.[130] Although this ruling worked in favour of the negligent buyer, it remains an exception, as Article 35 explicitly allows judges to disregard the interests of reckless buyers.[131] In essence, while the CISG provides some room for protecting buyers in cases of negligence, it still leans towards protecting sellers in situations where the buyer fails to notice the nonconformity, which can be seen as a disadvantage for all forms of buyers.

---

[129] *Oberlandesgericht Köln*, 22 U 4/96 (21 May 1996, Germany).
[130] CISG arts 7, 40.
[131] *Ibid* art 35.

Under CISG, buyers are obligated to inspect goods upon receipt[132] and provide notice of any nonconformities[133] to trigger remedies. English law, however, does not impose such a notice requirement, meaning buyers are not required to inspect goods or notify the seller to unlock remedies. This places an additional burden on buyers under CISG and appears to benefit the seller by allowing them to remedy defects. In contrast, English law's focus on termination as a primary remedy does not require notice, making it more favourable for buyers, especially those with less experience in legal matters. While the notice under CISG can be beneficial in cases involving unique or scarce goods, it may also be inconvenient in other situations. Therefore, English law's approach to nonconformity, which does not burden the buyer with a notice requirement, offers more practical protection for SME buyers.

Under the notice and inspection requirements of CISG, SMEs may lose remedies if they fail to detect or formally notify defects in a timely manner. SMEs often operate under time pressure and commercial constraints, making strict notice rules riskier for them. English law's approach, therefore, provides SMEs with greater practical protection by allowing them to pursue remedies without risking technical loss of rights due to procedural errors.

Article 38 of the CISG obliges buyers to inspect goods within a short time frame,[134] which can be interpreted strictly in some jurisdictions, limiting the inspection period to just a few days regardless of the goods' nature or complexity. This is especially challenging for more sophisticated goods that may require additional time for proper inspection. Article 39, similarly, imposes tight deadlines for giving notice of nonconformities.[135] Although the CISG only

---

[132] *Ibid* art 38.
[133] *Ibid* art 39.
[134] *Ibid* art 38.
[135] *Ibid* art 39.

requires that the notice specify the defects, courts often demand highly detailed notices, expecting buyers to list every possible defect.[136] This creates an additional burden for buyers, despite CISG commentary suggesting they are not required to mention all foreseeable defects.[137]

The requirement under the CISG for buyers to provide adequate notice of nonconformities within a restrictive time frame and with detailed content puts significant pressure on buyers, especially SMEs. Failing to comply with these requirements can result in the loss of important remedies, including the right to damages.[138] Given these burdens, it is suggested that English law might be a better option for SMEs, as it does not impose similar preconditions to access remedies.

Under English law, the primary remedy for breaching a condition is termination of the contract, regardless of the severity of the breach.[139] Even a minor breach allows for repudiation of the contract, as seen in *Re Moore v Landeur*, where the court allowed termination despite no loss being suffered by the buyer.[140] However, in B2B contracts, a slight breach does not usually justify termination under English law.[141]

In CISG, termination is only permitted for a "fundamental breach", which has led some scholars like Min Yan to argue that English law is more lenient, allowing termination for minor breaches.[142] It should be acknowledged that while

---

[136] *Namur v Wesco* (n 70).
[137] CISG Advisory Council (n 72).
[138] Kennedy (n 36).
[139] P Atiyah, John N Adams and Hector L McQueen, *The Sale of Goods* (11th edn, Pearson Education 2005) 499.
[140] *Re Moore & Co Ltd v Landauer & Co* [1921] 2 KB 519.
[141] SGA 1979 s 15A.
[142] Min Yan 'Remedies under the Convention on Contracts for the International Sale of Goods and the United Kingdom's Sale of Goods Act: A Comparative Examination' (2011) 3(1) *City University Hong Kong Law Review* 109, 114.

there is some overlap between the obligations under CISG and English law, the term "fundamental breach" under CISG is sometimes interpreted liberally by courts, which challenges the strict interpretation of the term as requiring a very serious breach.

With the introduction of section 15A to the Sale of Goods Act (SOGA)[143], cases like *Re Moore v Landeur*[144] would likely be interpreted differently today, as English law now also limits termination for minor breaches. While the uncertainty surrounding the concept of "fundamental breach" in CISG may seem problematic, it can be beneficial in allowing courts to balance the rights of both parties. For example, if a more flexible approach like the one found in the CISG had been applied in *Re Moore v Landeur*[145], the outcome could have been fairer, as termination for a minor breach with no actual loss would be seen as unjust to the seller.

Min Yan argues that the main issue with the concept of "fundamental breach" is its unpredictability, as it is unclear when or if parties will have the right to terminate the contract.[146] English law also does not permit repudiation in B2B sales for slight breaches,[147] so in this regard, the results under both CISG and English law may align depending on how courts interpret the terms. Defining a "fundamental breach" is as difficult as defining a "slight" breach, and courts may determine a term to be a warranty rather than a condition,[148] even if the parties intended otherwise.

---

[143] SGA 1979 s 15A.
[144] *Re Moore* (n 140).
[145] *Ibid.*
[146] Yan (n 142) 117.
[147] SGA s 15A.
[148] *L Schuler AG v Wickman Machine Tool Sales Ltd* [1973] 2 WLR 683.

Thus, the availability of termination as a remedy largely depends on the judge's interpretation, regardless of whether the governing law is CISG or English law. There are cases where courts have interpreted "fundamental breach" in favour of the buyer,[149] and others where they have not,[150] indicating that it is not guaranteed that English law will always provide better protection. In fact, the Secretariat's commentary on the CISG draft emphasized that remedies should be decided based on the specific circumstances, such as monetary harm or the value of the breach, suggesting that the outcome depends more on the facts of the case than the choice of law itself.[151] This could be beneficial to SME buyers because they often lack the legal resources to litigate complex interpretations of breach. Clearer classification of contractual obligations under English law, compared to the "fundamental breach" test under CISG, gives SMEs greater legal certainty.

Under English law, specific performance is a discretionary remedy and can only be granted in limited situations,[152] typically when a party can demonstrate difficulty in obtaining substitute goods.[153] Similarly, Article 28 of the CISG provides that while specific performance is a possible remedy under the convention, the court is not obligated to order it, and domestic law will prevail. This means that, like English law, specific performance under CISG is discretionary. This contradicts the view held by some academics who consider

[149] *Lamina System v Coelian* (n 114).
[150] *Cobalt Sulphate* (n 109).
[151] United Nations Commission on International Trade Law, *United Nations Conference on Contracts for the International Sale of Goods, Vienna, 10 March- 11 April 1908: Official Records* (United Nations 1981) < https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/a-conf-97-19-ocred-eng.pdf> accessed 23 June 2025.
[152] Edwin Peel (ed), *Treitel: The Law of Contracts* (15th edn, Sweet & Maxwell 2020) 843.
[153] *Ibid*.

specific performance to be the primary remedy under the CISG.[154] Honnold argues that Article 28 of CISG allows domestic law to override the provisions in Articles 46 and 62, which typically provide for specific performance.[155]

In both *Styles v Movie Star* (CISG)[156] and *Sky Petroleum v VIP Petroleum*[157] (English law), courts required buyers to prove difficulty in obtaining substitute goods before granting specific performance. Thus, specific performance is considered an exceptional remedy under both systems, available primarily in cases involving unique goods or where hardship in obtaining alternatives exists.

However, buyers cannot predict with certainty whether specific performance will be granted, as it depends on the circumstances of the case. Under the CISG, specific performance is formally recognised as a primary remedy under Articles 46 and 62, although Article 28 significantly qualifies its practical availability by permitting courts to apply domestic restrictions on the remedy. By contrast, English law treats specific performance as an exceptional discretionary remedy, with damages remaining the primary response to breach of contract., other remedies available under the CISG, such as price reduction[158] and the right to cure,[159] are unique to the convention and not found in English law. These remedies provide additional options for buyers that are not typically available in English contract law.

The price reduction remedy has been criticized, because it forces the buyer to pay even a portion of the price for defective goods.[160] This remedy can be

---

[154] A Szakats 'The Influence of Common Law Principles on the Uniform Law on the International Sale of Goods' (1966) 12 *International and Comparative Law Quarterly* 761.
[155] Honnold (n 73).
[156] *Styles* (n 81).
[157] *Sky Petroleum v VIP Petroleum* [1974] 1 WLR 576.
[158] CISG art 50.
[159] CISG art 47.
[160] Okoli (n 80).

unreasonable in cases where the goods are useless to the buyer. Schlechtriem views it as beneficial to the buyer compared to damages.[161] Additionally, Piliounis highlights the challenges a buyer might face when executing this remedy, particularly if the full price has already been paid.[162] The CISG price reduction remedy can be unfavourable to SME buyers in certain situations. Although it allows buyers to reduce the price of non-conforming goods without proving damage, it still requires them to retain and pay for defective goods. As SMEs are particularly affected because they often lack the financial capacity to absorb such losses or repurpose defective goods. As Piliounis notes, difficulties also arise when the full price has already been paid, requiring recovery efforts.[163] While Schlechtriem and Schwenzer view the remedy as procedurally advantageous, it may not provide economically adequate relief for SMEs.[164]

The right to cure, another unique CISG remedy, allows the seller extra time to fulfil their contract.[165] While it may seem biased toward the seller, it can be beneficial if the court allows a reasonable period for the seller to perform without burdening the buyer. The buyer can also claim damages if the seller fails to deliver within this period. This remedy, according to Honnold, should be seen as a tool for cooperation, not a punitive measure.[166] The right to cure under CISG is unique and has no direct counterpart in English law. Initially, it may seem seller friendly as it gives the seller extra time to fulfil the contract if they fail to deliver on time. Critics argue that this is unreasonable, forcing the buyer to give

---

[161] Peter Schlechtriem and Ingeborg Schwenzer (eds), *Commentary on the UN Convention on Contracts for the International Sale of Goods (CISG)* (2nd edn, Oxford University Press 1998) 177.

[162] P Piliounis 'The Remedies of Specific Performance, Price Reduction and Additional Time Under the CISG: Are These Worthwhile Changes or Additions to English Sales Law?' (2000) 12 *Pace International Law Review* 1, 26.

[163] *Ibid.*

[164] Schlechtriem and Schwenzer (n 161).

[165] CISG art 47.

[166] Honnold (n 73).

a breaching seller another opportunity. However, it should be emphasized that under Article 47(1) CISG, the buyer only needs to allow a "reasonable period" for the seller to fulfil their obligations.[167] If this period is interpreted in a way that does not burden the buyer, the remedy becomes beneficial, as it enables the buyer to obtain what they contracted for without resorting to costly litigation. Additionally, if the seller still fails to perform, the buyer can claim damages under Article 47(2).[168]

If judges interpret the additional time for performance under CISG reasonably, considering both parties' interests, this remedy can be a useful tool for amicable settlements, giving sellers a second chance to rectify mistakes. However, due to past interpretations of CISG provisions by courts that have followed a strict formalistic approach, there is a risk that this remedy may unfairly disadvantage buyers. Therefore, the effectiveness of this remedy largely depends on how courts and tribunals apply and interpret it.

The analysis of key provisions in CISG and English law shows that while the CISG aims to be fair to both parties, its provisions tend to favour the seller more than English law does. The use of imprecise and open-textured language in the CISG has led to inconsistent interpretations by courts in different countries. However, as demonstrated by case law, the lack of clarity has led to vastly different interpretations of the same provisions.

Given the inconsistent interpretations of CISG provisions, the only way buyers can protect themselves is by including specific contractual provisions that limit the potential negative impact of CISG's ambiguous terms. However, SME buyers may lack the legal or technical expertise to amend contracts effectively or know how to issue a proper notice to preserve their right to remedies.

---

[167] CISG art 47(1).
[168] CISG art 47(2).

Despite the initial intention of the CISG to support SME owners in international contracts,[169] the uncertainties in its interpretation and the strict notice requirements often create more challenges than benefits for small businesses. As a result, English law is likely a more advantageous choice for business buyers, including SME owners, due to its predictability and the availability of remedies without any preconditions. This makes English law a more accessible and reliable option for businesses of all sizes.

While the CISG offers unique remedies like price reduction and the right to cure, these remedies are tied to a notice requirement, which is often difficult to satisfy. As a result, buyers risk losing both common and novel remedies under the CISG. Additionally, remedies like price reduction are less favourable to buyers, although the right to cure provides a better balance of interests. Given these factors, buyers, especially SMEs should opt for English law, as it provides certainty, predictability, and access to remedies without the stringent preconditions required by the CISG.

Despite offering greater certainty, English law is also not ideal for protecting SME buyers. Compared with the CISG, English law provides predictability but not enhanced protection, as neither regime fully recognises the commercial reality that SME buyers occupy a vulnerable position. Although formally classified as B2B parties, SMEs often lack the legal sophistication of larger commercial entities.

Under English law, SME buyers are not granted any special protective status. Their protection is limited to the implied terms and remedies available under the Sale of Goods Act 1979 and the common law. While the Unfair Contract Terms Act 1977 provides important safeguards for business buyers, its limited

[169] United Nations Commission on International Trade Law (n 151).

application in international commercial contracts significantly reduces its practical value for SME buyers engaged in cross-border trade, where such protection is most needed.

The term "business buyer" should be redefined to differentiate small business owners from larger enterprises. This redefinition would help create specific protections for SME buyers, like consumer protections. While "business buyer" is not clearly defined, UK law categorizes small and medium-sized enterprises (SMEs) based on the number of employees and annual turnover.[170] Businesses with fewer than 250 employees and a turnover under 50 million GBP are classified as SMEs.[171] Using this criterion to redefine business buyers could provide targeted protection for SMEs in international transactions.

The European Commission defines a micro-business as one with fewer than 10 employees and a turnover of less than 2 million Euro.[172] According to BERR statistics, 95% of the 4.4 million SMEs in the UK have fewer than 10 employees.[173] Using this categorization, business buyers could be divided into three groups: micro-business buyers, SMEs, and large business buyers. Since micro-businesses are like consumers due to their small size and lack of access to specialized legal support, it is suggested that the Consumer Rights Act 2015 should be applied to protect their interests. Given that micro-businesses make up most SMEs, safeguarding their interests is crucial.

---

[170] Lee Roberts, 'Bionic's Guide to Business Essentials' (*Bionic*, 21 July 2022) <https://bionic.co.uk/business-finance/guides/what-is-a-small-business/> accessed 1 August 2025.

[171] *Ibid.*

[172] European Commission, *The New SME Definition: User Guide and Model Declaration* (Enterprise and Industry Publications, 2005) <https://www.eusmecentre.org.cn/wp-content/uploads/2022/12/SME-Definition.pdf> accessed 31 July 2025.

[173] Office of Gas and Electricity Markets (Ofgem), *Defining "Micro-businesses"* (2008) <https://www.ofgem.gov.uk/sites/default/files/docs/2008/04/ofgem---defining-micro-businesses-180308.pdf> accessed 7 February 2026.

It is acknowledged that the difficulty in achieving universal agreement on criteria for defining SMEs and business buyers, noting that definitions vary between the European Union and the UK.[174] However, setting official benchmarks could help address this issue. The size of a business impacts various factors like loans and insurance, and similarly, it should influence the level of legal protection available. The solution would be to categorise business buyers into three groups: micro-business buyers, SME buyers, and professional business buyers. It is suggested that micro-business buyers be protected under consumer protection laws due to their similarities with consumers. Additionally, SMEs should have a new statutory mechanism for protecting their interests. However, no specific protection is proposed for larger business buyers, as they typically have access to specialized legal departments.

The most significant practical problem with the CISG is not the absence of remedies but rather the loss of remedies resulting from procedural complexities and interpretative uncertainty. Unlike micro-businesses, SME buyers could not be treated as consumers. However, their limited legal and technical capacity justifies a modified CISG framework. One possible model would retain the existing inspection and notice requirements while allowing courts greater discretion to excuse procedural defects where an SME buyer has acted in good faith but lacks the commercial and legal expertise necessary to navigate the legal complexities and uncertainties. The comparative analysis with English law demonstrates that buyer remedies can be protected without making them excessively dependent on technical procedural requirements. Such a framework would preserve commercial certainty while recognising the intermediate position occupied by SME buyers. Accordingly, the most coherent

[174] Roberts (n 170).

reform would be a three-tier approach: micro-businesses would receive consumer-law protections; SME buyers would benefit from greater procedural flexibility and safeguards against the disproportionate loss of remedies; and large commercial entities would remain subject to the ordinary CISG regime.

Under English law, buyer remedies are not made excessively dependent upon technical procedural requirements. One of the principal difficulties faced by SME buyers under the CISG is the risk of losing substantive remedies because of non-compliance with Articles 38 and 39. While English law does not provide special protection for SME buyers, it generally permits buyers to pursue remedies without first satisfying comparable inspection and notice requirements. This approach offers greater practical protection to smaller businesses that may lack in-house legal expertise. Therefore, future reform of the CISG could retain the notice mechanism while introducing greater flexibility for SME buyers. This will allow courts to excuse minor procedural defects where the buyer has acted in good faith and the seller has suffered no prejudice. Such an approach would reduce the disproportionate burden currently imposed on smaller enterprises.

5 Conclusion

In conclusion, this article has demonstrated that while CISG aspires to strike a neutral and balanced allocation of rights and obligations between buyers and sellers, its practical operation does not sufficiently accommodate the structural vulnerability of SME buyers in international B2B transactions. The Convention's underlying assumption of commercial parity fails to reflect contemporary market realities, where micro and small enterprises increasingly participate in cross-border trade without equivalent legal sophistication, bargaining power, or financial resilience.

The analysis of Articles 35, 38, 39, 47, 49 and 50 reveals that ambiguity, strict notice requirements, and the high threshold for fundamental breach can operate harshly against SMEs. Although the text of the CISG is not inherently biased, inconsistent judicial interpretation and reliance on discretionary standards such as "reasonable time," "fundamental breach," and "unreasonable inconvenience" generate uncertainty that disproportionately burdens smaller businesses. Large commercial actors are better equipped to absorb this uncertainty through legal expertise and risk allocation mechanisms, whereas SMEs face heightened exposure to procedural forfeiture of substantive rights.

The comparison with English law further demonstrates that greater doctrinal certainty does not necessarily translate into adequate protection for SME buyers. Although English law avoids some of the procedural burdens associated with the CISG (particularly the strict inspection and notice requirements), it similarly treats SME buyers as ordinary commercial actors rather than recognising their structural vulnerability. Consequently, the comparative analysis suggests that the central problem is not confined to the CISG. Rather, both international and domestic sales law continue to operate on the assumption that all business parties possess comparable bargaining power, expertise, and resources. The comparison therefore reinforces the argument that SME buyers require distinct legal recognition to reflect contemporary market realities.Ultimately, formal equality within the CISG masks substantive inequality. Recognising SME buyers as a distinct category within international sales law, and adopting interpretive approaches sensitive to commercial vulnerability, would better align the Convention with modern economic realities and promote fairer participation in global trade.

scripted

Volume 23, Issue 01, June 2026

The Thaler Decision in India and the Crisis of Anthropocentric Patent Theory: AI, Inventorship and the Future of Innovation Governance

*Barasha Borthakur**

DOI: 10.2218/scrip.12263

Abstract

This commentary examines the Indian Patent Office's refusal of Stephen Thaler's DABUS patent application as a significant moment in the legal governance of artificial intelligence and innovation. It argues that the decision is doctrinally defensible under the Indian Patents Act, 1970, but theoretically revealing because it exposes the anthropocentric assumptions on which patent law continues to rest. The Controller's reasoning links inventorship to legal personality, entitlement, assignment and proof of right under Sections 6, 7 and 10, concluding that DABUS cannot be a "true and first inventor" because it cannot hold rights, execute legal instruments or transfer title. The commentary situates this reasoning within wider DABUS jurisprudence in various jurisdictions, where AI inventorship has similarly been analysed through statutory interpretation. Yet this convergence does not resolve the deeper question of how patent law should respond to AI-generated or AI-assisted invention. The case comment further places the Indian refusal against India's broader AI policy ambitions, including its promotion of AI-driven innovation and

technological sovereignty. It argues that this produces a regulatory contradiction between developmental AI governance and a human-centred patent framework, making DABUS a transitional case for rethinking inventorship, entitlement and innovation governance.

Keywords
Artificial intelligence, patent law, Indian intellectual property framework, DABUS.

* Lecturer, University of Southampton.

1 Introduction

"What we know for certain is that at some point in the early twenty-first century all of mankind was united in celebration. We marvelled at our own magnificence as we gave birth to AI."[1]

Not many cases in contemporary intellectual property ("IP") law have generated as much theoretical discomfort as The Device for the Autonomous Bootstrapping of Unified Sentience ("DABUS") litigations.[2] The controversy appears deceptively simple. Can an artificial intelligence ("AI") system be recognised as an inventor under patent law?[3] Yet beneath this apparently technical question lies a far more profound challenge to the conceptual architecture of modern legal systems. The DABUS applications compel courts, patent offices and policymakers to confront an uncomfortable possibility: what if invention, long regarded as one of the defining expressions of human ingenuity, is no longer an exclusively human activity?

For more than two centuries, patent law has operated on an assumption so deeply embedded that it rarely required explicit articulation; and innovation was understood as the product of human cognition.[4] The inventor occupied a privileged position within patent jurisprudence because invention itself was viewed as a distinctly human act involving ingenuity and intellectual labour.

---

[1] Morpheus at The Matrix, *The Matrix* (The Wachowskis, Warner Bros 1999).
[2] The details of patent applications across multiple countries are available at https://artificialinventor.com/patent/ (Accessed on 4 June 2026).
[3] *See*, for example, Abbot argues that "more ambitiously, treating computational inventions as patentable and recognizing creative computers as inventors would be consistent with the Constitutional rationale for patent protection. It would encourage innovation under an incentive theory": Ryan Abbott "I Think, Therefore I Invent: Creative Computers and the Future of Patent Law" (2016) 57(4) *Boston College Law Review* 1079-1126, p. 1104.
[4] Cheng Lim Saw and Samuel Zheng Wen Chan, "Of Inventorship and Patent Ownership: Examining the Intersection Between Artificial Intelligence and Patent Law" (2023) 1 *Singapore Journal of Legal Studies* 27-51, pp. 27- 29.

Consequently, patent systems evolved around a relatively stable conceptual framework in which inventorship, ownership, entitlement, rights and obligations were all linked to human agency. The emergence of increasingly sophisticated AI systems destabilises this framework by challenging the premise upon which it rests.[5]

DABUS, developed by Stephen Thaler, has become the leading legal test of AI inventorship.[6] Thaler's litigation campaign sought not merely patent protection but a definitive answer to a fundamental question: if a machine creates an invention, who – or what – is the inventor?[7] The Indian Patent Office's refusal to recognise DABUS as an inventor provides a significant response.[8] Although overshadowed by developments in the UK, USA, Australia, South Africa and many more,[9] the Indian decision warrants independent analysis. As an emerging technological power actively promoting AI, India occupies a distinctive position in the global innovation landscape. Yet when faced with AI inventorship, Indian patent law adopted a traditional approach, maintaining that only human beings can be inventors.

This commentary argues that the Indian DABUS refusal reveals a deeper crisis within contemporary patent theory. The decision is doctrinally correct in the sense that it faithfully interprets the Patents Act 1970.[10] However, it is theoretically inadequate because it exposes the growing inability of patent law to

---

[5] Martin Muller, "Issues in Patenting 'Artificial Intelligence' from an EPO Perspective" (2024) 19(3) *Journal of Intellectual Property Law and Practice* 234-249, p.241.
[6] *See* Artificial Inventor, https://artificialinventor.com (Accessed on 4 June 2026).
[7] *See* Jeffrey Wu, "Bridging the AI Inventorship Gap" (2023) 91(6) *Fordham Law Review* 2515-2547.
[8] In re Patent Application No. 202017019068, Order under Section 15 of the Patents Act, 1970 (Patent Office Apr. 15, 2026), https://www.intepat.com/wp-content/uploads/2026/04/202017019068-Order-Section-15.pdf (Accessed on 4 June 2026).
[9] *See* Artificial Inventor, https://artificialinventor.com (Accessed on 4 June 2026).
[10] Patents Act 1970 (India) (hereinafter Patents Act 1970).

accommodate technological developments that challenge its anthropocentric foundations. The Indian Patent Office successfully defended the existing legal architecture of inventorship, but only by reaffirming assumptions about creativity, agency and legal personality that are becoming increasingly unstable in the age of AI.[11]

This is not to suggest that the recognition of AI-generated inventions as patentable subject matter, or the attribution of inventorship to AI systems, is an uncontroversial or necessarily desirable development. There remains significant debate over whether patent law should move in this direction at all, including concerns about the purpose of the patent system, the risk of over-protection, and the continuing importance of human creativity within the innovation process. Those broader normative questions fall beyond the scope of this case comment, but they must be acknowledged in order to avoid assuming that legal adaptation to AI-generated invention is self-evidently required.

More fundamentally, the DABUS decision should not be understood merely as a dispute concerning statutory interpretation. It is a conflict between two competing visions of innovation. One vision reflects the traditional patent paradigm in which invention is necessarily linked to human creativity and legal personhood. The other reflects an emerging technological reality in which innovation increasingly emerges from complex interactions between humans, algorithms, datasets and autonomous computational systems. The refusal to recognise AI inventorship therefore represents an attempt to preserve the former against the disruptive implications of the latter.

[11] In re Patent Application No. 202017019068 (n 8).

2 The Thaler Decision in India: A Defence of Anthropocentric Patent Theory

2.1 Factual and Procedural Background

The patent application related to a food container.[12] The application was filed in India on 5 May 2020 and originally contained twenty claims.[13]

The application was examined under Sections 12 and 13 of the Patents Act, 1970. A First Examination Report ("FER") was issued on 26 October 2021.[14] The FER raised standard objections, including lack of novelty under Section 2(1)(j), lack of inventive step under Section 2(1)(ja), non-compliance with unity of invention under Section 10(5), and indefiniteness of claims.[15] In addition to these ordinary patentability objections, the FER raised a special objection because the named inventor was DABUS, an AI system. The FER stated that the existing Indian legal framework permitted only natural persons to be recognised as inventors, and therefore naming an AI-based non-human entity as inventor was impermissible under the Act and Rules.[16] In response, the applicant filed a detailed response to the FER on 25 July 2022, accompanied by amended claims.[17]

A hearing under Section 14 was later offered. The hearing notice maintained objections concerning inventive step under Section 2(1)(ja) and objections on inventorship under Sections 6, 7, and 10.[18] The final hearing took

[12] *Ibid.*, para 1.
[13] *Ibid.*
[14] *Ibid.* para 2; see https://iprsearch.ipindia.gov.in/PublicSearch/PublicationSearch/ApplicationStatus enter application no. 202017019068, complete the captcha, then open View Documents at the bottom of the result page (Accessed on 4 June 2026).
[15] In re Patent Application No. 202017019068 (n 8), para 2.
[16] *Ibid.*
[17] *Ibid.*, para 4.
[18] *Ibid.*, para 6.

place on 12 March 2026,[19] attended by the authorised agent, and post-hearing written submissions were filed on 23 March 2026.[20]

2.2 Issues for Determination

Apart from the objection of lack of inventive step under Section 2(1)(ja) (not discussed further here), the issues were:[21]

(1) Whether an AI system, DABUS, could be recognised as a "true and first inventor" under Section 6(1)(a) of the Patents Act, 1970.[22]
(2) Whether the applicant complied with Sections 6, 7, and 10 regarding declaration of inventorship and proof of right.[23]
(3) Whether reliance on a declaration under Patent Cooperation Treaty ("PCT") Rule 4.17(ii) satisfied the requirements of Indian patent law.[24]

These issues show that the Assistant Controller treated the case not merely as a formal defect in naming the inventor, but as a deeper question about

---

[19] *Ibid.*, para 16.
[20] *Ibid.*, para 17.
[21] *Ibid.*, para 18.
[22] Section 6(1)(a) Patents Act 1970: "[A]n application for a patent for an invention may be made by any of the following persons, that is to say,— (a) by any person claiming to be the true and first inventor of the invention".
[23] See in particular Section 7(2) Patents Act 1970 ("Where the application is made by virtue of an assignment of the right to apply for a patent for the invention, there shall be furnished with the application, or within such period as may be prescribed after the filing of the application, proof of the right to make the application"), Section 7(3) ("Every application under this section shall state that the applicant is in possession of the invention and shall name the person claiming to be the true and first inventor; and where the person so claiming is not the applicant or one of the applicants, the application shall contain a declaration that the applicant believes the person so named to be the true and first inventor") and Section 10(6) ("A declaration as to the inventorship of the invention shall, in such cases as may be prescribed, be furnished in the prescribed form").
[24] PCT Rule 4(17)(ii): "The request may, for the purposes of the national law applicable in one or more designated States, contain one or more of the following declarations, worded as prescribed by the Administrative Instructions:... (ii) a declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent...".

entitlement, legal personality, assignment, statutory construction, and the relationship between international PCT procedure and Indian national law.

2.3 Thaler's Submissions

2.3.1 Submissions on Inventorship

Thaler's principal submission was that DABUS had autonomously generated the invention and therefore had to be recognised as the true and first inventor as no natural person qualified as the inventor. This submission appears first in the FER/hearing-notice, where the applicant is recorded as reiterating that DABUS was the "true and first deviser" of the invention.[25]

The applicant further argued that the Indian Patents Act does not expressly restrict inventorship to natural persons.[26] Thaler's position was therefore that, in the absence of an express statutory exclusion of AI inventors, the Act should be interpreted expansively to accommodate technological developments. The submission was essentially purposive and future-oriented: if an AI system in fact generated the invention, then the legal system should not force the applicant to misidentify a human inventor.

Section 2(1)(y) Patents Act was relied upon which defines "true and first inventor" negatively by excluding the first importer of an invention into India or a person to whom an invention is merely communicated from outside India.[27] Thaler argued that because Section 2(1)(y) does not affirmatively state that an inventor must be human, the provision should not be read as excluding non-

[25] *Ibid.,* para 9.
[26] *Ibid.,* para 19.
[27] *Ibid.,* para 20; Patents Act 1970, s 2(1)(y) (""true and first inventor" does not include either the first importer of an invention into India, or a person to whom an invention is first communicated from outside India").

human inventors. Section 2(1)(s) Patents Act was also relied upon which defines "person" to include the Government.[28] Thaler's point appears to have been that because Indian patent law recognises Government as a "person", inventorship should not automatically be confined to human beings.

2.3.2 Submissions on Proof of Right

During oral hearing, the applicant's agent submitted that AI could execute proof of right if required.[29] The applicant also submitted that Thaler was the owner of the DABUS source code, the owner of the computer on which DABUS operated, and the person responsible for the maintenance, operation, and costs of DABUS and its underlying infrastructure.[30] The core of this argument was that Thaler's ownership and control of the AI system should be sufficient to ground entitlement to apply for a patent. In other words, even if DABUS was the actual deviser of the invention, Thaler claimed the right to apply by virtue of ownership, control, operation, and responsibility for the AI system.

2.3.3 Submissions on the Policy Gap for AI-Generated Inventions

Thaler submitted that if AI-generated inventions were denied protection merely because an AI system could not be recognised as inventor, a genuine category of inventions would fall outside the patent system altogether.[31] He also argued that the Indian Patents Act does not define "person" and "true and first inventor" in a way that unequivocally excludes non-human inventors, hence the statutory

---

[28] *Ibid.,* para 21; Patents Act 1970, s 2(1)(s) (""person" includes the Government").
[29] *Ibid.,* para 22.
[30] *Ibid.*
[31] *Ibid.,* para 23.

language left room for interpretive flexibility in light of emerging technological realities.[32]

This submission was important because it framed the case as one involving a legislative gap. Thaler's argument was not simply that the Assistant Controller should stretch the text. Rather, it was that refusing recognition would produce an undesirable and innovation-hostile consequence that the inventions created by autonomous AI systems might become unpatentable despite being technically genuine.

2.3.4 Reliance on PCT Rule 4.17(ii) and Dow AgroSciences

Thaler relied on a declaration filed under PCT Rule 4.17(ii)[33] and also referred to *Dow AgroSciences LLC v Controller of Patents*.[34] The submission appears to have been that PCT-related declarations and previous Indian jurisprudence on proof of right should assist in satisfying the formal entitlement requirements in India.[35]

2.3.5 Reliance on Report No. 161 of the Rajya Sabha Parliamentary Committee

Thaler highlighted that the Report No. 161 of the Rajya Sabha Parliamentary Committee on the Review of the Intellectual Property Rights Regime in India recognised the economic importance of AI and noted that AI-related innovations could contribute significantly to the Indian economy.[36] A portion of the report recommended the creation of a separate category of rights for AI and AI-related

---

[32] *Ibid.*

[33] Patent Cooperation Treaty (adopted 19 June 1970, entered into force 24 January 1978) 1160 UNTS 231, Regulations, r 4.17(ii).

[34] *Dow AgroSciences LLC v Controller of Patents* OA/63/2020/PT/DEL (Intellectual Property Appellate Board, 27 October 2020).

[35] In re Patent Application No. 202017019068 (n 8), para 25.

[36] *Ibid.*, para 25.

inventions and suggested reviewing the Patents Act, 1970 and Copyright Act, 1957 to bring emerging AI technologies within their ambit.[37] Thaler used this report to argue that Indian law should adapt to AI-based inventions and that the Patent Office should interpret the Act in a way that does not exclude such inventions from protection.

2.4 Assistant Controller's Reasoning on AI Inventorship: A Defence of Anthropocentric Patent Theory

2.4.1 Section 6: Only a Legally Recognisable Inventor Can Ground Entitlement

Section 6 of the Patents Act permits a patent application to be made by a person who is the true and first inventor; a person who is the assignee of the true and first inventor; or a person who is the legal representative of a deceased true and first inventor.[38] The Assistant Controller reasoned that because an AI system cannot possess rights, assign rights, or have legal representatives upon death, DABUS cannot fall within any of the categories contemplated by Section 6.[39]

This is one of the most important aspects of the order and the Assistant Controller did not merely say that the word "inventor" ordinarily means a human being. Instead, they looked at the entitlement structure of the Act.[40] If an applicant claims as assignee, there must be an assignor. If an applicant claims as legal representative, the inventor must be capable of death and succession. These statutory mechanisms make sense only where the inventor is a natural person or

[37] *Ibid.,* para 9.
[38] *Ibid.,* para 10.1; Patents Act 1970, s 6.
[39] *Ibid.,* para 19.
[40] *Ibid.*

at least a legally recognised person. DABUS, being neither, cannot be the legal source of patent entitlement.

2.4.2 Section 2(1)(y): "True and First Inventor" Must Be Read Harmoniously

The applicant had argued that Section 2(1)(y) does not expressly restrict inventorship to humans. The Assistant Controller answered that Section 2(1)(y) must be read harmoniously with Sections 6, 7, and 10, and when these provisions are read together, the term "inventor" presupposes a human actor or legally competent person.[41] The requirements of declaration, assignment, legal representation, and proof of right imply legal capacity, which an AI system does not possess.

Thus, they adopted a contextual interpretation. The absence of the phrase "natural person" in Section 2(1)(y) was not enough to include AI systems. The structure of the Act itself supplied the limitation.

2.4.3 Section 2(1)(s): Government as "Person" Does Not Help AI Inventorship

The Assistant Controller rejected the argument that because Section 2(1)(s) includes Government within the definition of "person", non-human inventorship should be accepted.[42] They distinguished the Government as a juristic person capable of owning property, assigning rights, and suing or being sued. AI systems possess none of those legal attributes.[43]

---

[41] *Ibid.,* para 20.
[42] *Ibid.,* para 21; Patents Act 1970, s 2(1)(s).
[43] *Ibid.,* para 21.

Their reasoning is that Indian law recognises non-natural persons only when it expressly does so.[44] Since no statutory extension exists for machines, AI systems, algorithms, or technological constructs, DABUS cannot be treated as a person, inventor, or source of assignable rights.

2.4.4 Natural Person, Legal Capacity, and Juristic Personality

The Assistant Controller gave an extended jurisprudential explanation of why DABUS cannot be treated as a natural person or juristic person and held that the expression "natural person" has a settled legal meaning and refers only to a human being recognised by law as capable of holding rights and duties.[45] A natural person derives legal personality by birth and has inherent capacity to acquire rights, incur obligations, and participate in legal relations.

They then explained that AI systems lack biological existence and therefore cannot be natural persons as they also lack legal capacity: they cannot own property, enter legal relationships, assume responsibility, make enforceable declarations, or be subject to rights and liabilities.[46]

They further referred to Section 3(42) of the General Clauses Act, 1897,[47] which provides that "person" includes any company, association, or body of individuals, whether incorporated or not. The Assistant Controller treated this as extending personhood to legally recognised entities, not to technological systems.[48] Similarly, the Assistant Controller referred to Section 2(26) of the Bharatiya Nyaya Sanhita, 2023,[49] which includes companies, associations, and

---

[44] *Ibid.*
[45] *Ibid.,* para 23.
[46] *Ibid.*
[47] General Clauses Act 1897 (India), s 3(42).
[48] In re Patent Application No. 202017019068 (n 8), para 23.
[49] Bharatiya Nyaya Sanhita 2023 (India), s 2(26).

bodies of persons within the word "person" but does not extend the term to computational entities lacking legal status.[50]

The order also states that artificial or juristic persons exist only because the law recognises them and the corporations, governments, societies, and trusts are treated as persons because legal personality is attributed to them by law.[51] Since no Indian statute attributes legal personality to AI systems, DABUS cannot be treated as a person.

It was also added that persons must be capable of responsibility, intention, and accountability. AI systems operate through algorithmic processes and lack independent volition, intention, or consciousness in the legal sense. They also lack capacity for succession and legal representation. These features confirmed, in the Assistant Controller's view, that DABUS cannot qualify as inventor.[52]

2.5 Assistant Controller's Reasoning on Proof of Right

The Assistant Controller rejected the submission that Thaler's ownership of the DABUS source code and computer was sufficient.[53] Section 7(2) requires proof of right derived from the inventor.[54] Ownership of a machine does not confer entitlement to inventions allegedly generated by that machine unless the assignment originates from a legally recognised inventor.[55] This is a crucial distinction. Property ownership in the AI system is not the same as entitlement to the invention. If DABUS is not a legally recognised inventor, it cannot assign rights. If it cannot assign rights, Thaler cannot establish proof of right by claiming

[50] In re Patent Application No. 202017019068 (n 8), para 23.
[51] *Ibid.*
[52] *Ibid.*
[53] *Ibid.*, para 22
[54] *Ibid.*
[55] *Ibid.*

to be the assignee of DABUS. The Assistant Controller therefore treated ownership, operation, and maintenance of the machine as legally irrelevant to patent entitlement.

The Assistant Controller further rejected reliance on PCT Rule 4.17(ii). The order states that a PCT declaration cannot override Sections 6, 7, and 10 of the Indian Patents Act.[56] Where the designated inventor is not legally recognisable under national law, procedural declarations cannot cure the defect. The Assistant Controller also distinguished *Dow AgroSciences LLC v Controller of Patents*,[57] stating that it was silent on Section 138(4) of the Patents Act.[58] The Assistant Controller referred to an IPAB order, OA/39/2011/PT/CH dated 28 October 2013, for the proposition that formal proof of right by assignment or employment agreement remains mandatory for PCT national phase applications in India.[59]

The point was the reliance on ownership of the machine, PCT declarations, or policy recommendations cannot override the entitlement structure of the Act. Because DABUS lacks legal personality and statutory recognition, the declaration of inventorship and proof-of-right requirements remained unfulfilled.[60]

2.6 Assistant Controller's Reasoning on the Rajya Sabha Parliamentary Committee Report No. 161

The applicant relied on the Rajya Sabha Parliamentary Committee Report No. 161 to show that AI-generated inventions require protection.[61] The Assistant

---

[56] *Ibid.,* para 24.
[57] *Dow AgroSciences LLC v Controller of Patents* OA/63/2020/PT/DEL (Intellectual Property Appellate Board, 27 October 2020).
[58] In re Patent Application No. 202017019068, (n 8), para 24.
[59] *Ibid*.
[60] *Ibid.,* para 26.
[61] Department Related Parliamentary Standing Committee on Commerce, Review of the Intellectual Property Rights Regime in India, Report No 161 (Rajya Sabha Secretariat 2021) https://files.lbr.cloud/public/2021-07/161_2021_7_15.pdf (Accessed on 4 June 2026).

Controller accepted that the report reflected policy concerns and recommendations.[62] However, they held that such recommendations do not alter the statutory position as until Parliament amends the law, inventorship must be determined strictly according to Sections 6, 7, and 10.[63]

This reasoning is significant as the Assistant Controller acknowledged that there may be a policy case for AI-related protection, but separated policy desirability from current legal authority. The order's position is that administrative authorities cannot create a new category of AI inventorship merely because a parliamentary committee recommended legislative review.

2.7 Comparative Jurisprudence Used by the Assistant Controller

The Indian Patent Office did not arrive at its conclusion in isolation. Rather, the DABUS refusal forms part of a broader and still-developing transnational jurisprudence in which most major patent offices and courts have refused to recognise AI systems as inventors, even though a small number of jurisdictions or procedural contexts have produced more permissive outcomes. The dominant trend, however, has been to treat AI inventorship as incompatible with existing patent statutes framed around human legal personality, entitlement and transfer of rights.[64] Although these decisions arise from different statutory frameworks, they reveal a remarkable degree of conceptual convergence. More importantly, they demonstrate a common judicial strategy of avoiding normative questions concerning AI and innovation by framing the dispute as a narrow problem of statutory interpretation.

---

[62] In re Patent Application No. 202017019068 (n 8), para 25.
[63] *Ibid*.
[64] Artificial Inventor, https://artificialinventor.com (Accessed on 4 June 2026).

2.7.1 United Kingdom Supreme Court

The UK Supreme Court decision in *Thaler v Comptroller of Patents*[65] construed Section 7 of the UK Patents Act 1977, which the Assistant Controller considered materially analogous to Section 6 of the Indian Patents Act and mentions that the UK Supreme Court held that an inventor must be a natural person capable of owning and transferring rights and that an AI system cannot qualify as inventor.[66] The Assistant Controller further relies on this UK Supreme Court decision to reject the argument that the absence of an express statutory prohibition implies inclusion.[67] It was stated that the UK Supreme Court rejected an identical argument, holding that where the statutory structure presupposes human inventorship, the absence of express exclusion does not bring AI systems within the statute.[68]

The UK decision is therefore used for two propositions: first, that entitlement provisions based on assignment and succession require a natural person inventor; and secondly, that silence in the statute does not amount to permission to name an AI as inventor.

2.7.2 European Patent Office Board of Appeal

The Assistant Controller notes that the EPO Board of Appeal interpreted Article 81 EPC read with Rule 19 EPC, which require designation of the inventor by name and address.[69] They also noted the EPO decision that those requirements

---

[65] *Thaler v Comptroller-General of Patents, Designs and Trade Marks* [2023] UKSC 49.
[66] In re Patent Application No. 202017019068 (n 8), para 19.
[67] *Ibid.,* para 23.
[68] *Ibid.*
[69] *Ibid.,* para 20.

necessarily imply human inventorship because only a natural person can be identified in the manner contemplated by the statute.[70]

The Assistant Controller treated the EPC provisions as functionally corresponding to Sections 7(3) and 10(6) of the Indian Patents Act.[71] The EPO jurisprudence was therefore used to support the proposition that formal requirements of identifying and declaring the inventor are not empty procedural requirements; they assume the inventor is a legally identifiable human being.

2.7.3 Full Federal Court of Australia

The Assistant Controller refers to the Full Federal Court of Australia in *Commissioner of Patents v Thaler*.[72] The Australian decision is used for the proposition that entitlement provisions analogous to Section 7 of the Indian Act require derivation of rights from a natural person inventor and this supports the Assistant Controller's rejection of Thaler's argument that ownership of DABUS or its computer infrastructure is enough to establish proof of right.[73]

2.7.4 United States, Germany, Japan, Australia, UK, and EPO: General Comparative Consensus

The Assistant Controller also states that courts in the United States, United Kingdom, Germany, Japan, and Australia have uniformly interpreted "natural person" as referring only to human beings in the context of AI inventorship.[74] It was also mentioned that the DABUS applications have been rejected across jurisdictions, including the United Kingdom Supreme Court, United States

[70] *Ibid.*
[71] *Ibid.*
[72] *Commissioner of Patents v Thaler* [2022] FCAFC 62.
[73] In re Patent Application No. 202017019068 n 8), para 22.
[74] *Ibid.,* para 23.

Federal Circuit, German Federal Court of Justice, Japan IP High Court, European Patent Office Board of Appeal, and Full Federal Court of Australia.[75] This comparative jurisprudence is used not as binding authority, but as persuasive confirmation that patent statutes built around inventorship, assignment, legal personality, and entitlement have generally not been interpreted to permit AI inventorship without legislative amendment.

2.7.5 Comparative Jurisprudence as Statutory Support, Not Policy Determination

The Assistant Controller's use of comparative law is conservative and statutory. The order does not use foreign cases to decide whether AI inventorship should be recognised as a matter of innovation policy. Instead, it uses them to confirm that similarly structured patent statutes have been interpreted as requiring human inventors. The comparative authorities strengthen the Assistant Controller's conclusion that the Indian Act cannot be judicially or administratively extended to AI systems in the absence of legislative change.

3 India's AI Ambitions and the Contradictions of Developmental Governance

The limitations of the Indian DABUS refusal become particularly visible when situated within India's broader technological strategy. Over the past decade, India has embraced AI as a central component of economic development and technological competitiveness.[76] Through initiatives such as the National

[75] *Ibid.*, para 25.
[76] Ashok Panigrahi, Shrinivas C Ahirrao and Arav Patel, "Impact of Artificial Intelligence on Indian Economy" (2024) 11(1) *Journal of Management and Research Analysis* 33-44, p. 33.

Strategy for AI,[77] Digital India,[78] the IndiaAI Mission[79] and the National Data Governance Framework,[80] the Indian state has explicitly identified AI as a transformative technology capable of reshaping sectors ranging from healthcare and agriculture to manufacturing and public administration.

This commitment reflects a broader developmental vision. India seeks not merely to consume AI technologies developed elsewhere but to become an active participant in the global AI economy. Government report have emphasised the importance of indigenous innovation, AI-driven entrepreneurship and technological sovereignty.[81] AI is increasingly presented as a strategic resource capable of enhancing economic growth, national competitiveness and geopolitical influence.

Against this backdrop, the DABUS decision reveals a striking contradiction. India's innovation policy assumes that AI will become a significant source of economic value and technological advancement. Yet its patent system continues to operate according to assumptions that innovation originates exclusively from human inventors. This tension may be understood through Mariana Mazzucato's theory of the developmental state where she argues that modern innovation economies depend upon active state participation in shaping

[77] National Strategy for Artificial Intelligence, NITI Aayog, https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf (accessed on 4 June 2026).
[78] Digital India, Ministry of Electronics and Information Technology, https://www.digitalindia.gov.in/ (accessed on 4 June 2026).
[79] IndiaAI Mission, https://indiaai.gov.in/ (accessed on 4 June 2026).
[80] National Data Governance Framework (draft), https://www.thehinducentre.com/resources/67557000-National-Data-Governance-Framework-Policy_compressed.pdf (accessed on 4 June 2026).
[81] 161st Report on the Review of the Intellectual Property Rights Regime, Parliament Standing Committee, Rajya Sabha Secretariat, Government of India, https://files.lbr.cloud/public/2021-07/161_2021_7_15.pdf?VersionId=S01fCQEC5DzDqKNymsGgxal6YXmJbUwM (accessed on 4 June 2026).

technological markets.[82] However, successful innovation governance requires coherence between industrial policy and regulatory institutions where technological ambitions advance more rapidly than legal frameworks, regulatory contradictions emerge.

The DABUS refusal exemplifies such a contradiction. The Indian state actively encourages AI-driven innovation while simultaneously maintaining a patent regime that lacks a coherent response to AI-generated invention. This does not mean that the Indian Patent Office was legally incorrect. Rather, it highlights a broader disconnect between innovation policy and IP policy.

The issue is particularly important because patent systems perform a crucial signalling function within innovation ecosystems. They determine how technological contributions are recognised, rewarded and commercialised. If AI becomes increasingly capable of generating commercially valuable inventions, the continued insistence upon exclusively human inventorship may create uncertainty regarding ownership, disclosure and investment incentives. The DABUS controversy therefore raises questions extending far beyond patent doctrine. It concerns the ability of legal institutions to support the technological ambitions that states themselves actively promote.

Evidence that these tensions are already being recognised within Indian policy circles can be found in the Parliamentary Standing Committee's 161st Report on the Review of the Intellectual Property Rights Regime.[83] Although the Committee did not endorse AI inventorship, it acknowledged the growing significance of AI and emphasised the need to reconsider IP frameworks in light of emerging technologies.

---

[82] Mariana Mazzucato, *The Entrepreneurial State*, (Harlow: England, Penguin Books, 2018).
[83] Department Related Parliamentary Standing Committee on Commerce, Review of the Intellectual Property Rights Regime in India, Report No 161 (Rajya Sabha Secretariat 2021) https://files.lbr.cloud/public/2021-07/161_2021_7_15.pdf (Accessed on 4 June 2026).

The Committee's observations are important because they implicitly recognise that existing IP concepts may prove inadequate for governing AI-generated outputs. While the Indian Patent Office remains bound by the Patents Act 1970, policymakers increasingly appreciate that future technological developments may require legislative adaptation. This divergence between legislative awareness and administrative constraint illustrates a recurring feature of technological regulation. The DABUS refusal therefore represents a transitional moment rather than a definitive resolution. It marks the point at which existing legal categories begin to encounter technological developments they were never designed to accommodate.

4 Beyond DABUS: Rethinking Inventorship in the Age of AI

The ultimate significance of the DABUS litigation lies not in whether Stephen Thaler obtained a patent. Nor does it lie in the relatively narrow question of whether DABUS should be recognised as an inventor. The deeper significance of the case is that it forces patent law to confront assumptions that have long remained unquestioned.

For centuries, patent law has relied upon a relatively stable image of invention. An inventor conceives an idea, applies intellectual effort and receives legal recognition in exchange for public disclosure. This model reflects a world in which invention is inseparable from human cognition. AI challenges this model because it introduces the possibility that invention may no longer require direct human conception. Whether contemporary AI systems have truly reached this point remains contested.

The Indian Patent Office's refusal can therefore be understood as an attempt to defend the anthropocentric foundations of patent law. The decision

preserves the traditional relationship between inventorship, legal personality and entitlement. In doing so, it protects the internal coherence of the patent system. Yet coherence is not the same as adequacy. A legal system may remain internally consistent while becoming increasingly detached from the social and technological realities it seeks to regulate. The history of IP law demonstrates that periods of technological transformation often expose weaknesses within existing legal categories. The printing press transformed copyright. Industrialisation transformed patent law. Digital technologies transformed both.

AI may represent the next such transformation.

scripted

Volume 23, Issue 01, June 2026

From Sampling to Generative AI: The Scope of Pastiche after Pelham II

*Élodie Migliore**

DOI: 10.2218/scrip.12284

Abstract

Exceptions and limitations play a pivotal role in European copyright law and have been the subject of significant developments in the case law of the Court of Justice of the European Union. In this context, the judgment in *Pelham II* (C-590/23) is particularly noteworthy. First, it provides long-awaited clarification of the notion of "pastiche" under Article 5(3)(k) of Directive 2001/29/EC by recognising it as an autonomous concept of EU law and by articulating a structured framework governing its application. Secondly, the ruling may have far-reaching implications for the legal treatment of AI-generated outputs within the European copyright framework. This comment examines the Court's interpretation of pastiche as requiring an artistic or creative dialogue with a pre-existing work that is objectively recognisable, whilst rejecting any requirement of subjective intent on the part of the user. It further analyses the emergence of the "recognisability" criterion in the CJEU's recent case law and considers the broader implications of the judgment for transformative uses, artistic freedom, and the balancing of fundamental rights in EU copyright law. Particular attention is paid to the relevance of *Pelham II* for generative AI. This comment argues that the Court's flexible conception of pastiche may

encompass certain AI-generated outputs, whilst highlighting the continuing importance of the three-step test as a potential limiting principle.

Keywords: European copyright; exception; pastiche; artificial intelligence

* PhD Candidate, Centre d'études internationales de la propriété intellectuelle (CEIPI), Strasbourg, France; **elodiemigliore@gmail.com**.

1 Introduction

In April 2026, the Court of Justice of the European Union (CJEU) delivered its judgement in C-590/23, *Pelham II*[1], thereby bringing to a close almost two decades of litigation in the well-known *Pelham* saga. This long-awaited judgement is significant in several aspects. Firstly, it provides clarification of the concept of "pastiche" as a copyright exception under European law, whilst also offering broader reflections on the possible treatment of AI-generated outputs within the European copyright framework. More importantly, the decision may result in the three-step test emerging as the key limiting principle governing AI-generated outputs following the Court's flexible conception of pastiche.

The dispute stems from the unauthorised use, by the producers of the song "*Nur mir*," released in 1997 and interpreted by Sabrina Setlur, of a musical sample lasting approximately two seconds, reproducing a rhythmic sequence from the 1977 track "*Metall auf Metall*" by the band Kraftwerk.

After lengthy proceedings before the German courts, marked by numerous decisions and reversals since 2004, the CJEU issued its first ruling in 2019 in *Pelham I*[2]. That judgement attracted considerable academic commentary[3]. It notably held that the use of a sound sample, even of a very short duration, constitutes an act of reproduction requiring the authorisation of the phonogram producer where the sample is recognisable[4]. The decision therefore introduced a

---

[1] Case C-590/23 *CG and YN v Pelham GmbH* (Pelham II) ECLI:EU:C:2026:290.

[2] Case C-476/17 *Pelham GmbH v Hütter* (Pelham I) ECLI:EU:C:2019:624.

[3] Bernd Justin Jütte and João Pedro Quintais, 'The Pelham Chronicles: Sampling, Copyright and Fundamental Rights' (2021) 16 Journal of Intellectual Property Law & Practice 213 <https://doi.org/10.1093/jiplp/jpab040> accessed 11 May 2026; Martin Senftleben, 'Flexibility Grave – Partial Reproduction Focus and Closed System Fetishism in CJEU, Pelham' (2020) 51 IIC - International Review of Intellectual Property and Competition Law 751 <https://doi.org/10.1007/s40319-020-00940-z> accessed 11 May 2026.

[4] Pelham I (n 2) para 39.

novel criterion for infringement, namely the 'recognisability' test, according to which infringement will arise only where the protected subject matter remains recognisable within the allegedly infringing work. Although this criterion was initially confined to neighbouring rights in *Pelham I*, it was subsequently reaffirmed by the CJEU in *Mio and Konektra*, this time with regard to copyright[5]. The Court further adopted a restrictive interpretation of the quotation exception, holding that its application presupposes engagement with an identifiable work, thus excluding the form of sampling at issue in the present case. As the quotation exception was therefore deemed inapplicable, the dispute shifted towards the scope and interpretation of the pastiche exception.

In this context, the *Bundesgerichtshof* (Federal Court of Justice) referred, once again, the matter to the CJEU for a preliminary ruling, seeking clarifications on the scope of the pastiche exception provided for under Article 5(3)(k) of Directive 2001/29, the InfoSoc directive[6].

The referring court submitted two questions to the CJEU for a preliminary ruling.

By its first question, the referring court asks, in essence, whether Article 5(3)(k) of Directive 2001/29 must be interpreted as meaning that the exception for "pastiche", within the meaning of that provision, has a catch-all nature which covers, at the very least, any artistic engagement with an existing work, including in the form of sampling, without it being necessary for that engagement to be an expression of humour, a stylistic imitation or a tribute.

---

[5] The "recognisability" test was subsequently reaffirmed by the CJEU in Mio and Konektra, this time in the context of copyright infringement, see Joined cases C-580/23 and C-795/23 *Mio and Konektra* ECLI:EU:C:2025:941.

[6] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L167/10 (InfoSoc Directive).

By its second question, the referring court sought clarification as to whether use "for the purposes" of pastiche requires a finding that the user intended to use a copyright-protected work for the purposes of a pastiche, or is it sufficient that the pastiche character is recognisable to persons familiar with the copyright-protected work to which reference is made and has the requisite intellectual understanding to perceive the pastiche?

This comment argues that *Pelham II* represents a significant step forward in clarifying the scope of the pastiche exception, with potentially far-reaching consequences for the legal treatment of AI-generated outputs under EU copyright law. In particular, it contends that whilst the Court's flexible conception of pastiche may accommodate certain AI outputs, the three-step test is likely to emerge as the principal limiting principle in this context, especially where such outputs risk substituting for original works in existing markets.

2 Pastiche after Pelham II: Towards an Autonomous EU Law Concept

The decision begins by observing that the concept of "pastiche" is not defined in the InfoSoc Directive, and must therefore be regarded as an autonomous concept of EU law[7]. As a consequence, the notion requires a uniform interpretation throughout the European Union.

The Court further notes that pastiche is a rarely used term capable of encompassing a variety of meanings[8]. Certain definitions conceive pastiche as a form of concealed imitation, whereas others require an overt and recognisable

[7] *Pelham I* (n 2) para 34.

[8] On the various meanings attributed to the concept of pastiche, see European Copyright Society, 'Opinion of the European Copyright Society on CG and YN v Pelham GmbH and Others, Case C-590/23 (Pelham II)' (6 November 2024) < https://europeancopyrightsociety.org/wp-content/uploads/2024/11/ecs-opinion-pelham-ii-1.pdf> accessed 11 may 2026.

use of characteristic elements drawn from one or more pre-existing works within a new creation that imitates those works in order to establish an artistic or creative dialogue with them[9].

In order to determine the appropriate interpretation of the exception, the Court must also consider the broader context in which the notion of pastiche operates, together with the objectives pursued by Article 5(3)(k) of Directive 2001/29/EC.

First, the pastiche exception is included alongside caricature and parody within the same provision. Although those concepts share common characteristics, notably the reference to a pre-existing work and the possible presence of humour or mockery, the Court emphasises that they nonetheless remain distinct concepts. The EU legislature intended to recognise three separate categories of use, and the interpretation adopted must preserve the practical effectiveness (*l'effet utile*) of each exception so as to avoid rendering them legally redundant[10].

The Court further clarified that the notion of pastiche cannot extend to disguised reproductions of protected works or to plagiarism. Rather, the concept presupposes an open and recognisable use of protected subject matter as such[11].

Against this background, the CJEU proceeds to define the concept of pastiche. The Court first rejects the proposition that pastiche constitutes a residual or catch-all exception. This notion covers "creations which evoke one or more existing works, while being noticeably different from them, and which uses […] some of those works' characteristic elements protected by copyright"[12].

---

[9] *Pelham I* (n 2) paras 35-37.
[10] *Ibid* paras 40-41.
[11] *Ibid* para 49.
[12] *Ibid* para 58.

Without such differentiation, the exception would be devoid of independent purpose. Moreover, the use must "engage with those works in an artistic or creative dialogue that is recognisable as such"[13].

According to the Court, this dialogue may take various forms, including, in particular, open stylistic imitation, tribute, or humorous or critical engagement with the referenced works[14]. Significantly, the conception of pastiche adopted in *Pelham II* appears broader and more flexible than that previously associated with parody. Humour is no longer treated as a defining element of the exception, but merely as one possible manifestation thereof. Furthermore, the forms that such creative dialogue may assume are not exhaustive, as demonstrated by the Court's use of the expression "in particular"[15]. Within this framework, the Court expressly acknowledges that sampling is, in principle, capable of falling within the scope of the pastiche exception[16].

As noted by A. Guadamuz[17], the decision makes it then possible to derive a structured test for determining whether a use falls within the scope of the pastiche exception, composed of four cumulative elements:

---

[13] *Ibid*.

[14] *Ibid* paras 50- 56. As previously noted, the requirement of engagement or "dialogue" with the referenced work had already been identified by the CJEU in Pelham I as a condition for the application of the quotation exception, see Pelham I (n 2) paras 71-73.

[15] *Ibid* paras 53 and 58.

[16] *Ibid* para 55.

[17] Andres Guadamuz, 'Pastiche or Cliché? What Pelham II Might Mean for AI Outputs' (TechnoLlama) <https://www.technollama.co.uk/pastiche-or-cliche-what-pelham-ii-might-mean-for-ai-outputs> accessed 11 May 2026. The structure of the test created by the judgements is not without recalling the notion of transformative use under the US fair use doctrine. The transformative nature of AI-generated outputs is currently the subject of significant litigation in the United States.

> (1) the evocation of an existing work; (2) a noticeable difference from it; (3) the use of characteristic, copyright-protected elements of that work; and (4) an engagement in an artistic or creative dialogue that is recognisable as such.

More importantly, the Court clarified that it is irrelevant whether the user intended to create a pastiche. What matters instead is whether the pastiche character of the use is recognisable to a person familiar with the original work[18], thereby extending the "recognisability" test developed in the CJEU's recent case law.

3 The "Person Familiar with the Existing Work"

Another noteworthy aspect of the judgment lies in the Court's reliance on the perspective of a "person who is familiar with [the] existing work and who has the requisite intellectual understanding"[19] in order to determine whether a use may qualify as a pastiche.

According to the CJEU, the pastiche character of a work must therefore be recognisable from the standpoint of such a person familiar with the source material from which the protected elements are borrowed. Is EU copyright law witnessing the emergence of its own fictional legal person? Other branches of intellectual property law are already structured around similar normative figures, such as the "person skilled in the art" in patent law, the "average consumer" in trademark law, or the "informed user" in design law. As Eleonora Rosati observes, the Court's formulation may also assist in "elucidating the (puzzling) recognisability standard embraced in Pelham I and, more recently, in

18 *Ibid*.
19 *Pelham I* (n 2) para 62.

Mio/Konektra"[20]. In those decision, the CJEU's relied on recognisability as a criterion for infringement without expressely detailing how this criterion should be assessed. By referring to a "person familiar with the work" in *Pelham II*[21], the Court seems to provide a more concrete criterion for assessing if protected elements are recognisable.

4 The Purpose of the Pastiche Exception and its Balancing Against Other Rights

The decision also addresses the thorny issue of balancing intellectual property rights against competing rights, and especially fundamental rights. In examining the purpose of the pastiche exception, the Court reiterates that Article 5(3)(k) of Directive 2001/29/EC seeks, particularly within the digital environment, to strike a fair balance between, on the one hand, the interests of copyright and related rights holders in the protection of their intellectual property rights and, on the other hand, the protection of the interests and fundamental rights of users of protected works, including freedom of expression and freedom of the arts, guaranteed respectively by Articles 11 and 13 of the Charter of Fundamental Rights of the European Union, as well as the general interest[22].

The Court hence confirmed that the application of the exception requires a balancing exercise between these competing rights and interests. Since the right to intellectual property, protected under Article 17(2) of the Charter, is not absolute, the concept of pastiche must not be interpreted restrictively, but rather

---

[20] Eleonora Rosati, 'CJEU Delivers Pastiche-Style Judgment on … Pastiche' (The IPKat) <https://ipkitten.blogspot.com/2026/04/cjeu-delivers-pastiche-style-judgment.html> accessed 11 May 2026.

[21] *Pelham I* (n 2) para 62.

[22] *Ibid* para 45.

in a manner consistent with the freedoms and objectives underpinning Article 5(3)(k)[23].

5 The Curious Absence of the Three-Step Test

Another distinctive feature of the decision is the absence of any explicit reference to the three-step test.

Article 9(2) of the Berne Convention first introduced the three-step test during the 1967 Stockholm Revision, confining permissible reproductions to certain special cases that neither conflict with the normal exploitation of the work nor unreasonably prejudice the legitimate interests of the author[24]. This formulation was adopted into EU copyright law through Article 5(5) of Directive 2001/29/EC[25], which applies horizontally across the exceptions and limitations provided for under that Directive.

---

[23] *Ibid* para 48. Prior to 2019, the CJEU endorsed a strict interpretation of copyright exceptions and limitations, see for example, Case C-265/16 *VCAST Limited v R.T.I. SpA* ECLI:EU:C:2017:913, para 32. Since then, however, the Court's case law has appeared to adopt a more flexible approach, maintaining the principle of a closed list of exceptions under EU copyright law while interpreting certain exceptions in light of competing fundamental rights and the requirement to ensure their effectiveness, see, in this regard, Case C-469/17 *Funke Medien v Bundesrepublik Deutschland* ECLI:EU:C:2019:623, paras. 69–71 ; Case C-516/17 *Spiegel Online GmbH v Volker Beck* ECLI:EU:C:2019:625, paras. 53–55. On this notion, see also, Elena Izyumenko, 'Op-Ed: "Pelham II and the Notion of Pastiche in EU Copyright Law: Is the Court of Justice Finally Giving Creative Reuse Some Breathing Space?"' (EU Law Live, 16 April 2026) <https://eulawlive.com/op-ed-pelham-ii-and-the-notion-of-pastiche-in-eu-copyright-law-is-the-court-of-justice-finally-giving-creative-reuse-some-breathing-space/> accessed 12 May 2026.

[24] Article 9, paragraph 2, Berne Convention for the Protection of Literary and Artistic Works (adopted 9 September 1886, as amended on September 28, 1979).

[25] On the three step, see Daniel Jongsma, 'The Nature and Content of the Three-Step Test in EU Copyright Law: A Reappraisal' The Routledge Handbook of EU Copyright Law (Eleonora Rosati, Routledge 2021) <https://papers.ssrn.com/abstract=3665934> accessed 9 June 2026; Richard Arnold and Eleonora Rosati, 'Are National Courts the Addressees of the InfoSoc Three-Step Test?' (2015) 10 Journal of Intellectual Property Law & Practice 741 <https://doi.org/10.1093/jiplp/jpv138> accessed 9 June 2026.

Despite this, the Court made no express reference to the three-step test in *Pelham II*. However, some commentators[26] note that by rejecting an interpretation of the pastiche exception that would authorise any form of more or less creative reuse, and by emphasising the requirement of an objective justification for the use at issue, the Court implicitly acknowledged the limits of the concept and, consequently, the boundaries of the resulting defence. The three-step test might also play an important role regarding AI-generated outputs.

6 The Implications of Pelham II for AI-Generated Outputs

Lastly, the judgement is of particular significance in relation to one of the most topical issues in contemporary copyright law, namely the legal treatment of AI-generated outputs. Indeed, where AI-generated outputs incorporate or evoke protected works, one possible defence to infringement under EU law may lie in the application of the pastiche exception. Prior to *Pelham II*, however, the concept of pastiche remained largely undefined, leaving considerable uncertainty as to its scope and practical application.

The test articulated by the Court appears capable of applying to a significant number of outputs generated by generative AI systems. As A. Guadamuz observes, the definition adopted by the Court is sufficiently broad to encompass a substantial proportion of what generative AI systems actually do[27]. Indeed, many generated outputs may evoke pre-existing works while simultaneously presenting perceptible differences from them, incorporating recognisable copyright-protected elements, and engaging in a form of artistic or creative dialogue with the referenced works. Recent examples illustrate this

[26] Rosati (n 20).
[27] Guadamuz (n 17).

phenomenon. For instance, in 2025, OpenAI unveiled an image-generation tool integrated into ChatGPT capable of producing visuals inspired by recognisable artistic universes, including the aesthetic associated with Studio Ghibli. Although copyright law does not protect artistic style as such, users rapidly generated images closely evoking the visual identity of Ghibli's works whilst differing in their specific expression and composition.

Such outputs may therefore satisfy several of the criteria identified by the Court in *Pelham II*, notably the evocation of an existing work, perceptible differentiation, and the existence of a recognisable creative dialogue with the referenced material. These outputs may also incorporate recognisable copyright-protected elements of the referenced works themselves, thereby fulfilling all the conditions of the test, and making reliance on a copyright exception necessary to avoid infringement. Nevertheless, the criteria established by the Court should not be understood as legitimising all forms of AI-generated content. In particular, outputs amounting merely to the reproduction or regurgitation of memorised[28] content would likely remain excluded from the scope of the exception, since such uses would not involve any genuine artistic or creative dialogue, but rather mere copying. Indeed, as noted beforehand, the Court expressly clarified that the notion of pastiche cannot extend to disguised reproductions of protected works or to plagiarism[29].

---

[28] Memorisation is a phenomenon that may occur in foundation models, including large language models. It refers to the ability of a model to memorise portions of its training data and, when appropriately prompted, to reproduce certain of those data verbatim in its outputs. Some authors further argue that where memorisation occurs, the training data are not merely reproduced in the model's outputs, but are also encoded within the model's parameters themselves. See on this issue, Nicholas Carlini and others, 'Quantifying Memorization Across Neural Language Models' (arXiv, 6 March 2023) <https://doi.org/10.48550/arXiv.2202.07646> accessed 9 June 2026; A Cooper and James Grimmelmann, 'The Files Are in the Computer: On Copyright, Memorization, and Generative AI' (2025) 100 Chicago-Kent Law Review 141 <https://scholarship.kentlaw.iit.edu/cklawreview/vol100/iss1/9> accessed 9 June 2026.

[29] *Pelham I* (n 2) para 49.

A further difficulty arises from the interaction between the objective recognisability test established in *Pelham II* and the specific nature of AI-generated outputs. Under the Court's approach, subjective intent is irrelevant; what matters is whether the pastiche character of the use is recognisable to a person familiar with the referenced work. However, the application of this criterion becomes more complex in the context of generative AI. The judgment leaves unresolved the question from whose perspective recognisability should be assessed, and at what stage of the creative process. If the relevant perspective is that of the user prompting the system, doubts may arise as to whether that person possesses sufficient familiarity with the referenced works, particularly where outputs are generated with limited human involvement. Indeed, AI systems are often described through the distinction between the training phase and the output or deployment phase. Although this distinction is technically simplified, it remains useful for understanding the general functioning of generative AI systems. Broadly speaking, the training phase consists in the development of the model by the provider, including the design of the model's architecture, the curation of training datasets, and fine-tuning processes. This is then followed by the deployment phase, during which users interact with the system by prompting it in order to generate outputs, often with limited human involvement. Consequently, users generally have no control over the composition of the training data. As a result, prompting the system may trigger an engagement with a particular protected work even where no such engagement was intended by the user, and despite the relatively limited degree of intervention exercised by them in the generation process.In this respect, the framework articulated by the Court, seemingly conceived with human acts of creation in mind, may ultimately require further judicial refinement or legislative clarification in order to accommodate the realities of AI-generated content.

However, as A. Guadamuz[30] further notes, Article 5(5) of Directive 2001/29/EC and the three-step test continue to operate in the background as important limiting principles. Even where a use *prima facie* satisfies the requirements of the pastiche exception, it must still not conflict with the normal exploitation of the work or unreasonably prejudice the legitimate interests of the rightsholder. From this perspective, large-scale commercial AI outputs capable of substituting for original works within their natural market may remain vulnerable under the third step of the test. Generative AI systems are capable of producing substantial volumes of content at minimal cost, including outputs that may compete directly with works created by human authors. Where such outputs are generated through systems trained on protected works and reproduce recognisable elements thereof, they may risk conflicting with the normal exploitation of those works, particularly if they operate as market substitutes for commissioned artistic. Moreover, the large-scale production and commercial dissemination of such outputs could cause unreasonable prejudice to the legitimate interests of rightholders, especially where the economic value of their works is affected without corresponding authorisation or remuneration. In such circumstances, even if a use were *prima facie* capable of qualifying as a pastiche under *Pelham II*, it could nonetheless fail to satisfy the conditions imposed by the three-step test.

Similar concerns have also been expressed in academic commentary[31], which emphasises that the three-step test may become the principal, if not the sole, remaining constraint preventing AI-generated outputs from being regarded as lawful pastiches where the exception does not require any specific intention

[30] Guadamuz (n 17).

[31] Söğüt Atilla-Aydın, 'ECS's Opinion on Pelham II and Its Potential Implications for AI-Generated Pastiches – Part 2' (The IPKat) <https://ipkitten.blogspot.com/2025/01/ecss-opinion-on-pelham-ii-and-its.html> accessed 12 May 2026.

on the part of the user, as is the case under the approach adopted in *Pelham II*. Accordingly, the Court's silence on the matter should be approached with caution, as the three-step test remains highly relevant. This context underlines the growing importance of the three-step test, which appears to constitute one of the most suitable tools for addressing disruptive uses in copyright law.

The European Parliament's Voss Resolution of March 2026 reflects precisely this tension, calling on the Commission to prevent infringements arising from AI-generated outputs whilst ensuring that lawful exceptions, including pastiche, remain available. The Resolution's explicit mention of pastiche in this context suggests an emerging awareness that the exception may serve as a defence for certain AI outputs[32].

7 Concluding Remarks

While the Pelham saga may now have come to an end, *Pelham II* constitutes a landmark ruling in EU copyright law and, more specifically, in the interpretation of the exceptions and limitations provided for under Directive 2001/29/EC. By recognising pastiche as an autonomous concept of EU law and articulating a structured framework for its application, the CJEU has provided long-awaited clarification of what had, until now, remained a blurry and uncertain notion.

At the same time, *Pelham II* is likely to assume particular significance in the context of ongoing debates surrounding AI-generated outputs. The judgment offers a conceptual framework capable of accommodating certain forms of AI-assisted or AI-generated content, while reaffirming that disguised reproductions

[32] European Parliament resolution of 3 February 2026 on copyright and generative artificial intelligence – opportunities and challenges (2026/2051(INI)) P10_TA(2026)0066, https://www.europarl.europa.eu/doceo/document/TA-10-2026-0066_EN.html accessed 12 May 2026.

and acts of plagiarism remain excluded from the scope of lawful pastiche. In this context, however, the three-step test appears likely to assume a central role in the near future, particularly where AI-generated outputs may compete with or substitute for original works within existing markets.

scripted

Volume 23, Issue 01, June 2026

Book review: *Deciphering IP Law and Its Conflict and Complementarity With Competition Law: Global Norms Against Asian Context*

Kung-Chung Liu
Abingdon, Oxon: Routledge, 2025. 316 pages. ISBN 9781032978536. £155.00.

Reviewed by Qi Jun Kwong*

DOI: 10.2218/scrip.12220

* Associate Professor, Graduate School of Law, Hokkaido University. The reviewer is grateful to Routledge for kindly making a copy of the book available for review.

1 Introduction

For every exclusive right that IP law carves out of the public domain, a boundary problem follows: how far, how long, and at whose expense? Professor Kung-Chung Liu's monograph *Deciphering IP Law and Its Conflict and Complementarity With Competition Law: Global Norms Against Asian Context* at the outset, prefaces his answer: IP is a form of market regulation, where under-protection causes fewer incentives to innovate, and over-protection leads to market failure.

Liu first sets out the three main strands in Part I of this book: a descriptive theory of IP as market regulation, an exposition of market competition and competition law, and a normative proposal for an IP code. These foundations anchor the monograph's remaining parts, which cover compulsory licensing (Part II), patent and trade mark databases (Part III), Fair, Reasonable, and Non-Discriminatory ("FRAND") licensing of standard-essential patents ("SEPs") (Part IV), second-hand branded-goods market (Part V), and the tangle of data, algorithms and IP (Part VI).

2 The grand theory: Part I

Liu opens with a survey of the intersection between IP and competition law, drawing on examples from across the full range of IP rights on a global scale – the LEGO trade mark cases, Google's book-archiving project and author's rights, Philips' patent pool with one royalty formula, Qualcomm's licensing practices, and more. Each example ends with targeted questions to identify a common problem – when IP rights produce outcomes that strain their own rationale or lead to unfair results, what can and should competition law do?

Chapter 2 is Liu's answer at the level of theory. Dissatisfied with the lack of an accessible general theory of IP law, Liu asserts that one should seek to

"democratise IP law to become laws for people on the streets."[1] Drawing on Robert Merges, Liu characterises IP as a sector-specific market regulation and outright rejects arguments that IP is an absolute natural right.[2] IP is, on this view, strictly instrumental: the exclusivity it confers is justified only to the extent that it incentivises innovation, fosters competition, and expands the public domain. Liu's framework is organised around two dimensions. The internal dimension, modelled on the Berne Convention's three-step test, concerns how IP rights are granted, used, and terminated, while the external dimension governs IP's relationship with competition law.

In Chapter 3, Liu identifies a shared goal between IP and competition law: enriching the public domain through the optimal allocation of limited resources. He surveys how competition law has variously checked and deferred to IP, citing US antitrust scepticism toward patent-related contracts in the 1960s and Germany's 1965 grant of immunity to collective societies for the exercise of copyright. He then examines how different jurisdictions apply a rule of reason approach in place of *per se* rules: an effects-based analysis in the US, a case-by-case approach in the EU, and a broad acceptance of the rule of reason across Asian jurisdictions save where IP holders engage in specific anti-competitive conduct.

Liu warns against IP exceptionalism and that IP should not displace other laws *lex specialis* in Chapter 2. In Chapter 4, Liu calls for a general theory of IP that elevates it as a standalone discipline. The case for codification is clear: "without codification, our lives will be ungovernable."[3] This is presented as a

---

[1] Kung-Chung Liu, *Deciphering IP Law and Its Conflict and Complementarity with Competition Law: Global Norms against Asian Context* (Routledge, 2025) p.30.

[2] Robert P Merges, *American Patent Law: A Business and Economic History.* (Cambridge University Press, 2022) pp.22-23.

[3] Liu (n 1), p.76.

remedy for divergent regulation of similar problems, vulnerability to lobbying pressure, and the recurring temptation to address each new issue by layering on more substantive law rather than integrating substantive and procedural rights into a coherent code.

Liu sets out fifteen principles for his IP Code, intended to apply across IP rights, though with varying force. The examples raised are, unsurprisingly, drawn from civil-law jurisdictions, but are framed as shared approaches rather than by legal tradition. Two principles are worth noting. The first, technical neutrality, challenges the special treatment accorded to semiconductor technology. According to Liu, *sui generis* protection of IC layout designs is unnecessary when patent law would suffice. The sixth – "fair sharing of economic fruits derived from one's creation"[4] – stands out: Liu floats the possibility of an AI levy system to provide authors with equitable remuneration, while candidly questioning its workability. The chapter closes with an international perspective: non-conformity with the Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS") should be tolerated where a country's actual circumstances require it, provided the principles of free trade are upheld, and Article 8(2) of TRIPS should be revised to mandate that competition law prohibit any abuse of IP rights that restraints or excludes competition.[5]

3 Applying the theory: Parts II–VI

3.1 Compulsory licensing (Part II)

With the theoretical framework in place, Parts II-VI turns to its application across specific doctrinal areas. Part II applies competition principles to compulsory

[4] Liu (n 1), p.90.
[5] Agreement on Trade-Related Aspects of Intellectual Property Rights, Article 8(2).

licensing. Liu offers a cursory view of how compulsory licensing has been, or may be, applied across major IP rights, excluding trade marks in line with TRIPS. Particularly notable is his call to apply the essential facilities doctrine which Liu notes is accepted globally and retains substantive influence in China. To my mind however, the doctrine has been relatively dormant in the US ever since the Supreme Court "neither recognised nor repudiated" it.[6] Similarly in the EU, the conditions have been further restricted following the *Android Auto* case.[7]

Liu also calls for revision of TRIPS to affirm compulsory licensing under several conditions: when domestic demand is not met, when an SEP is held by a dominant undertaking, or when a later IP cannot be exploited without infringing prior IP. Yet as Liu himself notes earlier in the chapter, the real bottleneck for compulsory licensing has been political rather than textual. The proposed revisions might also duplicate existing flexibilities. For example, Article 31(l) of TRIPS already addresses dependent patents.[8] That said, expanding compulsory licensing to cover unmet domestic demand remains politically contentious, and its application to SEPs warrants further exploration.

3.2 Aggregating IP (Part III) & FRAND Licensing (Part IV)

Part III offers a systematic comparison of how different jurisdictions approach patent pools and work pools, alongside a somewhat oddly placed proposal for a well-known marks database. The unifying concern is that the concentration of rights, while necessary to facilitate licensing, carries an inherent risk of restraining market competition.

---

[6] *Verizon Communications Inc. v. Law Offices of Curtis V. Trinko*, LLP, 540 U.S. 398 (2004).

[7] Case C-233/23, *Alphabet Inc and Others v Autorità Garante della Concorrenza e del Mercato* (Android Auto) EU:C:2025:110 (Grand Chamber, 25 February 2025).

[8] Agreement on Trade-Related Aspects of Intellectual Property Rights, Article 31(l).

For patent pools, Liu sets out several principles to prevent horizontal collusion: excluding substitute technologies, ensuring reasonable royalties, and retaining openness via a non-exclusive requirement. On work pools, Liu traces a shift in bargaining power from copyright management societies and voluntary agencies to internet provider platforms, examining the potential abuse of dominant position, and how competition authorities have responded. Liu proposes a dual response: ex-ante codification through copyright law or a *sui generis* collective rights management law, combined with ex-post control by competition law. On well-known trade marks, Liu identifies a market distortion when latecomers seeking to register or use a mark cannot determine whether a well-known but unregistered prior mark exists. The proposed remedy is a centralised online database which is governed by several reasonable, but largely aspirational principles: accuracy, all-inclusive, user-friendly, informative, and timeliness.

Part IV builds on Liu's long-standing work on FRAND licensing of SEPs and it is here where his comparative expertise is most fully deployed. Liu surveys the main jurisdictional fault lines: the hold-up and hold-out flip in US case law; good-faith and transparency obligations on both SEP holders and willing licensees in Germany and China; the bundling of non-essential with essential patents addressed in Korea, Japan, and Taiwan; royalty bases as determined by the Delhi High Court,[9] and national-versus-global portfolio licences as in *Unwired Planet v Huawei*.[10] Liu also addresses the deficiencies of the current licensing landscape: over-declaration, confidentiality of licensing terms and standard-setting organisation ("SSO") patent policies, and forum-shopping via anti-suit

[9] See e.g. *Dolby International AB & Anr. v GDN Enterprises Private Limited & Ors*. (2016) Delhi High Court, CS(COMM) 1425/2016.

[10] *Unwired Planet International Ltd v Huawei Technologies (UK) Co Ltd* [2020] UKSC 37.

and anti-anti-suit injunctions. Liu's solution, alongside a softer call for "dialogue and mutual persuasion,"[11] is that Asian jurisdictions, which tend to treat injunctive relief against a willing licensee as an abuse of right or dominance, should recognise FRAND commitments as contracts with third-party beneficiaries, as the US and UK do to forestall hold-ups. The continued relevance of competition law intervention in Asia is also underscored by an imbalance that Liu aptly flags: most SSOs are established in the US and France, leaving Asian jurisdictions as rule-takers rather than rule-makers.

Liu further proposes an institutional solution: SSOs should establish a one-stop competence centre, staffed by professionals already involved in the standard-setting process, and open to both SEP patentees and implementers. The centre would conduct essentiality checks, maintain a rates depository, and provide FRAND-targeted arbitration. On FRAND arbitration specifically, Liu contrasts it with standard arbitration where arbitrators are "clueless" as to appropriate FRAND rates.[12] The problem outlined by Liu however is access to FRAND data, and not competence. Arbitrator selection is a natural product of party autonomy, and parties to a FRAND dispute would logically elect arbitrators with FRAND-specific expertise, as the existing rosters at several arbitral institutions already make possible. What those arbitrators need is just access to the database. Liu's proposal would be more persuasive if, for instance, it is made clearer that confidentiality obligations require the repository to be accessible only to the SSO's own roster of vetted arbitrators. Still, the arbitrability of competition law issues in FRAND disputes, combined with the consent requirement inherent in arbitration means that where forum-shopping offers

[11] Liu (n 1), p.238.
[12] Liu (n 1), p.253.

strategic advantages, it is hard to see why parties would commit to a centralised procedure that affords them the least room to manoeuvre.

3.3 Second-hand branded goods (Part V) and Data and algorithms (Part VI)

Part V focuses on second-hand branded-goods market. Liu uses the problem of counterfeits and authenticity to frame a broader question about the integrity of the second-hand ecosystem. Expansive trade mark protection, Liu notes, obstructs competition where brand owners deny resellers retail and advertising relationships and dismiss them as counterfeiters. The prescription is pragmatic and draws on Howard Bowen's corporate social responsibility framework – brand owners should proactively support independent third-party authentication and accreditation bodies, while resellers should develop industry-wide standards on counterfeit prevention and liability.[13]

Part VI covers data and algorithms. Liu's premise is that big data, IP-protected or not, should not be prevented from forming, accumulating, and flowing freely. Liu points out that competition law is poorly suited to addressing access to big data because it is too slow and inefficient ex-post in a fast-moving market. The proposed alternative is an ex-ante FRAND-like licensing mechanism to compensate copyright holders. The treatment of algorithms follows a similar logic: algorithms drive online trading and develop patterns that resist easy detection, yet their internal decision-making processes remain undisclosed. The chapter is not explicit as to how algorithms are situated under IP law, focusing instead on governance and transparency in a data-driven economy – disclosure

[13] Howard R. Bowen, *Social Responsibilities of the Businessman* (University of Iowa Press, 2013).

obligations on deployers and operators, and effective audit regimes by the regulators.

4 Critical Reflections

Deciphering IP Law is a pragmatic monograph that situates IP law within broader governance considerations. It promises a comparative account of global IP norms tested against Asian responses, and on that promise it delivers. The monograph proceeds in a utilitarian-consequentialist manner, but readers seeking a deep dive into doctrinal disputes or normative theory will nonetheless find value in the handpicked cases and targeted questions that Liu deploys throughout the book.

Prospective readers should note several developments that have emerged since the book's publication in 2025. The landscape which Liu described, including the European Commission's draft SEP Regulation which contemplated FRAND-rate determination through a structured procedure was withdrawn in 2025, and the revised Technology Transfer Block Exemption Regulation, adopted in May 2026, is shaping EU's competition treatment of technology-licensing agreements and patent pools. None of this defeats Liu's framework; if anything, the continuing changes illustrates the durability of Liu's principle-based analyses and solutions.

One limitation worth flagging is that the monograph's account of Asia is geographically narrower than its framing suggests, centred on China, Korea, Japan, and India, with occasional appearances from Singapore, Taiwan, and Malaysia. The selection is understandable since only a handful of jurisdictions have resolved disputes on core IP and competition law issues or made them accessible in the literature. But these are the costs of pragmatism rather than reasons against it. Liu's analysis is methodical, comparative, and patient in

working through what a competition-based IP system would look like in operation. For policymakers, scholars working on Asian IP, and practitioners navigating the FRAND and compulsory-licensing puzzles that the next decade will continue to generate, Liu's monograph offers a holistic and governance-oriented point of departure.

scripted

Volume 23, Issue 01, June 2026

Book review: *Chilling Effects: Repression, Conformity, and Power in the Digital Age*

Jonathon W. Penney

Cambridge, United Kingdom: Cambridge University Press, 2025, 286 pages. ISBN 1108725309. £23.

*Reviewed by Te-Ying Chen**

DOI: 10.2218/scrip.12294

* PhD Candidate, Edinburgh Law School, University of Edinburgh, Edinburgh, UK, Te-Ying.Chen@ed.ac.uk

1. The Ubiquitous Chilling Effect

The traditional theory of chilling effects expects an Orwellian societal-level repression of speech and ideas. While that can be what chilling effects look like, it is not always the case. Imagine a scenario at a crowded bus stop, even though there is no designated queue, people naturally form a line. Although standing outside this queue is not illegal, those who try to cut in might be scolded. As a result, passengers will wait either in the queue or outside of it, resigning themselves to be the last ones to board. This situation is rarely recognised as a result of a chilling effect, but there is a similar theoretical framework underlying this behaviour.

Chilling Effects: Repression, Conformity, and Power in the Digital Age, written by Jonathon W. Penney, a legal scholar and social scientist at Osgoode Hall Law School, York University, Toronto, takes a relatively wide perspective to reshape the concept of chilling effects. Consequently, his theory helps us understand the far-reaching scale and scope of these effects, and how they are toxic and corrosive to democracy and civil society. This book is the culmination of his research; in addition to his insightful legal analysis, social science expertise is integrated throughout the text, making it rich, diverse, interdisciplinary, and accessible.

The chilling effect is an abstract idea that first gained prominence in US through a series of cases decided during the 1950s and 60s. During this period, the US Supreme Court invoked the concept to strike down overreaching legislation from the McCarthy Era, when the government focused on addressing public fear and hysteria regarding the supposed threat of communism.[1] The concept

[1] Jonathon W Penney, *Chilling Effects: Repression, Conformity, and Power in the Digital Age* (CUP, 2025), pp. 19-20

was also central to civil rights movements challenging laws that chilled freedom of speech and other expressive activities protected under the First Amendment.[2] Beginning with Frederick Schauer, prominent free speech scholars started theorising the idea of chilling effect, focusing on how legislation with uncertain provisions constrains citizens' free expression. However, a purely legalistic focus on chilling effects leaves a significant gap when compared to the results of empirical research. While the traditional understanding of chilling effects is based on deterrence theory, which assumes individuals make decisions based on rational cost-benefit calculations, results from empirical research do not seem to support this theory.[3]

2. Reconstructing the Chilling Effect Beyond Legal Contexts

This book aims to bridge the gap between the conventional, legalistic conceptualisation of chilling effects and the inconsistent empirical evidence in current scholarship. It is divided into three parts: Part I elaborates on and analyses chilling effect theory as built upon traditional viewpoints, specifically, those rooted in the fear of legal or privacy-related harms. Traditionally, the chilling effects is understood through a deterrence model involving rational choice. Individuals engage in self-censorship due to a calculated fear of consequence. Penney references Orwell's *Nineteen Eighty-Four* and Huxley's *Brave New World* to illustrate how totalitarian regimes deploy technology and mass surveillance to maintain total population control.

---

[2] Jonathon W Penney, 'Chilling Effects: Online Surveillance and Wikipedia Use' (2016) 31(1) *Berkeley Technology Law Journal* 117-182, pp. 125-127; Jonathon W Penney, 'Understanding Chilling Effects' (2022) 106(3) *Minnesota Law Review* 1451-1530, pp. 1464-1465; Frederick Schauer, 'Fear, Risk and the First Amendment: Unraveling the "Chilling Effect"' (1978) 58 *Boston University Law Review* 685-732, p. 685.

[3] Penney (n 1), p. 25.

However, he highlights a substantial disconnect between this legacy theory and empirical findings. Drawing on social science and psychology, the author shows that people do not consistently engage in rational choice or possess the high level of legal awareness that deterrence theory assumes.[4] Because humans are not entirely rational actors, they often make suboptimal decisions based on limited information, decisions they may be regret only minutes later. In this section, Penney effectively exposes the limitations of the traditional chilling effect doctrine.

In Part II, Penney bridges chilling effects theory with interdisciplinary knowledge. Adopting a social science perspective, he discusses how social conditions shape individual behaviour. He explores the compelling case of how communal power affects behaviour in areas where formal law is difficult to enforce. Since law is often the greatest common denominator of social customs, evolving from local habits for dispute resolution, the community frequently exerts a more immediate influence on individuals than the law itself.

Subsequently, Penney introduces four core elements causing chilling effects: observation, uncertainty, personalisation, and power/authority. These align with research in biology and psychology to explain why the chilling effect is so potent. This foundation leads to his 'conformity theory of chilling effect', which he applies to various domains: information and data, legal frameworks, and social or infrastructural systems.

[4] Robert Prentice, 'Chicago Man, K-T Man, and the Future of Behavioral Law and Economics' (2003) 56(6) *Vanderbilt Law Review* 1663-1777, pp. 1666-1667; Paul H Robinson and John M Darley, 'Does Criminal Law Deter? A Behavioral Science Investigation' (2005), pp. 173-174, available at https://papers.ssrn.com/abstract=660742; Janice Nadler, 'Expressive Law, Social Norms, and Social Groups' (2017) 42(1) *Law & Social Inquiry* 60-75, pp. 62-63.

Part III provides a comprehensive discussion of the chilling effect's broader implications. Penney first examines its dangers. Drawing on Foucault,[5] he argues that chilling effects are not merely repressive to stop individuals from being active, but also productive, creating entirely new social and cultural realities. These effects undermine individual autonomy and personal development while fostering societal polarisation and extremism.

These dangers are not merely theoretical. Penney uses Texas Senate Bill 8 (the Texas Heartbeat Act) as a case study to demonstrate how chilling effects can be weaponised. A narrow legal focus might fail to recognise how such provisions generate a 'chill', but such an approach underestimates the Act's profound extra-legal impacts and ignores the rights of the targeted minority.

To address cases where interests like data privacy and national security are difficult to balance, Penny proposes a framework to predict and evaluate these effects. By quantifying his four core elements causing chilling effects, he concludes that scenarios involving personalisation and personal threats produce the greatest chill.[6] Finally, Penney advocates for a dual transformation of the chilling effects doctrine, operating at both microscopic and macroscopic levels. On the microscopic level, he argues that courts must expand their focus to account for diverse, multifaceted harms when assessing whether a legal provision includes a chill. Conversely, on the macroscopic level, he addresses structural threats. Here, he utilises China's AI-driven mass surveillance and automated law enforcement as a cautionary archetype of the future of technological control. To mitigate these systemic risks, Penney ultimately

---

[5] Michel Foucault, *Discipline and Punish: The Birth of the Prison* (Alan Sheridan tr, 2nd edn, Random House, 1995) p. 194.

[6] Penney (n 1), p. 137.

proposes a suite of comprehensive structural solutions: strictly regulating surveillance, reducing legal uncertainty, curtailing personalised threats, and placing meaningful constraints on institutional power.

3. Toward a New Theoretical Understanding of the Chilling Effect

As a PhD student researching freedom of expression, I initially expected a series of discussions focused on how chilling effects limit individual expression and behaviour. Naturally, I anticipated the discourse would stem from liberal theory to examine the impact on individual liberty. However, this book significantly broadened my perspective on the comprehensive nature and systemic impact of chilling effects.

The interdisciplinary approach is particularly compelling. For instance, while social polarisation is often attributed to 'echo chamber'[7] or 'filter bubble'[8] created by internet architecture, Penney explores polarisation as a result of chilling effects intertwined with fundamental human behaviour. He notes that conformity to the group is an evolutionary trait embedded within us.[9] Social conformity activates

[7] An 'echo chamber' is a metaphor used to describe a bounded, enclosed media space that has the potential to both magnify the messages delivered within it and insulate them from rebuttal: Kathleen Hall Jamieson and Joseph N Cappella, *Echo Chamber: Rush Limbaugh and the Conservative Media Establishment* (OUP, 2008) p. 76.

[8] The term 'filter bubble' is often used interchangeably with 'echo chamber'. However, unlike an echo chamber, which might be actively chosen by information receivers, the filter bubble emphasises how ranking algorithms engage in passive personalisation, curating information in certain ways that effectively lock users into their own echo chambers: Amy Ross Arguedas, Craig T. Robertson, Richard Fletcher and Rasmus Kleis Nielsen, 'Echo chambers, filter bubbles, and polarisation: a literature review' (*Reuters Institute for the Study of Journalism*, 19 January 2022) available at https://reutersinstitute.politics.ox.ac.uk/echo-chambers-filter-bubbles-and-polarisation-literature-review, accessed 25 May 2026 (DOI: 10.60625/risj-etxj-7k60). More details can be found in Eli Pariser, *The Filter Bubble: What the Internet Is Hiding from You* (Penguin, 2012).

[9] Ruthie Pliskin, Amit Goldenberg, Efrat Ambar and Daniel Bar-Tal, 'Speaking Out and Breaking the Silence' in Daniel Bar-Tal, Rafi Nets-Zehngut and Keren Sharvit (eds) *Self-Censorship in Contexts of Conflict: Theory and Research* (Springer, 2017); Penney (n 1), pp. 60-61.

the brain's reward systems, whereas social rejection and ostracism trigger the same neural pathways associated with physical pain.[10] These biological predispositions have been weaponised by both public and private entities to marginalise 'minorities', whether they be women affected by the Texas Heartbeat Act, ethnic minorities in China, or any group categorised by specific 'tag'.

Ultimately, Penny asserts that chilling effects are not merely a legal concept, but a social fact. This phenomenon is generated not only by vague legislation that stifles speech but also by individual behavioural choices and the society those choices collectively form. Here, the chilling effect takes on a productive dimension. Some might argue that the society remains 'free' because mass surveillance has not physically stopped people from speaking, and online platforms continue to serve as the 'modern public square'.[11] However, the negative impact of chilling effects is not diminished by the normalisation of surveillance. On the contrary, it steadily erodes personal autonomy and identity development, eventually corroding the foundations of liberty and democracy. Over the long term, this process poses a devastating threat to democratic society.

If there is a minor drawback, it is perhaps the heavy focus on US case studies. While 'Big Tech' is primarily based in the US, the boundary-crossing nature of technology means that chilling effects are global, not local. While the book touches upon European online platform accountability and China's autocratic surveillance, a deeper exploration of how online chilling effect evolve through globalisation would have been a great critical evaluation and addition.

---

[10] Pliskin *et al* (n 9), p. 250; SL Neuberg, DT Kernick and M Schaller, 'Evolutionary Social Psychology' in Susan T Fiske, Daniel T Gilbert and Gardner Lindzey (eds), *Handbook of Social Psychology* (Wiley, 2010) p. 778; Steven Fein, Hazel Markus and Saul Kassin, *Social Psychology* (10th edn, Wadsworth Publishing, 2016) pp. 271-272.

[11] *Packingham v North Carolina* 582 US 98 (2017).

Nevertheless, this does not diminish the profound contribution of this work. Penney employs an accessible writing style and a wealth of case studies to ground abstract theory. By bridging traditional legal perspectives with interdisciplinary research, he provides a clear 'silhouette' for a complex concept, successfully closing the gap between theory and reality. This book is an insightful commentary and an excellent introduction to the field. I strongly recommend it to anyone seeking to understand the chilling effect beyond a strictly legalistic definition.

scripted

Volume 23, Issue 01, June 2026

Book review: *Law and Technology: A Methodical Approach*

Ryan Calo
Oxford: Oxford University Press, 2025. 160 pages. ISBN 0197526136. £25.99 (Hardcover).

*Reviewed by Guan Yue (Yuma) Wu**

DOI: 10.2218/scrip.12111

* PhD Student, Graduate Studies in Law, University of Ottawa, Ottawa, Canada, yuma.wu@uottawa.ca

1 Introduction

The field of law and technology has a problem, so diagnoses esteemed law and technology scholar Ryan Calo in his new book, *Law and Technology: A Methodical Approach*. The study of law and technology "often lacks the rigor, coherence, and consistency that analysis of technology demands."[1] As a result, scholars of this pursuit are "poorly situated to address a subject matter as complex, dynamic, and frankly *disorienting* as technology."[2] This need not be. Calo offers a solution: a "formal approach to law and technology capable of navigating how technology daunts and confuses" that centres transparency, rigour, and consistency in the pursuit of legal interventions for technology: The Methodical Approach to Law and Technology (the "Methodical Approach").[3] Calo's work not only illuminates the path forward but also provides a valuable lens through which to view past works in law and technology.

2 A History of Law and Technology

In the first half of his book, Calo lays the foundation for his proposed Methodical Approach by exploring the conceptual challenges (Chapter One) and theoretical neighbours (Chapter Two) of technology and law.

Chapter One outlines three challenges with centring technology as a topic of legal analysis: *non-contingence*, *hidden will*, and *ungovernability*. Calo uses the term "*non-contingence*" to refer to the illusory inevitability of technology as a constant force of forward societal progress.[4] Instead, Calo contends, technology's

[1] Ryan Calo, *Law and Technology: A Methodical Approach* (Oxford: OUP, 2025), p. 4.
[2] *Ibid*.
[3] *Ibid*., p. 86.
[4] *Ibid*., p. 26–27.

legally salient potential to shape behaviours and outcomes is contingent on contemporaneous social circumstances.[5] Second, Calo uses "*hidden will*" to describe technology's ability to obscure the role of its creators.[6] As Calo observes, "technology means *someone else not present is participating*."[7] Complex as the issue of attributing legal responsibility in such mediated interactions may be, Calo's observation characterises the root of the problem as a diffusion of responsibility. This insight raises the potential for reforms aimed at explicitly locating and "concentrating" legal responsibility, such as strict liability regimes.[8] Third and lastly, Calo objects to the "myth" that novel technology is somehow *ungovernable*.[9] Calo identifies two variations of this myth: emerging technology is too *complicated* for lawmakers to address (the "*complexity problem*"), and that technology *outpaces* democratic decision-making for productive rule-making (the "*pacing problem*").[10] The reviewer suggests a qualification: while the complexity and pacing problems do indeed plague the regulation of novel technology, not all jurisdictions use these problems to justify non-regulation as the US has.[11] For instance, as Calo notes, EU regulators have pioneered a variety of legal frameworks in the tech law space despite these challenges.[12] While their innovations are far from perfect, with the aforementioned problems manifesting as challenges in reconciling conflicting definitions between different frameworks with the *Digital Service Act* and *General Data Protection Regulation* as well as in capturing novel iterations of technology such as general purpose AI programs

[5] *Ibid*., p. 28.
[6] *Ibid*., p. 31.
[7] *Ibid.*
[8] *Ibid*., p. 38.
[9] *Ibid*., p. 39.
[10] *Ibid*., p. 39–40.
[11] See *e.g. ibid*., p. 44–45.
[12] *Ibid*., p. 44–45.

like ChatGPT in the *Artificial Intelligence Act*, it remains the case that the EU's early efforts to regulate novel technology are lending structure to previously ungoverned digital spaces.[13] The US departed from a similarly proactive approach to assessing and regulating technology through a series of conservative government policies, including but not limited to the defunding of the federal Office of Technology Assessment in 1995.[14]

Chapter Two situates the study of technology and law in relation to Science and Technology Studies ("STS"), which focuses on "how social, cultural, and other forces shape technology, and how, in turn, technology shapes people and society."[15] Calo observes that STS is a mature discipline with deep insights about the social construction of technology that alleviate the analytical burden of law and technology scholars.[16] Calo then identifies several insights by law and technology scholars that were preceded by insights in STS, such as the idea of generative technology, which is preceded by similar insights regarding conviviality in STS more than four decades prior.[17] Not only should law and technology scholars pay more attention to the valuable work of STS scholars, Calo argues, but they should also "share back" their insights with STS.[18] Namely, Calo notes that law and technology can supplement STS with their commitment to normativity and pragmatism, as "the vast majority of STS" is primarily theoretical and lacks normative analyses and practical interventions.[19] The

[13] See *e.g.* Maitrayee Pathak, "Data Governance Redefined: The Evolution of EU Data Regulations from the GDPR to the DMA, DSA, DGA, Data Act and AI Act" (2024) 10(1) *European Data Protection Law Review* 43-56.
[14] *Supra* n. 1, p. 138.
[15] *Ibid*., p. 53.
[16] *Ibid*., p. 62–66.
[17] *Ibid*., p. 64–65.
[18] *Ibid*., p. 69.
[19] *Ibid*., p. 72–74.

reviewer suggests another qualification to Calo's suggestion: law's commitment to normativity and pragmatism is valuable to STS scholars *insofar as* they share the same outcome-oriented goals as legal scholars do. While practical interventions with potential for real-world outcomes are powerful motivators for scholarship, they are not the sole determinant of a project's value. For example, a descriptive exercise without normative critique of the circumstances or practical interventions is still a valuable contribution, either as an expansion of human understanding or as the inspiration to later works that *do* hold normative commitments or pragmatic objectives. In other words, while explorations in STS would indeed benefit from the normative and pragmatic perspectives of legal scholarship where practical outcomes are the objective, adoption of legal and policy goals do not necessarily equate to an improvement for all of STS scholarship. Indeed, if STS scholars were assured that technology law scholars would take notice of their work when introducing novel policy interventions, then introducing pragmatic analysis may be more redundant than persuasive.

3 The Methodical Approach to Law and Technology

In the second half, Calo presents the Methodical Approach to law and technology in Chapter Three, followed by three applications in Chapter Four: augmented reality, machine learning, and cochlear implants. This review focuses on Chapter Three, which organises the Methodical Approach into four steps: (1) *Definition*, (2) *Envision*, (3) *Analysis*, and (4) *Intervention*. In each step, Calo proposes a set of "intellectual tasks" aimed at elucidating the normative and conceptual assumptions imbued in the work at hand.[20]

Definition. To begin, Calo asks a simple question: what are we talking

[20] *Ibid*., p. 89.

about?[21] Calo sets out three attributes for the author of the proposed work in law and technology to define: level of abstraction (technology in general versus a specific instance), essential attributes of the technology of study, and attributes that distinguish the technology from others.[22] Calo notes that this exercise invites the author to explore alternative configurations of their topic.[23] Adding to this, the reviewer posits that definitions from other fields that study the technology at hand should also inform the author's conception of the technology. A concept that harmonises with other disciplinary definitions enables interdisciplinary conversations and supports the adoption of cross-disciplinary interventions.

Envision. Next, Calo asks: "How does this particular technology affect how people live?"[24] Who is affected by this technology, and what are the effects?[25] Calo sets out sub-topics for the author to explore, such as distributive consequences of the technology and the timeline for the potential changes that the technology might bring.[26] Calo then suggests that authors undertaking this task apply epistemic frameworks from other disciplines, such as affordance theory, to "scaffold the envisioning of technological change".[27] There are different lenses of envisioning technological impact beyond what is suggested here,[28] and the reviewer adds that it is also essential to justify the choice of lens in the context of the author's normative baseline, as will be discussed next.

Analysis. Once the subject of study and its societal impacts have been

[21] *Ibid*., p. 90.
[22] *Ibid*., p. 92–93.
[23] *Ibid*., p. 93.
[24] *Ibid*., p. 95.
[25] *Ibid*., p. 96–100.
[26] *Ibid*., p. 96.
[27] *Ibid*., p. 96–100.
[28] *Ibid*., p. 100.

sketched out, Calo directs the author to a formalised framework for the legal analysis of technology, furnished by two questions: (1) Is the author interested in the relationship between the technology in question and the law in general, or the legal questions raised by a specific instantiation of technology, and (2), what is the "normative baseline" of the project?[29] Calo further sets out three potential normative baselines: restoration of the status quo before disruptions by the technology, advancement of a "preexisting normative goal" such as efficiency, or arguing for a new status quo in light of the new socio-technical conditions enabled by the technology.[30] From this and the Definition step discussed above, the reviewer observes a normative goal on Calo's part as well: increased transparency in law-and-technology discussions through the articulation of normative motivations. This will enable productive discussions of differences in the normative roots of proposed interventions and foster diversity in scholarship.

Intervention. Lastly, Calo sets out the final step: the selection and justification of a legal intervention.[31] Similar to previous stages, Calo advocates the recognition of alternative configurations and normative assumptions behind the choice of intervention.[32] Should the government regulate?[33] If so, how, and why?[34] Here, Calo juxtaposes government intervention with the lack thereof,[35] and the reviewer cautions that this dichotomy may not apply to all technology regulation. For instance, some of the earliest attempts to regulate AI-generated content online in a structured manner occurred on Reddit, where moderators set

[29] *Ibid*., p. 96–100.
[30] *Ibid*.
[31] *Ibid*., p. 111.
[32] *Ibid*.
[33] *Ibid*.
[34] *Ibid*., p. 113–14.
[35] *Ibid*., p. 114–15.

rules around AI usage to maintain the integrity of their communities.[36] The reviewers contend that authors would benefit from acknowledging other rulemaking in the same space. Expanding the scope of what constitutes an intervention in law and technology is especially useful given that non-governmental institutions, such as online communities, are often the "first line" in the adoption and sometimes resistance of novel technology. As such, incorporating these "outside" perspectives can enrich discussions and prevent redundancies in analyses.

4 Conclusion: Alternatives to The Methodical Approach

Following the conclusion of the book, an intrigue remains for Calo's proposed Methodical Approach. *What are the alternatives*? This review concludes by identifying two trailheads for future exploration: the *reverse approach* and the *ambiguous approach*.

4.1 The Reverse Approach

This approach reverses the Methodical Approach – instead of starting with a technology and ending with conclusions about the law, what if we used the law to reach conclusions about technology? By examining laws that focus on a piece of technology, researchers can gain valuable insights into which attributes lawmakers prioritise and whether existing definitions sufficiently capture the technology. The reviewer imagines four steps to the Reverse Approach:

(1) *Examining the "solution space"*: identifying legal interventions that are

[36] Travis Lloyd, Jennah Gosciak, Tung Nguyen, Mor Naaman, "AI Rules? Characterizing Reddit Community Policies Towards AI-Generated Content", Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems, available at dl.acm.org/doi/full/10.1145/3706598.3713292 (accessed 22 February 2026).

aimed at the same piece of technology, such as all legislation that mentions the term "autonomous vehicles".

(2) *Stating the normative baseline*: elucidating the author's normative baseline – by what measure is the law in question successful in its attempts to regulate its subject technology?

(3) *Assessing the impact of the law*: placing the laws in question relative to the author's identified normative baseline – was it successful in what they set out to do? Are there gaps or overlaps?

(4) *Defining the technology relative to the law*: What are the essential attributes of the technology as defined by lawmakers? Are there attributes that are over-inclusive or under-inclusive?

Drawing from Calo's recommendations in Chapter Two, this approach imports the STS framework of the Social Shaping Of Technology ("SCOT") into law and technology by imbuing it with normative and pragmatic commitments. Whereas SCOT has no explicit normative nor inherent pragmatic commitments, the Reverse Approach identifies the incumbent interventions and the successes or shortcomings that they may have based on the author's normative baseline.[37]

4.2 The Ambiguous Approach

Rather than seeking a unified vision of the legal challenge posed by the technology at hand, the Ambiguous Approach focuses on exploring the ambiguities in the socio-technical configuration of concern. For example, the

[37] See Trevor Pinch and Wiebe Bijker, "The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other" (1984) 14(3) *Social Studies of Science* 399-441.

Ambiguous Approach also asks the author to explore different definitions of "autonomous vehicle", but not to produce a single definition. Instead, this approach asks the author to explore different definitions that yield different legal and/or normative outcomes. The reviewer imagines four steps as follows:

(1) *Explore potential definitions of the technology in question and identify areas of ambiguity*: identifying uncertainty (whether from the lack of empirical evidence or from conceptual complexity), or potential contradictions between different definitions in theory or practice.

(2) *Assess the actual or potential impact of the ambiguity on how the technology is received, used, and discussed*: for example, does the ambiguity result in overestimations, underestimations, or mistaken understandings of the technology in question? How does it do that?

(3) *Evaluate the legal outcomes of these ambiguities in accordance with the author's stated normative baseline*: for example, do they lead to gaps or overlaps in lawmaking or enforcement? If that is undesirable, why is it so?

(4) *Identify interventions, if needed*: reduce the potential ambiguities identified or create new interventions that are more resilient to them.

This approach seeks to highlight the ambiguities, gaps, and contradictions in law and technology discussions. However, that does not mean that this approach is necessarily descriptive and illustrative. As seen in step (4), authors can use the Ambiguous Approach to highlight deficiencies in current interventions and recommend new ways forward.

scripted

Volume 23, Issue 01, June 2026

Book review: *Arcana Technicae: El derecho y la inteligencia artificial*

(Arcana Technicae: Law and Artificial Intelligence)

Carlos Amunátegui Perelló
Valencia: Editorial Tirant lo Blanch 2021. 128 pages.
ISBN 978-84-1355-020-6. 22 euros (eBook).

*Reviewed by Jorge Balmaceda Hoyos**

DOI: 10.2218/scrip.12285

* DIGI+ fellow, sponsored by the European Commission for the MSCA Global Postdoctoral Fellowships (101081609 — DIGI PLUS — HORIZON-MSCA-2021-COFUND-01) programme under the Horizon Europe (HORIZON) Marie Skłodowska-Curie Actions & Support to Experts. Researcher, School of Law, University of Galway, Galway, Ireland; **jorge.f.balmacedahoyos@universityofgalway.ie**

1 Defining and historicising artificial intelligence

Professor Carlos Amunátegui Perelló's *Arcana Technicae: Law and Artificial Intelligence*, is a timely and ambitious attempt to contextualise artificial intelligence (AI) within contemporary legal reasoning. The book is written in Spanish, and no English-language or other foreign-language translations are currently available.

Its significance is heightened by the current Chilean debate on a bill regulating AI (Bulleting No. 16.1821-19[1] presently in its first constitutional stage), which, while inspired by the European Union's Regulation (EU) 2024/1689[2], raises complex questions about transposing European regulatory models into a different cultural and economic environment. In this light, Amunátegui's monograph constitutes both an explanatory and a critical engagement with how law assimilates technological innovation across jurisdictions of the civil-law tradition.

Arcana Technicae is elegant in design and rich in learning. Structured in three chapters, it synthesises central issues concerning artificial intelligence and its legal implications, offering a Spanish-language bridge between technical and juridical discourse (a considerable contribution in a field dominated by English literature). Although concise, the work is accessible without losing rigour and succeeds in keeping its interdisciplinary core coherent.

---

[1] Cámara de Diputadas y Diputados de Chile, Regula los sistemas de inteligencia artificial, Boletín No 16821-19 (7 May 2024) <https://www.camara.cl/legislacion/proyectosdeley/tramitacion.aspx?prmBOLETIN=16821-19&prmID=17429> accessed 9 June 2026.

[2] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L 2024/1689.

The opening chapter introduces the concept and historical development of AI, tracing its origins to the Dartmouth Conference of 1956 and its subsequent "summers and winters." The author's pedagogical style makes abstract ideas tangible, explaining the structure and functioning of neural networks and their cognitive limitations (particularly their inability to abstract or manipulate concepts). Numerous examples help demystify these processes for readers unfamiliar with computational theory, enabling jurists and students alike to grasp the foundations of algorithmic reasoning.

Amunátegui also differentiates among expert systems, the Internet of Things, facial-recognition technologies, and autonomous vehicles, illustrating how these modalities shape the broader ecology of AI. His short yet accurate account of deep learning and the principal research schools captures the technological diversity underpinning AI's current evolution. The section concludes by addressing two core challenges of algorithmic systems (bias and opacity) and proposes responses grounded in European guidance, notably the Ethical Guidelines for Trustworthy AI.[3]

While introductory, this chapter establishes a solid conceptual foundation. A more critical reflection on the epistemological limits of "explainability" in AI could, however, enhance the dialogue between law and cognitive modelling – an area increasingly relevant to questions of accountability and due process.

2 Artificial intelligence in law

The second chapter, "Artificial Intelligence in Law," is the analytical heart of the book. Here, Amunátegui examines how automated systems intersect with

[3] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI* (European Commission, 8 April 2019) <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> accessed 9 June 2026.

fundamental legal and ethical principles: due process, equality before the law, respect for fundamental rights, human dignity, proportionality, and transparency. He identifies potential conflicts between algorithmic decision-making and procedural fairness, pointing to the need for human oversight (under user control) and adequate governance mechanisms.

The discussion is grounded in comparative jurisprudence. The author references *State v Loomis* (2016)[4], a seminal case on the use of risk-assessment algorithms in criminal sentencing and contrasts it with corporate responses such as Amazon's and Google's adoption of "Machine Learning Fairness".[5] These examples anchor abstract principles in concrete regulatory experiences, though the treatment sometimes leans descriptive; a deeper normative critique of how fairness is operationalised by private actors would have strengthened the argument.

Amunátegui's legal analysis extends beyond litigation analytics. He explores intellectual-property issues concerning AI-generated works, the potential legal personality of algorithms, obligations and contracts, and tort liability, areas often discussed in isolation but seldom synthesised coherently. Particularly engaging is his comparative use of Roman-law analogies, offering a doctrinal lens through which to assess the assignation of liability and ownership in autonomous systems. The scholarship here demonstrates both conceptual agility and cultural awareness, situating AI within a continuum of legal evolution rather than a rupture.

---

[4] *State v Loomis* 2016 WI 68, 371 Wis 2d 235, 881 NW 2d 749 (Wis 2016).

[5] This refers to Google's commitment to avoiding the creation or reinforcement of unfair bias. Google, 'AI Principles' (Google AI) https://ai.google/principles/#our-ai-principles-in-action accessed 10 June 2026.

3 The future and the profession

The final chapter reflects on AI's transformative potential for the legal profession. Amunátegui provokes the reader with a deceptively simple question: Is AI "the future," or have we already entered its "present"?[6] The inquiry recalls Richard Susskind's thesis that the legal profession must reconsider its models of service delivery and knowledge production in the face of automation.[7] Amunátegui shares this view yet tempers it with realism: AI should not replace the lawyer but may reshape how the lawyer reasons, acts, and values human judgment.[8]

The author surveys examples of increasing automation (notarial functions, registries, archiving, and contract-drafting processes) and evaluates their expansion beyond common-law jurisdictions into continental practice. He devotes particular attention to online dispute resolution (ODR) mechanisms, which use by commercial chambers and digital platforms such as Amazon and eBay has demonstrated procedural efficiency without necessarily undermining fairness. Notably, he warns against inferring efficiency as justice, insisting that any digital process must preserve an avenue for appeal and procedural transparency. This insistence on human-centred safeguards distinguishes his contribution from purely techno-optimistic literature.

In discussing data and predictive analytics, Amunátegui traces developments from the 1970s statistical models to today's advanced platforms by Thomson Reuters, Tirant lo Blanch, and LexisNexis. He observes that not all jurisdictions have embraced these tools, citing the example of France, where

---

[6] Carlos Amunátegui Perelló, *Arcana Technicae: El Derecho y la Inteligencia Artificial* (Tirant lo Blanch 2021) 97-103.

[7] Richard Susskind, *Tomorrow's Lawyers: An Introduction to Your Future* (2nd edn, Oxford University Press 2017) 59–122.

[8] Amunátegui Perelló (n 6) 108.

legislation enacted in 2019 restricts the use of certain predictive justice tools[9]. This law prohibits misusing magistrates' identity data to compare or predict judicial behaviour in criminal matters, effectively limiting predictive analytics to private-law domains. The case epitomises the tension between innovation and privacy, a topic ripe for further empirical exploration.

One of the book's most engaging sections concerns legal education. In the final chapter, Amunátegui questions whether current pedagogies have become obsolete or whether room remains for adaptation in a digital environment. Echoing Hunter (2020), he suggests that while many legal tasks — notably drafting and reviewing contracts — may be automated, the initial framing of a legal problem and the subsequent evaluation of algorithmic outputs will remain human responsibilities[10]. These require judgment, ethical reflection, and conceptual abstraction, capacities that no silicon-based system can yet emulate. Hence, he proposes revisiting curricula to emphasise analytical and ethical competencies over rote doctrinal learning. His argument echoes broader global debates about "law and technology" instruction but is contextualised effectively within the civil-law educational tradition.

4 Concluding remarks

The principal virtue of *Arcana Technicae* lies in the author's ability to integrate technical, philosophical, and legal insights into a compact and approachable text. For Spanish-speaking audiences, it provides not only a translation of complex English-language debates but also an interpretive framework anchored in

[9] Loi n° 2019-222 du 23 mars 2019 de programmation 2018–2022 et de réforme pour la justice (23 March 2019), codified in arts 226-18, 226-24 and 226-31 of the French Penal Code.

[10] Dan Hunter, 'The Death of the Legal Profession and the Future of Law' (2020) 43(4) *UNSW Law Journal* 1199.

Roman-law logic and continental methodology. Its pedagogical merit is undeniable.

Yet the book's brevity occasionally limits critical depth. While Amunátegui concisely outlines problems such as bias, opacity, and accountability, there is limited engagement with competing theoretical positions (particularly those emerging from critical algorithm studies or feminist legal theory) which could enrich the work's normative scope. Similarly, an explicit treatment of Latin American contextual realities (beyond the Chilean legislative reference) would further consolidate the comparative ambition implied in the introduction.

These caveats, however, are minor in comparison to the monograph's overall achievement. Amunátegui's command of both technical substance and legal doctrine makes *Arcana Technicae* stand out within the Spanish-language literature. It succeeds in making AI legible to lawyers without simplifying its complexity, and in portraying law as a living system capable of absorbing technological change while retaining humanistic orientation.

Arcana Technicae contributes meaningfully to the civil-law perspective on AI and legal transformation. By combining doctrinal clarity with conceptual breadth, it enables readers to situate artificial intelligence within the continuum of legal reasoning rather than outside it. The text's accessibility makes it suitable for a wide audience, from judges and practitioners to academics and advanced students, without sacrificing scholarly precision.

Future editions would benefit from incorporating developments in jurisdictions where AI is already operational in judicial contexts, notably Argentina and China, and perhaps from issuing a comprehensive English translation to extend its reach. Despite its concise scope, the work's synthesis of law, computer science, history, and ethics secures its place as a reference point in the Spanish-language scholarship on AI and law.