Cambridge Law Journal, **85(1)**, March 2026, pp. 151–185 © The Author(s), 2026. Published by Cambridge University Press on behalf of The Faculty of Law, University of Cambridge. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.
doi:10.1017/S0008197325101086

RECONCILING TRADE SECRETS AND AI PUBLIC TRANSPARENCY

PERRY KELLER AND TANYA APLIN*

ABSTRACT. *Poor public understanding of artificial intelligence (AI) systems has become a matter of acute concern. Even when lacking expert technical knowledge, there are good democratic, economic and other societal reasons for ensuring that the public right to know operates effectively in the AI era. Yet, the trade-secret claims of AI providers and deployers are widely seen as a potential barrier to information disclosure rights and duties, which has provoked calls for areas of significant public interest to be carved out from the protections of trade-secrets law. Such transparency carve-outs are, however, likely to lead to uncertainty, over-inclusion and ineffectiveness. In this article, we argue that the dynamic, public-driven character of the right to know can be better secured through third-party participation and public-interest stewardship innovations in AI transparency.*

KEYWORDS: *transparency*, *artificial intelligence*, *trade secrets*, *access*, *disclosure*.

I. CONTESTING AI PUBLIC TRANSPARENCY

The growing ubiquity and impact of artificial intelligence (AI) systems in many aspects of ordinary life has, after years of simmering public awareness, become a matter of widespread concern. While increasingly reliant on AI-driven services, humans are also frequently anxious about the risks of AI-caused harms and their diverse individual and collective impacts. Those concerns have helped to make AI-system transparency a foundational element in efforts to increase the scrutiny, contestability and accountability of AI.[1]

These concerns are usefully illustrated by the growing impact of AI on recruitment and employment. In this essential sphere of human life, AI systems are not only emergent tools for work or co-working, but are also tools or agents for employee management and, increasingly, as

* King's College London, Dickson Poon School of Law, Strand, London WC2R 2LS. Address for correspondence: Emails: perry.keller@kcl.ac.uk; tanya.aplin@kcl.ac.uk. Our thanks to the anonymous C.L.J. reviewers and the editor for their much valued comments.

[1] B.G.S. Schor et al., "Mind the Gap: Designers and Standards on Algorithmic System Transparency for Users" in F.F. Mueller et al. (eds.), *CHI 2024: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (New York 2024), 1–16.

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

competitors for work.[2] This is a transformation not just of human work, but also of relations between human and machines within work, in which humans are quantifiable objects of machine attention. In recruitment, for example, AI evaluation and filtering of applicants, which is already based on qualifications and psychometrics, is likely to extend further into AI-inferred personal attributes, such as honesty, commitment and attentiveness.[3]

Undoubtedly, humans will often enjoy the benefits of AI in the workplace, despite being aware that AI systems also carry risks of harm to individuals and to workforces generally.[4] Aside from the consequences of AI-system errors and security breaches, potential risks for job applicants or employees include disinformation, discrimination, deceptive manipulation as well as intimidation or even coercion.[5] Interaction with AI systems through recruitment or employment may also restrict human capacities or opportunities for autonomy.[6]

In view of these risks to individuals, there are also collective concerns about risks of systemic biases that may exclude certain groups from employment or reinforce problematic employee attributes or behaviours in the workplace. These risks may be addressed collectively within the employment context or societally through legislative or regulatory interventions.[7] Nonetheless, the opacity and complexity of AI systems present major challenges for the liberal democratic ideal of effective public participation in governance. How, for example, are employees and job applicants, or those acting on their behalf, to know enough about specific AI systems in the workplace to contest their risks or to secure accountability for their harms through legal or regulatory processes? As we discuss in this article, public participation in AI governance requires innovative forms of public access and transparency throughout AI-system lifecycles as well as forms of AI explanation that aim to empower public participation rather than placate public anxieties.

Consequently, our focus is on the public transparency of AI systems as an essential element in the governance of their risks and on trade-secret claims as barriers to that transparency.[8] The notion of public empowerment through

[2] "The Impact of AI on the Labour Market", available at https://institute.global/insights/economic-prosperity/the-impact-of-ai-on-the-labour-market (last accessed 13 August 2025).
[3] S.M.H. Motlagh, M.H. Rezvani and M. Khounsiavash, "AI Methods for Personality Traits Recognition: A Systematic Review" (2025) 640 Neurocomputing 1.
[4] O. Giuntella et al., "Artificial Intelligence and the Wellbeing of Workers" (2025) 15 Scientific Reports 1.
[5] E. Ferrara, "Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies" (2024) 6 Sci 3; A. Fabris et al., "Fairness and Bias in Algorithmic Hiring: A Multidisciplinary Survey" (2025) 16 ACM Transactions on Intelligent Systems and Technology 1; N. Sheard, "Algorithm-Facilitated Discrimination: A Socio-Legal Study of the Use by Employers of Artificial Intelligence Hiring Systems" (2025) 52 Journal of Law and Society 269.
[6] E. Aizenberg, M.J. Dennis and J. van den Hoven, "Examining the Assumptions of AI Hiring Assessments and their Impact on Job Seekers' Autonomy Over Self-Representation" (2025) 40 AI & Society 919.
[7] See e.g. Commission Regulation (EU) No 1689/2024 (OJ 2024 L 1689 p.1), art. 5(1)(5) ("AI Act").
[8] Defined below in Section II.

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

public knowledge has been expressed in policy catchphrases, such as "the right to know", "the marketplace of ideas" and "the wisdom of the crowd".[9] While these phrases capture different perspectives, they all reflect an ideal of informed and publicly determined action within liberal democratic societies and their market economies. The public right to know embraces principles of informed citizen participation in representative politics, including elections as well as direct involvement in political affairs, such as digital petitions or street demonstrations.[10] In contemporary networked and digitised societies, participatory public action has developed into hybrids of online and real-world life, in which intermediaries have acquired a critical role in accessing and organising information for public-interest purposes.[11] In addition to the agencies of the state, the focus for public contestation is now often on commercially funded Internet platforms and services, which are able to use big data and algorithmic processing resources to structure the public sphere.[12]

In parallel, economic arguments for improving public transparency of AI stem from market-based concerns about innovation, growth and fair competition.[13] These concerns have become a key feature in policy debates about the role of major technology companies in developing and deploying methods that may block new entrants and suppress alternative innovation in the digital economy.[14] The public disclosure of risks of AI-related harms is, consequently, an important tool for both effective democratic participation and competitive innovation. In workplace settings, embedding opaque AI systems in operations and management may, for example, limit employee capacities to contest emerging rules of work while also reinforcing market dominance.

Nonetheless, while public transparency is an essential element within liberal democratic conceptions of governance, it carries risks of significant and potentially irreparable harms. To limit those risks, classes of personal, commercial and state information are routinely protected against public-transparency rights and duties, including trade secrets and commercially confidential information. In addition to these historically

[9] M. Schudson, *The Rise of the Right to Know: Politics and the Culture of Transparency, 1945-1975* (Cambridge, MA 2015).

[10] S. Elstub, "Deliberative and Participatory Democracy" in A. Bächtiger et al. (eds.), *The Oxford Handbook of Deliberative Democracy* (Oxford 2018); OECD, "Innovative Citizen Participation and New Democratic Institutions: Catching the Deliberative Wave", available at https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/06/innovative-citizen-participation-and-new-democratic-institutions_11aa2baf/339306da-en.pdf (last accessed 18 August 2025).

[11] See e.g. R. Modhvadia and O. Field Reid, "Participatory and Inclusive Data Stewardship: A Landscape Review", available at https://www.adalovelaceinstitute.org/report/participatory-inclusive-data-stewardship/ (last accessed 13 August 2025).

[12] A. Applebaum, *Autocracy, Inc.: The Dictators who Want to Run the World* (London 2024).

[13] W.N. Price II and A.K. Rai, "Clearing Opacity through Machine Learning" (2021) 106 Iowa Law Review 775.

[14] OECD, "Artificial Intelligence, Data and Competition", available at https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/05/artificial-intelligence-data-and-competition_9d0ac766/e7e88884-en.pdf (last accessed 13 August 2025).

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

protected classes, there is now an acute public interest in protecting information stored, communicated or produced in networked systems from malicious attacks by tightening technical and organisational controls on access.[15] Consequently, the inherent complexity and opacity of AI systems together with increased security measures have combined with historic concerns about harmful public information disclosures to create overlapping technical and legal obstacles to AI transparency.

Facing these barriers, applicants for work or for promotions in work who suspect AI bias or error may find it near impossible to access and understand the factors that affected an AI-determined negative decision. As Del Castillo and Taes point out:

> In an occupational setting, having access to the code behind an algorithm is not useful per se. What matters to workers is understanding the overall architecture of the AI model, the intended purpose; the context of use, how they are embedded in a system or layers of systems in the workplace; how they are exposed to or which personal data is collected from them.[16]

While AI systems have improved in their capacities to produce explanations of their outputs, significant gaps between such explanations and the comprehension level of non-specialists continue.[17]

Arguments for and against increased public scrutiny of AI systems are, consequently, being fought out in an increasingly dense field of design and operational options for providing different forms of AI transparency for different stakeholders. Importantly, debates about transparency processes for relevant stakeholders are occurring in a contemporary crisis of trust in public and private institutions. The claim for a public right to know is therefore not merely about appropriate information regarding specific AI systems for affected individuals to exercise presented options, it is also a challenge to established legal boundaries between transparency and confidentiality. In such circumstances, trade-secret claims have drawn considerable criticism as unjustifiable and pervasive barriers to the broader demands for public disclosure of AI risks.

Foss-Solbrekk succinctly summarised this groundswell of criticism, arguing that "[t]rade secret law [. . .] obfuscates access to the algorithm and to explanations behind automated decisions, dimming the

[15] E. Seger et al., "Democratising AI: Multiple Meanings, Goals, and Methods" in F. Rossi et al. (eds.), *AIES 2023: Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society* (New York 2023), 715–22.

[16] A.P. Del Castillo and S. Taes, "Artificial Intelligence and Labor Law" in N.A. Smuha (ed.), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (Cambridge 2025), 363.

[17] Q. Jiaming, J. Arguello and Y. Wang, "Understanding the Effects of Explaining Predictive but Unintuitive Features in Human-XAI Interaction" in *FAccT 2025: Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency* (New York 2025), 296–311; K. Haresamudram, S. Larsson and F. Heintz, "Three Levels of AI Transparency" (2023) 56 Computer 93.

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

transparency of the entire system".[18] Yet, despite criticism, the legal protection of trade secrets[19] remains formidable. Building on the historic physical and technical foundations of information control,[20] trade-secret law creates rights and duties to prevent unauthorised acquisition, use or disclosure of the protected information.[21] Where public interests in disclosure and non-disclosure conflict, it is often the case that trade-secret protection prevails. While transparency rights or duties can be used to require public disclosure of trade secrets, this will normally require demonstration of a compelling public interest in disclosure specific to the circumstances. Even here, however, advantages remain with the trade-secret holder, who may control access to the essential information needed to demonstrate that compelling public interest.

In this article, we review the weaknesses of UK and EU public-transparency laws in compelling the disclosure of trade secrets that affect matters of public importance. In that context, we investigate current arguments for reducing the scope of trade-secret protections for AI systems by carving out areas from legal protection that are deemed to be of major public interest, such as information regarding products and services affecting health and safety or decision-making by public authorities. Despite the academic upsurge of support for public-transparency "carve-outs" of this kind, we argue that their evident strengths are considerably outweighed by their weaknesses, which include uncertainty, over-inclusion and ineffectiveness. In general, these proposals run high risks of causing commercial harm without

[18] K. Foss-Solbrekk, "Three Routes to Protecting AI Systems and Their Algorithms under IP Law: The Good, the Bad and the Ugly" (2021) 16 Journal of Intellectual Property Law & Practice 247, 258; see also F. Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Cambridge, MA 2015), 193, 217; S.K. Katyal, "The Paradox of Source Code Secrecy" (2019) 104 Cornell Law Review 1183, 1191, 1237; C.A. Tschider, "Beyond the 'Black Box'" (2021) 98 Denver Law Review 683, 709; C.T. Graves and S.K. Katyal, "From Trade Secrecy to Seclusion" (2021) 109 The Georgetown Law Journal 1337, 1343; A. Kapcyznski, "The Public History of Trade Secrets" (2022) 55 UC Davis Law Review 1367, 1371; S. Lu, "Data Privacy, Human Rights and Algorithmic Opacity" (2022) 110 California Law Review 101, 118–19, 125; O. Kokoulina, "Transparency of Algorithmic Decision-Making: Limits Posed by IPRs and Trade Secrets" in J. Schovsbo (ed.), *The Exploitation of Intellectual Property Rights* (Cheltenham 2023), 51–56.

[19] In this article, when referring to "trade secrets", we acknowledge that there is not a consistent definition across jurisdictions. We take the definition in Article 39(2) of the Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS") as a starting point, i.e. where information is secret, commercially valuable because of that secrecy and where there have been reasonable steps to keep the information secret. However, in referring to "trade secrets" in this article, we also include confidential information that is subject to legal protection.

[20] M. Risch, "Why Do We Have Trade Secrets?" (2007) 11 Marquette Intellectual Property Law Review 26, 43; M.A. Lemley, "The Surprising Virtues of Treating Trade Secrets as IP Rights" (2008) 62 Stanford Law Review 311.

[21] See e.g. EU Parliament and Council Directive (EU) No 943/2016 (OJ 2016 L 157 p.1) ("Trade Secrets Directive"), arts. 4(2)–(3), implemented in the UK via the Trade Secrets (Enforcement, etc.) Regulations 2018, SI 2018/597, reg. 3 ("Trade Secrets Regulations"). Trade-secrets law in the UK is also inextricably linked to the action for breach of confidence: Trade Secrets Regulations, reg. 3(1). The action for breach of confidence requires confidential information, agreement or actual or constructive knowledge that the information is confidential and unauthorised use or disclosure: *Vestergaard Frandsen A/S v Bestnet Europe Ltd.* [2013] UKSC 31, [2013] 1 W.L.R. 1556, at [22]–[23] (Lord Neuberger, with whom Lord Clarke, Lord Sumption, Lord Reed and Lord Carnwath agree).

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

significantly developing legal or technical capacities for public scrutiny and contestation of AI risks.

In our view, there are more effective and appropriate solutions to be found through innovations in public-transparency law and practices that meet the technical and organisational challenges of AI transparency. In general terms, we argue that the vitally important public right to know should be reconsidered and adapted to the AI era. We therefore suggest three areas for further research and development: incorporating timely third-party review of trade-secret claims into developing public-transparency challenge and contestation processes for AI systems, which would remove some of the key unilateral advantages of trade-secret holders; widening the scope of vetted third-party participation in standard setting and compliance assessment within the trade-secrets barrier; and, developing public authority or agency responsibilities to report and disclose matters of public interest in the course of AI regulatory supervision and enforcement, while creating opportunities to contest the reasons for those disclosure choices. Throughout these areas, timely and authoritative assessment of the scope of trade-secret claims and conflicting public-interest claims will be key.

To make our argument, this article is structured as follows: Section II introduces "public transparency" as a specific variant of the concept of transparency and explains its relationship with the contrasting notion of "regulatory transparency". Section III explains the definitive features of established public-transparency regimes, which continue to dominate conceptual thinking about public-transparency rights and duties. In Section IV, we discuss the disadvantages of proposals to introduce public disclosure presumptions or carve-outs in areas of high public interest. Section V explains the contemporary evolution of public transparency towards narrower targeting of specific disclosure needs and the strengths and weaknesses of this model. In Section VI, we argue that the threat that trade-secret claims pose for the public transparency of AI systems needs to be resolved through innovations in AI transparency concepts and practices and propose areas for development.

II. Regulatory Transparency and Compelled Disclosure

Public transparency – a term we use in this article to refer to the unrestricted use and sharing of information for lawful purposes – is the opposite of trade secrecy.[22] Public information use and sharing thus occurs outside the legal barrier that guards trade-secret claims against unauthorised disclosures.

[22] The concept of transparency is ubiquitous in legal, policy and other disciplines and, consequently, requires careful definition. In this article, we use the terms "public transparency" and "regulatory transparency" as essential for our purposes, without criticism of alternative terms used in the literature, which have different applications.

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

Within that barrier, there is, however, a highly flexible sphere of transparency for privileged participants. These include employees, commercial partners and other stakeholders as well as auditors, regulators and other law enforcement authorities. The potential for trade-secret barriers to accommodate third parties undoubtedly provides openings for public-interest scrutiny of trade-secret information and even its public disclosure in redacted form through intermediaries. Yet, disclosures to third parties within the trade-secret barrier are not without risk. Aside from unauthorised sharing or leaks, once trade-secret information is widely shared it may lose the essential element of secrecy that is required for legal protection.[23]

On one level, public transparency stands in obvious contrast to disclosure to third parties within the trade-secrets barrier, including what we refer to as "regulatory transparency". This form of transparency occurs either through voluntary information disclosure to government authorities or through the exercise of the state's legal powers to compel information disclosures. These include a wide array of powers to search property, including electronic networks and databases, to seize material, including data, and to compel individuals to attend interviews. The powers that enable regulatory transparency descend from the historic exercise of coercive state powers to enter premises, confiscate possessions and question individuals, which liberal democracies now restrict substantively and procedurally. In the UK, for example, police forces and designated law enforcement bodies are authorised to conduct searches and interviews under the Police and Criminal Evidence Act 1984.[24] Other regulators, such as the Financial Conduct Authority and the Prudential Regulation Authority, have bespoke powers to obtain search warrants and compel interviews.[25] While the exercise of these powers is open to legal challenge, their effect is to render trade-secret rights largely irrelevant to a lawful investigation or enforcement.

Aside from confidentiality commitments to disclosing parties, regulatory agencies and other public authorities are routinely subject to strict confidentiality duties that limit further disclosure. In addition to general confidentiality principles governing their operations and sometimes specific statutory obligations,[26] public authorities in the UK may enforce

[23] This is a consequence of the definition of "trade secret" in Trade Secrets Directive, art. 2 and Trade Secrets Regulations, reg. 2, and the notion of "confidential information" in English law, on which see T. Aplin et al., *Gurry on Confidence*, 2nd ed. (Oxford 2012), at [5.14]–[5.72].

[24] Police and Criminal Evidence Act 1984, s. 8; Police and Criminal Evidence Act 1984 (Application to Revenue and Customs) Order 2015, s. 3.

[25] Financial Services and Markets Act 2000, ss. 171–173, 122D, 176; see also e.g. Health and Safety at Work etc. Act 1974, s. 20; Environmental Protection Act 1990, s. 34b; Environment Act 1995, s. 108; Proceeds of Crime Act 2002, s. 47A; and Public Authorities (Fraud, Error and Recovery) Bill, Clause 7 (currently before Parliament).

[26] See e.g. *R (on the application of Ingenious Media Holdings plc) v Commissioners for Her Majesty's Revenue and Customs* [2016] UKSC 54, [2016] 1 W.L.R. 4164.

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

confidentiality through employment contracts and codes of conduct.[27] In the EU, comparable confidentiality obligations for regulators are typically included in legislation that creates information disclosure duties or powers. For example, the Artificial Intelligence Act ("AI Act") requires, among its other transparency obligations, providers of general-purpose AI models to maintain up-to-date technical documentation of their models, which must be provided on request to the new EU AI Office and national competent authorities.[28] In exercising their powers, AI Act regulatory bodies must, however, take due account of the rights and interests of the information providers, including the protection of confidential information, such as trade secrets.[29]

Despite powers to compel the confidential disclosure of trade-secret information, regulatory transparency is a close cousin to public transparency. Public authorities and agencies are, first, primary information sources for Freedom of Information ("FOI") requests. Consequently, public bodies have a key role in determining whether the balance of opposing public interests favours the disclosure of trade secrets they may hold. Additionally, when exercising scrutiny and investigation functions, they frequently act as transparency intermediaries, providing degrees of essential public disclosure enabled by privileged access to trade secrets.[30] As we discuss further, the notion of using the state as an instrument for AI public transparency extends to the use of government bargaining powers to require the public disclosure of trade secrets when contracting with AI application providers across many state functions.[31]

III. Public Transparency's Trade-Secrets Deference Challenge

As compared with regulatory powers to compel information disclosure, public-transparency regimes provide much more limited potential for compelling the disclosure of information subject to trade-secret protection. Within these regimes, such as FOI law, disclosure rights and duties are structured to protect overlapping, and even aggregated, classes of personal, commercial and governmental information from being accessed or shared.[32] Procedurally, this deference operates in the complex

[27] See e.g. The Police (Conduct) Regulations 2020, sched. 2; College of Policing, "Police Information and Records Management Code of Practice", available at https://www.college.police.uk/guidance/police-information-and-records-management-code-practice (last accessed 14 August 2025).

[28] AI Act, art. 53(1).

[29] Ibid., arts. 53(7), 78.

[30] See C.J. Morten, "Publicizing Corporate Secrets" (2023) 171 University of Pennsylvania Law Review 1319.

[31] E.A. Rowe and N. Prior, "Procuring Algorithmic Transparency" (2022) 74 Alabama Law Review 303, 343; see also A. Sanchez-Graells, *Digital Technologies and Public Procurement* (Oxford 2024), querying whether public procurement can act as an effective means for regulating technologies, including AI.

[32] *Department for Business and Trade v The Information Commissioner* [2025] UKSC 27, [2025] 1 W.L.R. 3456.

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

interplay between the public-interest defences for unauthorised disclosure built into trade-secrets law and public disclosure rights and duties located outside trade-secrets law.

While not property rights as such, trade secrets are an important element within intellectual property rights regimes and are secured not only by domestic laws, but also by EU law and international trade obligations, importantly including the Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS").[33] In many jurisdictions, such as the UK and some other common law countries or territories, this protection occurs through legal duties of confidence, which if breached may result in an action for breach of confidence and an award of damages.[34] In the UK, the long-standing protection of trade secrets through duties of confidentiality was augmented by domestic implementation of the EU Trade Secrets Directive, which prohibits unauthorised acquisition, use or disclosure of trade secrets.[35]

In addition to legal protection against unauthorised disclosure, trade-secret claims enjoy further advantages over demands for more extensive AI public transparency. In contrast to patented inventions and copyright works, information protected as a trade secret is not made public precisely because of its secrecy and thus, unlike patents, is not registered. Accordingly, unsound or inflated claims of trade-secret protection, which are often outwardly indistinguishable from legitimate ones, can be asserted against public access demands without prior third-party evaluation.[36] Without resort to third-party review and possible invalidation, unjustifiable claims cannot be overcome.[37] As Graves and Katyal have argued, trade-secret "claimants can choose their own narrative of trade secrecy to serve whatever their immediate goal may be".[38] Even when unsound or inflated assertions of trade secrecy are made in good faith, such as those regarding new technologies, the self-judged nature of an initial trade-secret claim advantages the holder of the information.[39]

While AI developers may, therefore, resist access to their training data on the basis that they are a trade secret, this claim is weak where training data have been drawn from Internet scraping, large-scale publicly accessible

[33] T. Aplin, "Trade Secrets and Property" in C. Geiger (ed.), *Research Handbook on Human Rights and Intellectual Property* (London 2015), 421–37.
[34] See also Aplin et al., *Gurry on Confidence.*
[35] See Trade Secrets Regulations; T. Aplin and R. Arnold, "UK Implementation of the Trade Secrets Directive" in J. Schovsbo, T. Minssen and T. Riis (eds.), *The Harmonisation and Protection of Trade Secrets in the EU: An Appraisal of the EU Directive* (London 2020), 65–85.
[36] Graves and Katyal, "From Trade Secrecy to Seclusion", 1350.
[37] Katyal, "Paradox of Source Code Secrecy", 1214; R. Brauneis and E.P. Goodman, "Algorithmic Transparency for the Smart City" (2018) 20 Yale Journal of Law & Technology 103, 153.
[38] Graves and Katyal, "From Trade Secrecy to Seclusion", 1351.
[39] T. Aplin et al., "The Role of EU Trade Secrets Law in the Data Economy: An Empirical Analysis" (2023) 54 International Review of Intellectual Property and Competition Law 826, 836.

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

datasets or from data generated from smart machines.[40] In the employment context, for example, one can imagine AI interview tools that have been trained on publicly accessible information about an organisation, such as its values, the skills and expertise offered by its workforce, and the services it provides, along with publicly accessible datasets of mock interviews in order to facilitate sentiment analysis.[41] Or we can envisage AI tools aimed at increasing employee productivity in relation to home repair services being trained on or applied to dynamic data about traffic conditions, distances travelled and complexity of service provided. While such training data may be valuable, it is doubtful that they are secret or that their value is attributable to any secrecy. Yet, where employee concerns about bias or error in those AI assessments arise, the claim of trade secrecy sets up a barrier to public disclosure.

The public-interest exceptions contained in trade-secrets laws, such as the Trade Secrets Directive, are not well adapted to forcing public disclosure as they are primarily defensive in nature. Where disclosure is not voluntary, there is no mechanism *within* trade-secrets law to *compel access* to information. Instead, the law legitimises or justifies instances where acquisition, use or disclosure of trade secrets to third parties, including the general public, occurs without the consent of the trade-secret holder.[42] These provisions protect unauthorised disclosures that serve several broad public-interest purposes, including the exercise of the right to freedom of expression or revealing misconduct, wrongdoing or illegal activity for public-interest reasons.[43] Yet, the structure of these defences is to protect unauthorised disclosure by individuals or entities who *already have access* to trade-secret-protected information.

For public transparency of AI, the problem is not legal protection for public disclosure but how to compel disclosure of the information. In the normal course, neither individuals nor collective organisations are likely to have internal access to information asserted to be trade secrets, such as data, hyperparameters or weights used in the training process of an AI model or the AI model itself. There is, consequently, a close conceptual and practical alignment between public-interest defences in trade-secrets law and public-interest protections for whistle-blowers from employment dismissal and other retribution for unauthorised disclosure in breach of employment obligations. While offering genuine protections, these laws

[40] S. Sandeen and T. Aplin, "Trade Secrecy, Factual Secrecy and the Hype Surrounding AI" in R. Abbott (ed.), *Research Handbook on Intellectual Property and Artificial Intelligence* (London 2022), 442–59.

[41] Such as the M.I.T. Interview Dataset: see M. Shifan P. et al., "Automated Analysis and Behavioural Prediction of Interview Performance using Computer Vision" in *2022 IEEE 19th India Council International Conference (INDICON)* (Kochi 2022), 951–57.

[42] R. Dreyfuss, "Trade Secrets and Deep Secrets" in G.B. Dinwoodie and A. Ohly (eds.), *Research Handbook on Unfair Competition and Passing Off* (Cheltenham forthcoming), available at https://ssrn.com/abstract=4918972 (last accessed 25 October 2025) refers to the information that is *not* revealed through limits or exceptions to trade-secret protection as "deep secrets".

[43] Trade Secrets Directive, art. 5.

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

also aim to control the extent of whistleblower disclosures of confidential information.[44]

On the other hand, trade-secret law exceptions for unauthorised disclosure and public-transparency regimes that create access rights are not as clearly aligned. Conventional public-transparency regimes, such as the FOI right of access, share three common structural features: public disclosure rights; exclusions from those rights for protected classes of information, including trade secrets; and, public-interest-based exceptions to some of those class exclusions. Primary rights to public disclosure tend to be robustly structured, permitting unlimited sharing and not requiring proof of an appropriate motive. That robustness is, however, invariably offset by broad exclusions for protected classes of information, effectively creating default non-disclosure barriers for these classes. The third common feature, public-interest-based exceptions to those broad exclusions, tends to be limited and narrowly construed. While the non-disclosure of trade secrets is thus open to narrow public-interest exceptions, other classes, such as classified government secret information, tend to be beyond right-to-know-based compelled disclosure.[45]

We turn now to consider the operation of these common features in two foundational public-transparency regimes: access to judicial proceedings and FOI. The experience of these regimes continues to shape our understanding of how conflicts between public interests in transparency and secrecy should be managed and resolved.

A. Open Justice

Often referred to as "open justice" in UK law, public access to court proceedings and the unrestricted sharing of information made public in those proceedings is a major precedent for the design of public-transparency regimes.[46] As a form of public scrutiny of a state institution, open justice reflects public transparency's traditional focus on governmental authority and power. Its importance as a specialised public-transparency regime is also indirectly recognised in the UK Freedom of Information Act ("FOIA"), which absolutely excludes information held in relation to court proceedings.[47] This, in effect, respects the right of the courts to manage their own form of public transparency.

[44] Employment Rights Act 1996, Part IVA, ss. 43A–43K, introduced by the Public Interest Disclosure Act 1998, s. 1. See also EU Parliament and Council Directive (EU) No 1937/2019 (OJ 2019 L 305 p.17) ("EU Whistleblowing Directive"). Regarding the balance of interests in whistleblower disclosures under the European Convention of Human Rights, see *Hrachya Harutyunyan v Armenia* (Application no. 15028/16), Judgment of 27 August 2024, not yet reported, at [44]. On the interaction between trade-secrets and whistleblower protection, see Trade Secrets Directive, rec. 20 and EU Whistleblowing Directive, rec. 98.

[45] See e.g. UK Official Secrets Act 1989.

[46] *Scott v Scott* [1913] A.C. 417 (H.L.).

[47] Freedom of Information Act 2000, s. 32.

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

In the UK, the courts have moved over time to entrench and broaden the public-interest rationales of open justice. The Supreme Court has, for example, affirmed the connection between open justice and the role of media reporting of matters of general interest,[48] linking public transparency of the state and the notion that social forces have a role in fostering accountability. Open justice has also evolved in response to changes in the ways that courts and litigants communicate information outside of open court proceedings, allowing greater public access to background evidence and submissions that are essential to understanding those proceedings

Although access to EU court proceedings has a different legal basis, there are important commonalities with UK law, including the reinforcing role of Article 6 of the European Convention on Human Rights ("ECHR"), concerning the right to a fair and public hearing. Within EU law, that fundamental right is also protected via Article 47 of the EU Charter of Fundamental Rights, concerning the principle of public access to the courts.[49] EU courts are also largely exempted from EU FOI legislation, which defers to their internal rules governing public access.[50] While this exemption under the EU FOI Regulation is in principle limited by a public-interest-based exception, the Court of Justice of the European Union ("CJEU") has used the EU treaties to interpret that exemption in broad terms.[51] Efforts to create compelled public disclosure duties for documents submitted to EU courts by parties to litigation or interested third parties have, moreover, been judicially resisted.[52]

Inevitably, the principle of public knowledge of judicial processes does not include unconditional access to information protected as trade secret.[53] When considering trade-secret claims that are relevant to judicial proceedings, courts will invariably require confidential disclosure of that information to other parties of the litigation where necessary in the interests of justice.[54] Trade secrets and other classes of protected information are, however, routinely exempted from disclosure in open

[48] *Cape Intermediate Holdings Ltd. v Dring (for and on behalf of Asbestos Victims Support Groups Forum UK)* [2019] UKSC 38, [2020] A.C. 629, at [14], [45] (Lady Hale).

[49] Charter of Fundamental Rights of the EU (OJ 2012 C 326 p.391), art. 47 ("CFR").

[50] Consolidated Treaty on the Functioning of the European Union (OJ 2012 C 326 p.47), art. 15(3) ("TFEU"); Council Regulation (EC) No 1049/2001 (OJ 2001 L 145 p.43), art. 4(2) ("EU FOI Regulation").

[51] Judgment of 21 September 2010, *Sweden v Association de la presse internationale A.S.B.L. (A.P.I.) and European Commission*, C-514/07 P, C-528/07 P and C-532/07 P, EU:C:2010:541, at [79], [83]–[84].

[52] Regulation (EU, Euratom) 2024/2019 of the European Parliament and of the Council of 11 April 2024 amending Protocol No 3 on the Statute of the Court of Justice of the European Union, rec. (4); CJEU Decision of 26 November 2019 concerning public access to documents held by the Court of Justice of the European Union in the exercise of its administrative functions (OJ 2020 C 45 p.2); I. Fevola and S. Montaldo, "Access to Written Submissions in Preliminary Reference Proceedings: An Evaluation of the CJEU Statute Reform and Its Contribution to Open Justice" (2025) 10 European Papers, 357, 365–69.

[53] See Aplin and Arnold, "UK Implementation", 81.

[54] See e.g. *Omers Administration Corporation v Tesco Plc* [2019] EWHC 109 (Ch), at [79] (Hildyard J.).

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

court unless a compelling public-interest justification is demonstrated. Indeed, where deemed necessary, disclosures between parties may be strictly limited to a litigant's legal representatives, who are subject to disciplinary remedies for breaches of confidentiality.[55] These restrictions on the right of the public to report on proceedings held in open court are subject to standards of legitimacy, necessity and proportionality, yet such restrictions are also routinely upheld.[56]

The treatment of trade secrets in relation to open justice illustrates several key issues arising in public transparency. First, the courts themselves are empowered to reject unsound or inflated claims to trade-secret protection relied on by litigants. This ready access to impartial third-party adjudication in open justice contexts not only demonstrates its importance in addressing the obfuscating effects of self-judged trade-secrets claims, but also the weaknesses of other public-transparency regimes where impartial third-party assessment is external to the process.

Second, the courts are also able to determine whether there is a compelling public interest in the disclosure of legitimately protected trade secrets in open court. On one level, this simply asks whether public disclosure is necessary to serve the purposes of open justice, which primarily concern public understanding and scrutiny of the justice system.[57] Trade-secret claims in litigation are, however, also open to the question of whether the public-interest exceptions internal to trade-secrets law are satisfied. A court may, therefore, determine that the public interest in protecting the trade-secret claim at issue is outweighed by a sufficiently cogent public interest in disclosure.[58]

B. Freedom of Information

While FOI laws were adopted long after the recognition of open justice as a legal principle, FOI is in many respects the definitive public-transparency right.[59] As the UK Government declared in its 1997 White Paper introducing the proposed FOIA, "[o]penness is fundamental to the political health of a modern state" and "[u]nnecessary secrecy in government leads to arrogance in governance and defective decision-making".[60] The CJEU has similarly stated that the right of access

[55] "The King's Bench Guide: A Guide to Working Practices of the King's Bench Division with the Royal Courts of Justice", at [3.37], available at https://www.judiciary.uk/wp-content/uploads/2025/04/35.16_JO_Kings_Bench_Division_Guide_2025_WEB4.pdf (last accessed 25 October 2025).

[56] *Guardian News and Media Ltd. v Incedal* [2016] EWCA Crim 11, [2016] 1 W.L.R. 1767; Justice Nicklin, "Transparency & Open Justice – Opportunities and Challenges", available at https://www.judiciary.uk/speech-by-mr-justice-nicklin-transparency-open-justice-opportunities-and-challenges/ (last accessed 14 August 2025).

[57] *Cape Intermediate Holdings v Dring* [2019] UKSC 38, at [37] (Lady Hale).

[58] In the context of breach of confidence, see Aplin et al., *Gurry on Confidence*, ch. 16.

[59] Schudson, *Rise of the Right to Know*.

[60] HM Government, "Your Right to Know: The Governments Proposals for a Freedom of Information Act", Cm. 3818 (London 1997), Foreword and at [1.1].

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

"enables citizens to participate more closely in the decision-making process and guarantees that the administration enjoys greater legitimacy and is more effective and more accountable to the citizen in a democratic system".[61]

Following the three common features described above, the UK's FOIA creates a general right to the public disclosure of information held by designated public authorities, introducing a powerful legislated skew towards the scrutiny of public power. The FOIA right is thus only indirectly applicable to private entities where the supply of goods or services or other interactions with the state involves sharing trade secrets or private information with public bodies.[62] Other FOI regimes rest on a similar public disclosure right, although they may be constructed on a narrower basis. For example, the UK Environmental Information Regulations 2004 ("EIR"), intended to implement EU law, only create a right to information falling within the defined sphere of "environmental information".[63] The EU FOI regime, established by Regulation (EC) No 1049/2001 and subsequently underpinned by Article 42 of the Charter of Fundamental Rights ("CFR"), creates a right of access only to "documents" held by EU institutions and not information in any wider meaning of that concept.[64]

Despite such differences, FOI regimes realise important elements of the public right to know, including the link between free public debate and democratic participation and the motive-blind disclosure of state information through FOI requests. Provided there is effective sharing through the media or other intermediaries, the release of information obtained through FOI requests potentially contributes to the democratic and economic goals of public transparency. Those expected benefits, however, occur alongside the utility of FOI rights for pursuit of private interests,[65] which raises problematic fit for purpose questions about the beneficiaries and justifications for FOI regimes.[66]

[61] Judgment of 9 November 2010, *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, C-92/09 and C-93/09, EU:C:2010:662, at [68]. See also Judgment of 22 February 2022, *Stichting Rookpreventie Jeugd and Others v Staatssecretaris van Volksgezondheid, Welzijn en Sport*, C-160/20, EU:C:2022:101, at [35].

[62] FOIA, s. 1. See also Information Commissioner's Office, "Outsourcing Oversight? The Case for Reforming Access to Information Law", at [2.3], available at https://ico.org.uk/media2/migrated/2614204/outsourcing-oversight-ico-report-to-parliament.pdf (last accessed 13 August 2025).

[63] Environmental Information Regulations 2004, SI 2004/3391; EU Parliament and Council Directive (EC) No 4/2003 (OJ 2003 L 41 p.26); Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters 2003 (UN Treaty Series, vol. 2161 p.447) ("Aarhus Convention").

[64] EU FOI Regulation; Judgment of 29 September 2021, *AlzChem Group A.G. v European Commission*, T-569/19, EU:T:2021:628, at [104]; see Treaty of the European Union ("TEU"), arts. 1, 10; see also TFEU, art. 15.

[65] M.B. Kwoka, "FOIA, Inc." (2016) 65 Duke Law Journal 1361, 1414; M.B. Kwoka, "First-Person FOIA" (2018) 127 Yale Law Journal 2204, 2244.

[66] D. Pozen and M. Schudson, "Introduction: Troubling Transparency" in D. Pozen and M. Schudson (eds.), *Troubling Transparency: The History and Future of Freedom of Information* (New York 2018), 1–10; J.K. Bannister, "Accountability or Participation? Disentangling the Rationales for FOI Access to Deliberative Material" (2015) 2 Revue Internationale des Gouvernements Ouverts 327.

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

Building on the general-purpose access right, liberal democratic FOI regimes typically create structured balances between the conflicting public interests in disclosing state-controlled information and protecting classes of sensitive information, including trade secrets, absolutely or conditionally from disclosure.[67] Nonetheless, non-disclosure of information protected by a trade-secret claim can be challenged by demonstrating that the claim does not satisfy trade-secret criteria or there are public-interest reasons to compel disclosure.

In the UK, section 41 of FOIA creates an exemption for information provided in confidence, whereas section 43 creates exemptions for trade secrets and information prejudicial to commercial interests. In comparison, the EU FOI Regulation has a simpler structure, establishing two general class exclusions from the right of access to EU institutional documents.[68] The narrower, first category concerns documents relating to the core interests of the state. The second category, found in Article 4(2), includes refusal of access where disclosure would undermine the protection of "commercial interests of a natural or legal person, including intellectual property". As discussed below, while the exemptions in the EU's and UK's FOI regimes are structured differently, they both typically favour the commercial interests of trade-secret holders over the public interest in disclosure.

Outwardly, FOI regimes create an efficient method for subjecting self-judged trade-secrets claims to third-party assessment and reasoned decision by a public authority when public disclosure is sought. The full impartiality of that third-party review, however, cannot be assured where the relevant public authority is directly or indirectly an interested party. This may occur, for example, where the trade-secret holder is an established or favoured service provider to a public authority. Yet, even without such a relationship, the public authority may have institutional reasons to favour non-disclosure. The UK Medicines & Healthcare products Regulatory Agency ("MHRA"), for example, has cited its own commercial interests as a factor in its decisions regarding section 43 of FOIA.[69] Institutional partiality may also have been present in the important EU FOI litigation in *Breyer v European Research Executive Agency (REA)*.[70] The Agency adopted an expansive view of what documentation fell within the scope of the exemption than was

[67] Freedom of Information Act 2000, ss. 41, 43.
[68] EU FOI Regulation.
[69] See e.g. "Freedom of Information Responses from the MHRA: 12 February 2024, FOI 24/050", available at https://assets.publishing.service.gov.uk/media/669e2376ce1fd0da7b592994/FOI_24-050_final_redaction.pdf (last accessed 25 October 2025).
[70] Judgment of 15 December 2021, *Patrick Breyer v European Research Executive Agency (REA)*, T-158/19, EU:T:2021:902; Judgment of 7 September 2023, *Patrick Breyer v European Research Agency (REA)*, C-135/22 P, EU:C:2023:640.

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

subsequently established through the applicant's pursuit of administrative and then judicial review.

C. Overriding Public Interest – Specific and General Interests

The rules regarding initial presumptions favouring disclosure or non-disclosure of trade secrets are markedly different in the EU and UK FOI regimes. The EU FOI Regulation provides that the general public interest in transparency in governmental affairs is not, by itself, sufficient to show an overriding public interest in the compelled disclosure of trade secrets.[71] As the CJEU reaffirmed in 2023, "general considerations alone are not capable of establishing that the principle of transparency is of particularly pressing concern".[72]

Critically, section 43 of UK FOIA is a qualified exemption subject to the Act's public-interest balancing test, in which the general public interest in disclosure of information held by public authorities in principle outweighs the public interest in non-disclosure expressed by the exemption. Nonetheless, outcomes in practice regarding trade-secret disclosure are closer to the EU standard than this formal difference implies. To change the balance in favour of non-disclosure under the FOIA public-interest test, it is necessary to show that "disclosure of the information would or would be likely to have a prejudicial effect".[73] That is, however, a low threshold in most trade-secrets cases, even taking into account that the prejudice must be "real and significant, more than hypothetical or remote".

To be protected under section 43, a trade secret is by definition "information, which, if disclosed to a competitor, would be liable to cause real (or significant) harm to the secret's owner".[74] That definition gives a trade-secret claim a substantial head start in showing the requisite prejudice. Assuming, for example, that a commercial provider of AI services has shared secret, commercially valuable information with a public authority subject to FOI access rights, it would not be difficult to show that the provider would suffer a loss of competitive advantage if such information became publicly available.

Consequently, once it is established that the requested information is a protected trade secret, the presumption in favour of public disclosure is

[71] EU FOI Regulation, art. 4(2).

[72] Judgment of 15 December 2021, *Breyer v European Research Agency*, at [75]; Judgment of 23 January 2017, *Association Justice & Environment, z.s. v European Commission*, T-727/15, EU:T:2017:18, at [79]: "as regards the arguments relating to the principles of transparency and democracy, it must be noted that such general considerations are not capable of demonstrating the existence of an overriding public interest in disclosure of the requested documents."

[73] See ICO, "The Public Interest Test", available at https://ico.org.uk/for-organisations/foi/freedom-of-information-and-environmental-information-regulations/the-public-interest-test/ (last accessed 13 August 2025).

[74] *Department for Work and Pensions v Information Commissioner* [2010] UKFTT 683 (GRC), at [67]–[69].

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

easily, if not automatically, overcome.[75] In that situation, like the EU FOI rule, the requesting party must then demonstrate a specific public interest that is sufficiently compelling to outweigh the public interest in preventing the likely harms of disclosure. While also based on an initial presumption favouring disclosure, the balancing test for the parallel UK Environmental Information Regulations exception covering trade secrets has a similarly low threshold for showing sufficient harm to outweigh that presumption.[76]

Where trade-secret-protected information disclosed to a public authority is covered by an overlapping duty of confidentiality, a FOIA request will also need to meet the higher bar of section 41. Here, however, the question of whether there is a public interest in disclosure that is sufficiently compelling to displace the public interest in protecting confidential information only arises indirectly. As an absolute exemption, section 41 excludes direct consideration of that question. Nonetheless, the section only protects actionable breaches of confidence, which requires consideration of whether there is a relevant public interest in disclosure that vitiates actionability. As a final twist, that assessment presumes the public interest in maintaining confidentiality will prevail unless outweighed by a specific public interest in disclosure that goes beyond the general public interest in transparency of governmental information and outweighs any harms that may result.[77]

As critics point out, there are potentially insurmountable practical difficulties in demonstrating a compelling, specific public interest in disclosure of trade-secret-protected information.[78] Without prior knowledge of the protected information, the validity challenge will often fail for lack of sufficient information to demonstrate a specific public interest that outweighs the potential commercial harms of public disclosure. An allegation of bias or error in AI-determined recruitment or promotion outcomes would, for example, require considerable evidence linking the AI tools involved to demonstrably clear and otherwise

[75] See e.g. application of the trade-secrets exemption in "Freedom of Information Responses from the MHRA". A review of MHRA FOIA decisions – see J. Grigg et al., "Transparency of the UK Medicines Regulator: Auditing Freedom of Information Requests and Reasons for Refusal" (2019) 24 BMJ Evidence-Based Medicine 20 – concluded that "[d]espite being the most commonly cited provision in our audit [s. 43], when the full response was available to analyse, the weight of public interest was never determined to overrule this exemption".

[76] See ICO, "Confidentiality of Commercial or Industrial Information (Regulation 12(5)(e))", at [72]–[73], available at https://nbn.org.uk/wp-content/uploads/2016/03/eir_confidentiality_of_commercial_or_industrial_information.pdf (last accessed 13 August 2025).

[77] See ICO, "Section 41 – Information Provided in Confidence", available at https://ico.org.uk/for-organisations/foi/freedom-of-information-and-environmental-information-regulations/section-41-information-provided-in-confidence/ (last accessed 25 October 2025).

[78] M. Dahlberg and D. Wyatt, "Is there a Public Interest in Knowing What Is Going On in Society? A Comparative Study of the European Courts" (2016) 26 Maastricht Journal of European and Comparative Law 691, 708; D. Wyatt, "The Anaemic Existence of the Overriding Public Interest in Disclosure in the EU's Access to Documents Regime" (2020) 21 German Law Journal 686, 696.

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

unexplained biased or wrong outcomes before a public-interest disclosure argument might prevail.

Despite the disproportionate advantage bestowed on trade-secret holders when the requester has the onus of evidencing an overriding specific public interest, this feature has survived the European constitutionalisation of the FOI disclosure right. Although the EU FOI Regulation was adopted before the EU Charter of Fundamental Rights, the CJEU has not considered that this requirement in the regulation is contrary to Article 42 of the Charter, which recognises the public right to access EU documents. At best, the Charter has heightened the importance of any factors associated with the exercise of fundamental rights to freedom of expression and information when balancing public interests in disclosure and non-disclosure.[79]

Recognition of a public right of access to information under Article 10 of the ECHR, relating to freedom of expression, has also failed to transform the established limits of public disclosure. In its ground breaking decision in *Magyar Helsinki Bizottság v Hungary* in 2016, the Grand Chamber of the European Court of Human Rights ("ECtHR") confirmed that Article 10 neither obliges a state party to collect and disseminate information nor confers on the individual a right of access to information held by a public authority.[80] Notwithstanding that general principle, the court also found that an information access right does arise under Article 10 when access to state-held information is instrumental to the exercise of the right to freedom of expression, setting out several indicative criteria for when individuals or entities acting in public or social watchdog roles may enjoy this right.[81] These criteria include the purpose of the information request; the nature of the information sought; the role of the applicant; and whether the information is readily available. The resulting fact-specific balancing test hinges on whether there are sufficient preponderant factors favouring public disclosure.[82] The UK Supreme Court has yet to be asked to re-consider the position in UK law in light of *Magyar Helsinki Bizottság v Hungary*, which the Court of Appeal has recently declined to examine.[83]

The established balancing principles regarding public disclosure and trade secrets recognised in *Magyar Helsinki Bizottság* are also undisturbed by the Council of Europe's new Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. According to the treaty's Explanatory Report, its Article 8

[79] Judgment of 15 December 2021, *Breyer v European Research Agency*, at [3]: "Openness contributes to strengthening the principles of democracy and respect for fundamental rights as laid down in Article 6 of the EU Treaty and in the Charter of Fundamental Rights of the European Union."
[80] *Magyar Helsinki Bizottság v Hungary* (2020) 71 E.H.R.R. 2, at [156].
[81] Ibid., at [157]–[170].
[82] Ibid., at [197].
[83] *R (on the application of Tortoise Media Ltd.) v Conservative and Unionist Party* [2025] EWCA Civ 673, [2025] 1 W.L.R. 4186, at [51] (Singh L.J.).

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

"adequate transparency" obligations remain subject to balancing principles where competing interests are affected.[84] Developments in international human rights law regarding rights of access to information have paralleled developments in the Council of Europe also without breaking significant new ground. The International Covenant on Civil and Political Rights (ICCPR) Human Rights Committee has declared that ICCPR, art. 19, para. 2 "embraces a right of access to information held by public bodies" and that "[a]uthorities should provide reasons for any refusal to provide access to information".[85] In other words, the Article 91(3) legitimate restrictions on national security or public order or in the interests of "the rights or reputations of others" apply.[86]

IV. Proposals for Cutting Back Trade-Secret Protections

In the face of transparency mechanisms structured to favour the non-disclosure of trade secrets, proponents of a fundamental reform of trade-secret protection argue that public-transparency law undervalues the general importance of public transparency.[87] Proposed alternatives would dispense with situation-specific public-interest balancing in selected areas of public concern and instead envision broad legislated presumptions of public disclosure in those areas.

These proposed transparency carve-outs identify diverse areas where trade-secrets protection could be narrowed, including governmental functions or public services,[88] products or services offered to consumers,[89] health and safety,[90] environment[91] or employment conditions.[92] These proposals,

[84] Council of Europe, "Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law" (Council of Europe Treaty Series – No. 225), at [62], available at https://rm.coe.int/1680afae67 (last accessed 14 August 2025).

[85] "General Comment No. 34 on Article 19 Freedoms of Opinion and Expression" (CCPR/C/GC/34), paras. 18–19, available at https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no34-article-19-freedoms-opinion-and (last accessed 25 October 2025); European Union Agency for Fundamental Rights, "Human Rights Committee, General Comment No. 34 (2011) – Article 19 Freedoms of Opinion and Expression", available at https://fra.europa.eu/en/law-reference/human-rights-committee-general-comment-no-34-2011-article-19-freedoms-opinion-and (last accessed 14 August 2025).

[86] P.M. Taylor, *A Commentary on the International Covenant on Civil and Political Rights: The UN Human Rights Committee's Monitoring of ICCPR Rights* (Cambridge 2020), 538–78.

[87] K. Foss-Solbrekk, "Searchlights across the Black Box: Trade Secrecy versus Access to Information" (2023) 50 Computer Law & Security Review 1.

[88] D.S. Levine, "Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure" (2007) 59 Florida Law Review 135, 191; Brauneis and Goodman, "Algorithmic Transparency for the Smart City", 165; M. Busuioc, D. Curtin and M. Almada, "Reclaiming Transparency: Contesting the Logics of Secrecy within the AI Act" (2023) 2 European Law Open 79, 100.

[89] A. Kapczynski, "The Public History of Trade Secrets" (2022) 55 UC Davis Law Review 1367, 1436–67.

[90] J.E. Zink, "When Trade Secrecy Goes Too Far: Public Health and Safety Should Trump Corporate Profits" (2018) 20 Vanderbilt Journal of Entertainment and Technology law 1135, 1172; A. Durkin et al., "Addressing the Risks that Trade Secret Protections Pose for Health and Rights" (2021) 23 Health and Human Rights 129.

[91] D.C. Vladeck, "Information Access – Surveying the Current Legal Landscape of Federal Right-to-Know Laws" (2009) 39 Environmental Law and Policy Annual Review 10773, 10779.

[92] Graves and Katyal, "From Trade Secrecy to Seclusion", 1385–420.

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

which suggest using different legal frameworks, such as FOI, data-protection law or AI regulation, identify the use of AI systems or applications as a key justification for narrowing protection for trade secrets.[93] These proposed carve-out fields include use of high risk AI systems,[94] Internet of Things applications[95] or public space facial recognition applications.[96]

Narrowing the scope of trade-secret protection through new public-interest-based carve-outs would undoubtedly increase the apparent scope of FOI and other public disclosure rights. In their spheres of operation, transparency carve-outs would sweep away not only the question of whether a trade-secret claim was unsound or inflated, but also whether a specific, overriding public interest could be demonstrated. In the AI sector, where the complexity and opacity of AI systems has made reverse engineering and other workarounds to trade secrets much more difficult to achieve, carve-outs could reduce unearned trade-secret-holder advantages.[97] Where AI is used to assess job and promotion applications or monitor employees, transparency carve-outs could extend the reach of workplace transparency rights, excluding trade-secret rationales for refusing public disclosure of information relevant to risks of AI discrimination, manipulation or error.

Nonetheless, in our view, transparency carve-out solutions have serious disadvantages that outweigh the apparent benefits of mandatory public disclosure of trade-secret-protected information in selected areas of public concern. We see serious, unexamined objections to these proposals grounded in problems of uncertainty, over-inclusion and effectiveness. Consequently, transparency carve-outs carry significant risks of creating destructive harms for trade-secret holders without appreciably advancing the objectives of public transparency.

[93] J.C. Fromer, "Machines as the New Oompa-Loompas: Trade Secrecy, the Cloud, Machine Learning, and Automation" (2019) 94 NYU Law Review 706, 717–36; Lu, "Data Privacy", 2101–47; K. Foss-Solbrekk and A.K. Glenster, "The Intersection of Data Protection Rights and Trade Secret Privileges in 'Algorithmic Transparency'" in E. Kosta, R. Leenes and I. Kamara (eds.), *Research Handbook on EU Data Protection Law* (London 2022), 163–83; U. Mylly, "Transparent AI? Navigating between Rules on Trade Secrets and Access to Information" (2023) 54 International Review of Intellectual Property and Competition Law 1013, 1017; H. Sun, "The Right to Know Social Media Algorithms" (2023) 18 Harvard Law & Policy Review 1, 21.

[94] Mylly, "Transparent AI?".

[95] G. Noto La Diega and C. Sappa, "The Internet of Things at the Intersection of Data Protection and Trade Secrets: Non-Conventional Paths to Counter Data Appropriation and Empower Consumers" (2020) 3 European Journal of Consumer Law 419.

[96] R. Matulionyte, "Transparency of Facial Recognition Technology and Trade Secrets" in R. Matulionyte and M. Zalnieriute (eds.), *Cambridge Handbook on Facial Recognition in the Modern State* (Cambridge 2024), 60–73.

[97] Katyal, "Paradox of Source Code Secrecy", 1249; Tschider, "Beyond the 'Black Box'", 721; E. Bayamlioglu, "Machine Learning and the Relevance of IP Rights: An Account of Transparency Requirements for AI" (2023) 32 European Review of Private Law 329, 359.

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

A. Uncertain Boundaries and Unbounded Risks of Harm

Commercial activities are unlikely to fit neatly within any sphere in which public transparency is deemed to be essential to societal interests and made subject to a transparency carve-out, such as health and safety or public space facial recognition. Mandatory public disclosure would therefore cut through commercial sectors, risking arbitrary effects amongst competing trade-secret holders. Employers in one business sector deemed to be in scope, for example, could be compelled to disclose trade-secret-protected information to their employees and through them to the public, while their competitors in an adjacent sector might not be in scope. Yet, despite commercially damaging costs, carve-outs would not necessarily ameliorate the imbalance of power present in highly mediated transparency processes. Indeed, by heightening the risk of harmful compelled disclosure, carve-outs could lead to greater obstruction and non-cooperation by trade-secret holders.

This potential can be seen in the FOI field in which the disclosure of "unwanted, unlabelled, unsorted, raw data" remains an unresolved disclosure practice.[98] In the context of AI transparency, which is imperfect and frequently aspirational, disclosures and explanations occur at different stages through design, training and operation. For parties wishing to avoid disclosure, there are ample opportunities for obfuscation. Public disclosure could also be legitimately refused on the grounds that the information does not fall within the scope of the carve-out category. In FOI contexts, that refusal would inevitably require adjudication, including the delays and costs associated with that.

The disclosure of trade secrets in a transparency carve-out sphere would also create unintended risks of wider economic harm. In some circumstances, the consequences of commercial investments or technical innovations foregone could be irreparable, especially for smaller or new competitors. The possibility of compelled public disclosure of commercially sensitive information through employee transparency rights could, for example, simply foreclose discussion of the potential benefits and risks of some AI applications. The downsides of introducing transparency carve-outs could, no doubt, be seen as a necessary trade-off between opposed forms of public interest, in which commercial interests must be restricted to achieve the benefits of an informed public. This view of public transparency is complacently managerial, failing to consider the incommensurability of such trade-offs and overlooking the multilayered and unstable conflicts present in liberal democratic transparency rights.

[98] M. Chowdhury, "'The House Always Wins': Empirical Reflections on UK Freedom of Information Legislation for Policing Research" (2022) 10 Salus Journal 51.

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

That instability arises out of the potentially unbounded nature of a public right to know that seeks to set aside established limits on public transparency without clarity about ultimate ends.[99] As a claim to open and direct public scrutiny of the workings of the state, the right to know is unmistakeably rooted in ideas of popular sovereignty and, in radical forms, the ultimate subordination of the institutions and laws of the state to notions of the will of the people.[100] In this familiar tension, the foundational legitimacy of the state rests on the people's constituent power, which exposes the institutional and legal order to risks of populist impairment or even destruction.[101] Once the right to know is understood as a manifestation of popular sovereignty, the potential for transparency rights to serve destructive political purposes in volatile times becomes clearer.[102]

In less antagonistic versions, popular sovereignty sustains demands for greater public participation in the processes of democratic governance and oversight,[103] linking public transparency with the scrutiny and contestation of power.[104] Inevitably, that conception of public scrutiny of power extends beyond the state to private exercises of power, which are enabled in part by intellectual property rights. Even from this moderate perspective, the proposed definitional boundaries for transparency carve-outs are weak and open to expansion, especially when their foundations in democratic principle are minimally developed or non-existent. One sectoral carve-out from trade-secret protection is likely to lead to others, while also placing pressure on the protection of sensitive governmental or personal information from public disclosure.

The defence of trade secrecy from unbounded public scrutiny rests on institutional responses to popular sovereignty, which assert legitimacy through representative democracy and constitutional order, importantly including the safeguarding of human security, dignity and autonomy.[105] Significantly, these responses undercut the normative significance of collective political agency by claiming the same broad moral principles

[99] D.S. Ardia, "Popular Sovereignty and a Right to Know about the Government" (2025) 67 Arizona Law Review 1.

[100] M. Loughlin, "The Concept of Constituent Power" (2014) 13 European Journal of Political Theory 218; G. Duke, "Habermas, Popular Sovereignty, and the Legitimacy of Law" (2024) 35 Law and Critique 237.

[101] L. Foisneau, "The Hobbesian Crowd Problem" (2023) 85 The Review of Politics 474; M. Herrero, "Carl Schmitt on the Transformations of the People in Modernity" (2023) 85 The Review of Politics 494.

[102] D. Pozen, "Transparency's Ideological Drift" (2018) 128 Yale Law Journal 100; R. Green, "FOIA-Flooded Elections" (2024) 85 Ohio State Law Journal 255.

[103] M. Levin et al., "Citizens' White Paper", available at https://demos.co.uk/wp-content/uploads/2024/07/Citizens-White-Paper-July-2024_final.pdf (last accessed 14 August 2024); V. Pavel, "Rethinking Data and Rebalancing Digital Power", available at https://www.adalovelaceinstitute.org/project/rethinking-data/ (last accessed 14 August 2025).

[104] M. Fenster, "Populism and Transparency: The Political Core of an Administrative Norm" (2021) 89 University of Cincinnati Law Review 286.

[105] R. Stacey, "Popular Sovereignty and Revolutionary Constitution-Making" in D. Dyzenhaus and M. Thorburn (eds.), *Philosophical Foundations of Constitutional Law* (Oxford 2016).

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

that underpin the people's right to know.[106] The resulting institutional legitimacy is essential to the complex rules and balancing mechanisms that currently govern public-transparency regimes, keeping the more destructive tendencies of the right to know in check.[107] Those defences are present not only in the broad exclusions for classes of trade secrets that offset public disclosure rights and duties, but also in the careful limits placed on public-interest-based exceptions to those protections.

Nonetheless, popular sovereignty's demands for unbounded public transparency may be checked but cannot be disarmed. The relationship between public disclosure rights and the protection of trade secrets of any kind is ultimately antagonistic and irresolvable. Consequently, while transparency carve-out proposals see the right to know and associated arguments for mandatory public transparency as benign and underserved, those proposals tend not to consider fully the need for constraints as well as reinvigoration.

B. An Ineffective Approach to Public Transparency

In several respects, there are anachronistic elements in proposals to address the obstructive effects of trade-secret protection on AI transparency through carve-outs. Since its relatively recent appearance in the canon of liberal democratic rights, public transparency continues to evolve, both conceptually and practically.[108] That evolution is, however, more than a response to the ongoing digital revolution in information technologies and applications, whose rise coincided with the introduction of FOI and data-protection rights. It also reflects changing ideas about democratic engagement and public participation and, equally, about the ways in which information markets generate innovation and economic growth. Moving from earlier generic rights, such as the FOIA right to information held by public authorities, to increasingly specialised and purpose defined rights, such as the EU Data Act[109] data-portability right, public transparency is now characterised by sets of overlapping disclosure rights and duties.

The increasing complexity and opacity of AI systems is, moreover, driving transparency concepts and methods rapidly through further technical and organisational specialisation.[110] This includes a range of novel information disclosure methods to facilitate AI's explainability,

[106] D. Mokrosinska, "The People's Right to Know and State Secrecy" (2018) 31 Canadian Journal of Law & Jurisprudence 87; D. Mokrosinska, *State Secrecy and Democracy: A Philosophical Inquiry* (Oxford 2023).

[107] Fenster, "Populism and Transparency".

[108] See *Magyar Helsinki Bizottság v Hungary* (2020) 71 E.H.R.R. 2, at [149]–[156].

[109] Commission Regulation (EU) No 2854/2023 (OJ 2023 L 2854 p.1) ("EU Data Act").

[110] J. Krook et al., "A Systematic Literature Review of Artificial Intelligence (AI) Transparency Laws in the European Union (EU) and United Kingdom (UK): A Socio-Legal Approach to AI Transparency Governance" (2025) 5 AI Ethics 4069.

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

interpretability and auditability. To be effective, these methods will often require technical expertise and other resources for parties on both sides of AI disclosure processes as participation and dialogue between developers, deployers and other participants becomes essential to effective transparency outputs.[111] Where responsibility is widely distributed through multiple parties, applications and outputs, effective AI transparency may need to encompass not only the full lifecycle of an AI system, but also the entire breadth of its socio-technical dimensions, which may also be transnational in scope.[112] Plainly, specialisation in AI transparency methods raises important questions about the future role of the public in these methods. For employees concerned about AI risks in the workplace, for example, the opportunities for contesting AI transparency outputs may lead to innovations in informed participation in AI transparency processes or, less optimistically, performative transparency, such as chatbots dispensing formulaic responses.

Proposals for transparency carve-outs tend not to be well adapted to the challenges of AI transparency specialisation. While aiming to narrow FOI's broad exclusions for trade secrets, they frequently look back to the design of FOI rights as a model for public disclosure. No doubt, FOI disclosure requirements have considerable potential for forcing the disclosure of information revealing AI risks and harms. Important elements of AI models or systems can, for example, be accessed without need for operational explainability, such as training data information as well as AI generated decisions, content and other outputs. Doctrinal developments in FOI law requiring that the information is disclosed in accessible and readable forms or formats can also be further developed in AI contexts.[113] There is, however, no evident interest at the governmental level in the UK or EU in introducing general rights to explanation into FOI laws.

Nonetheless, the comparatively simple FOI disclosure model is not structured to achieve the degree of participation and explanation needed to achieve comprehensively effective AI transparency.[114] In addition, its focus on public authorities only indirectly reaches the commercial providers of AI systems and applications through their information

[111] B. Rieder and J. Hofmann, "Towards Platform Observability" (2020) 9 Internet Policy Review 1.

[112] L. Sartori and A. Theodorou, "A Sociotechnical Perspective for the Future of AI: Narratives, Inequalities, and Human Control" (2022) 24 Ethics Information Technology 4; J. Cobbe, M. Veale and J. Singh, "Understanding Accountability in Algorithmic Supply Chains" in *FAccT '23: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency* (New York 2023), 1186–97.

[113] EU Parliament and Council Directive (EU) No 4/2003, art. 4; K. Pentney, "The Right of Access to 'Reliable' Information under Article 10 ECHR: From Meagre Beginnings to New Frontiers" (2024) 5 European Convention on Human Rights Law Review 230; *Association Burestop 55 v France* (Application nos. 56176/18, 56189/18, 56232/18 et al.), Judgment of 1 July 2021, not yet reported.

[114] H.P. Olsen et al., "The Right to Transparency in Public Governance: Freedom of Information and the Use of Artificial Intelligence by Public Agencies" (2024) 5 Digital Government Research and Practice 1.

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

sharing with public authorities.[115] These shortcomings indicate that the resolution of conflicts between public AI transparency and trade-secret claims will require an integration of the dynamic, public-driven qualities of the right to know with emerging methods of AI transparency, which transparency carve-outs cannot offer.

V. Meaningful Transparency through Targeting

Innovations in transparency regimes since the establishment of the FOI disclosure model offer considerable potential for disentangling public-transparency needs and trade-secret protection. In simple terms, disclosure rights and duties are becoming more targeted in their purposes, processes and intended parties, steering away from the broad access model of FOI. The aim of this targeting, which follows precedents in mandatory disclosure requirements for consumers and other relevant groups, has been to provide meaningful information disclosures for defined purposes and parties. As we discuss, targeting transparency rights or duties in this way can include as well as exclude the obligatory disclosure of trade secrets.

Despite these innovations, post-FOI public-transparency frameworks typically retain the three common features identified above: disclosure rights and duties; exclusions for protected classes, including trade secrets; and, in some cases, public-interest-based exceptions to those exclusions. Where it works well, targeted transparency can offer a method to achieve effective transparency results while avoiding unnecessary conflicts with trade-secret claims. Targeting transparency purposes not only reduces the scope of the disclosure requirement to fit the identified stakeholder's needs, but also considers whether a trade-secret claim is genuinely obstructive to those defined needs. Indeed, this evolution in public transparency towards targeting raises the question of whether creating transparency carve-outs is a necessary or relevant goal.

Data-protection law provides one of the best examples of targeting in public transparency, having two distinct public disclosure rights relevant to AI transparency. These include, first, the right of data subjects to access their personal data ("SARs") under General Data Protection Regulation ("GDPR"), art. 15, which, in some respects, resembles FOI access rights. SARs apply to all data controllers, whether public or private, thus overcoming the public/private split that often restricts the potential scope of FOI requests regarding matters of public interest. Like FOI requests, SARs are also a form of public transparency as the requester's motive is not a relevant consideration and any disclosed

[115] B. Hawkins et al., "The Law of Diminishing Returns? The Challenge of Using Freedom of Information Legislation for Health Policy Research" (2023) 33 Critical Public Health 383; Chowdhury, "House Always Wins".

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

information can be shared without restriction.[116] These rights are, consequently, widely used for non-data-protection collateral purposes, such as seeking information prior to a formal complaint or legal action in employment contexts.[117]

In other significant ways, SARs are more targeted than FOI rights, applying only to the personal data of the data subject who requests SAR disclosure. Additionally, their motive-blind character does not prevent their data-protection purposes from being taken into account when an SAR request is balanced against conflicting interests, such as a trade-secret claim. In the event of a conflict, the necessity and proportionality of the requester's data-protection interests will be weighed against the risk of commercial harm to the trade-secret claimant.[118] Aside from giving less weight to SARs made for collateral purposes, this context-specific inquiry will consider the relative importance of the personal data to the requester's ability to exercise specific data-protection rights, such as objection or erasure.[119]

Second, of rising importance for AI transparency, GDPR, art. 22 and associated provisions are arguably the basis for a data subject's "right to an explanation" in relation to automated processing of personal data.[120] This includes the right to receive meaningful information regarding the logic of that processing and an explanation of its potential consequences.[121] While this falls short of the complex demands of effective AI transparency, being neither a right to receive answers to questions or to participate in disclosure processes, it is a major advance over FOI rights or GDPR SAR rights where Article 22 is not engaged. As the CJEU has confirmed, the GDPR affords "a genuine right to an explanation as to the functioning of the mechanism involved in automated decision-making".[122] Nonetheless, while this requires simple, yet meaningful, explanations of the logic involved, it does not ordinarily require complex explanations.

In the EU, further innovations in targeted transparency have built on the experience of data-protection rights. These new forms of transparency rights and duties are more explicit in limiting access to trade secrets to defined parties and the sharing of disclosed data. The EU Data Act, following

[116] Article 29 Working Party, "Guidelines on Transparency under Regulation 2016/679", available at https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_en.pdf (last accessed 26 October 2025).
[117] A.A. Habu et al., "Data Subject Rights as a Research Methodology: A Systematic Literature Review" (2023) 16 Journal of Responsible Technology 100070.
[118] Judgment of 7 May 2009, *College van burgemeester en wethouders van Rotterdam v Rijkeboer*, C-553/07, EU:C:2009:293, at [49]–[54].
[119] *Harrison v Cameron* [2024] EWHC 1377 (KB), at [130] (Steyn J.).
[120] L. Edwards and M. Veale, "Slave to the Algorithm? Why a Right to Explanation Is Probably Not the Remedy You Are Looking For" (2017) 18 Duke Law & Technology Review 67.
[121] ICO and Alan Turing Institute, "Explaining Decisions Made with AI", available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/ (last accessed 14 August 2025).
[122] Judgment of 27 February 2025, *CK v Dun & Bradstreet Austria*, C-203/22, EU:C:2025:117, at [57], [60].

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

the GDPR's modest data-portability rights, has created a regime for the compelled disclosure of usage data for connected products and services to qualified users.[123] Any usage data protected by a trade-secrets claim need not be disclosed unless disclosure is strictly necessary for an EU Data Act purpose and the recipient party agrees to any measures necessary to preserve confidentiality.[124] The EU Data Act thus brings the qualified user within the trade-secret barrier, applying non-disclosure obligations to prevent unauthorised sharing.[125] While this is plainly not full public transparency, it does borrow elements of the right to know, such as the public initiated exercise of disclosure rights.

In providing access to data held by very large online platforms ("VLOP") or very large online search engines ("VLOSE") to qualified researchers ("vetted researchers"), Article 40 of the EU Digital Services Act ("DSA") creates a different solution to manage trade-secret transparency conflicts.[126] Vetted researcher requests are strictly purpose limited and subject to approval by an authorised National Digital Coordinator ("NDC") before submission to a VLOP or a VLOSE.[127] The subsequent obligation to provide researcher access to the requested data does not, moreover, apply if disclosure would lead to vulnerabilities in the protection of confidential information, including trade secrets. Thus, unlike the EU Data Act, the DSA keeps vetted researchers firmly outside the trade-secret barrier. At the same time, the DSA and its implementing rules do not create express powers for NDCs to invalidate trade-secrets claims where they are determined to be unsound or inflated or where a specific public interest is judged to outweigh the DSA presumption in favour of non-disclosure.[128]

While the GDPR, EU Data Act and DSA potentially apply to a host of AI applications, AI-specific regulation in the EU has so far not introduced major innovations in targeted transparency. The AI Act, which primarily concerns AI safety and risk management, creates basic public-transparency obligations consistent with consumer protection standards.[129] These aim to ensure that the public are aware of when high

[123] T. Aplin, "The Data Act and Trade Secrets: An Experiment in Compulsory Licensing" in A. Sattler and H. Zech (eds.), *The Data Act: First Assessments* (Trier 2024), 85–102.
[124] EU Data Act, arts. 4(6), 5(9).
[125] Contrast the portability disclosure right created by EU Parliament and Council Directive (EU) No 2831/2024 (OJ 2024 L 2831 p.1), art. 9(6), which assumes that trade secrets will not be disclosed.
[126] Commission Regulation (EU) No 2065/2022 (OJ 2022 L 277 p.1), art. 40 ("DSA").
[127] Ibid., art. 40(4): "or the sole purpose of conducting research that contributes to the detection, identification and understanding of systemic risks in the Union, as set out pursuant to Article 34(1), and to the assessment of the adequacy, efficiency and impacts of the risk mitigation measures pursuant to Article 35."
[128] European Commission, "Delegated Act on Data Access under the Digital Services Act (DSA)", available at https://digital-strategy.ec.europa.eu/en/library/delegated-act-data-access-under-digital-services-act-dsa#:~:text=The%20delegated%20act%20lays%20down,applications%20to%20access%20relevant%20datasets (last accessed 25 October 2025).
[129] AI Act, art. 50.

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

risk AI systems are being used, with special attention to particular applications such as emotion recognition or generation of deep fakes.[130] The public are not, however, significant rights bearers under the AI Act's product safety design, although the Act extends the GDPR right to an explanation.[131] In relation to AI discrimination in the workplace, for example, Article 77 of the AI Act empowers public authorities to compel disclosure of relevant information in an accessible language and format, but provides no equivalent for employees or their representatives. While the AI Act may therefore have disappointed those with aspirations for significant empowerment of public transparency, efforts continue to be made to develop forms of targeted transparency that provide meaningful transparency for particular needs.[132]

Undoubtedly, targeted transparency obligations for AI-system developers, deployers and users could substantially reduce the potential for public-transparency and trade-secret conflicts. A well-designed, targeted AI public-transparency framework could identify individual or collective needs for information disclosure, while also identifying and excluding unnecessary or disproportionate disclosures of trade-secret claims. The targeted transparency model, however, usefully makes clear that an explicit solution to the trade-secret barrier is required where trade-secret disclosure is unavoidably at issue. Adapting the EU Data Act model, disclosure to qualified and trustworthy third parties could be made subject to confidentiality obligations. Alternatively, the DSA-vetted researcher model could be adapted to protect information controllers subject to targeted disclosure requirements against disclosing trade-secret-protected information whose disclosure would risk serious commercial harm. Developing the DSA-vetted academic researcher access model for other contexts, such as workplace AI transparency, would undoubtedly present challenges in determining who would qualify for vetted access.

Targeted transparency obligations are, however, neither a form of nor a substitute for the right to know. In effect, a targeted transparency framework is a mechanism for legally determining the necessary scope and purposes of transparency on a "need to know" basis, which is entirely different from the dynamic, exploratory nature of a public

[130] Ibid.

[131] Busuioc, Curtin and Almada, "Reclaiming Transparency".

[132] Q.V. Liao and J. Wortman Vaughan, "AI Transparency in the Age of LLMs: A Human-Centered Research Roadmap", available at https://hdsr.mitpress.mit.edu/pub/aelql9qy/release/2 (last accessed 26 October 2025); Schor et al., "Mind the Gap"; A. Balayn et al., "Understanding Stakeholders' Perceptions and Needs Across the LLM Supply Chain, Human-Computer Interaction", available at https://arxiv.org/pdf/2405.16311 (last accessed 15 August 2025); U. Ehsan et al., "Human-Centered Explainable AI (HCXAI): Reloading Explainability in the Era of Large Language Models (LLMs)" in F.F. Mueller et al. (eds.), *CHI EA 2024: Extended Abstracts of the CHI Conference on Human Factors in Computing Systems* (New York 2024), 1–6.

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

exercised right to know.[133] There is, consequently, an inherent risk that the public-interest disclosure goals of a targeted transparency regime are structured to avoid conflicts with the protection of trade secrets. While targeted transparency usefully navigates the potential harms of the right to know, it also widens the risks of unaccountable secrecy, relying too heavily on institutional claims to democratic legitimacy and public trust.

VI. Trade Secrets and Innovations in AI Public Transparency

How effectively the right to know can be structured or function in the AI era remains to be seen. While transparency carve-outs from the scope of trade-secret protections are, on balance, poorly designed solutions and targeted forms of transparency negate important aspects of the right to know, alternative solutions ensuring that trade-secret claims do not obstruct necessary AI public transparency will require considerable innovation. As noted, the complexity and opacity of AI systems will often strengthen the inherent advantages of information controllers. Consequently, in many circumstances, demonstrating that the trade-secret claim is unsound or inflated or that there is a compelling public interest in disclosing trade-secret-protected information will require considerable technical expertise.

In our view, while AI public transparency is essential to protect the many collective and private interests at risk to AI systems,[134] protection for valid trade-secret claims remains in the general public interest. Yet, that baseline assumption begs several questions. How should the dynamic, public-driven character of the right to know be integrated into developing AI transparency processes; how should unsound or inflated trade-secret claims be evaluated; and how should overriding public interests in disclosure be demonstrated? Resolving these questions will require considerable innovation on both sides of the trade-secret barrier. In this concluding section, we examine key challenges to better AI public transparency and explain how trade-secret obstruction of legitimate transparency could be addressed as an integral part of the solutions to those challenges. Our purpose here is to outline areas for further research.

The challenges in delivering effective AI public transparency are multidimensional.[135] As AI systems are invariably networked and carry high risks of malicious or negligent use, transparency processes will need

[133] M.E. Kaminski, "Understanding Transparency in Algorithmic Accountability" in W. Barfield (ed.), *The Cambridge Handbook of the Law of Algorithms* (Cambridge 2020), 121–38; M. Maroni, "'Mediated Transparency': The Digital Services Act and the Legitimisation of Platform Power" in M. Hildebrandt, P. Leino-Sandberg and I. Koivisto (eds.), *(In)visible European Government: Critical Approaches to Transparency as an Ideal and a Practice* (Oxford 2023).

[134] I. Parker, A. Studman and E. Jones, "Learn Fast and Build Things: Lessons from Six Years of Studying AI in the Public Sector", available at https://www.adalovelaceinstitute.org/policy-briefing/public-sector-ai/ (last accessed 14 August 2025).

[135] Krook et al., "Systematic Literature Review".

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

to be security risk compliant. Public-transparency processes must also be designed to ensure that any disclosures of personal data are necessary and proportionate. Consequently, the protection of trade secrets is nestled within an overlapping set of public-interest reasons for limiting transparency to forms of low risk, targeted transparency. In that tendency, AI public transparency becomes the management of the public's need to know rather than facilitating the public's right to know, while also hazarding public trust in AI governance that operates without public scrutiny. In our view, AI public transparency requires external participation and independent observation in collaborative processes aimed at delivering explainability and interpretability of AI risks.[136] That requires methods of mitigating the risks of public disclosure, rather than their elimination.

We see three areas in which the right-to-know ideal could be developed in AI transparency processes. First, the incorporation of binding third-party review of trade-secret claims directly into public-transparency challenge and contestation rights for AI systems would remove some of the unilateral advantages of trade-secret holders. The vetted researcher access right, for example, found in DSA, art. 40, offers a potential, if not so far sufficient, model.[137] Interestingly, the CJEU has recently pushed in a similar direction. In its *Dun & Bradstreet* decision, the court interpreted the GDPR data subject access right to include the requirement that, where a controller's refuses access on the grounds of trade-secret protection, the controller must disclose the protected information to the relevant regulator or court if challenged by the data subject; the regulator or court must then determine whether non-disclosure is necessary and proportionate.[138]

Drawing on these formative ideas, it is worth investigating how to create faster and simpler intermediary review processes for trade-secret claims to compel disclosure of information where a claim is unsound or inflated or there is an overriding public interest. The latter element raises the issue, discussed above, of how specific that public interest in disclosure should be to overcome the general public interest in protecting legitimate trade secrets. Solutions may lie in requiring intermediary authorities to investigate proactively evidently reasonable public-interest arguments raised in access requests.

[136] S. Casper et al., "Black-Box Access Is Insufficient for Rigorous AI Audits" in *FAccT '24: Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency* (New York 2024), 2254–72.

[137] Office of Communications, "Researchers' Access to Information from Regulated Services", available at https://assets.publishing.service.gov.uk/media/68667c5a1f124a0bb0a3aa09/researchers__access_to_information_from_regulated_online_services.pdf (last accessed 14 August 2025); P. Leerssen, "Outside the Black Box: From Algorithmic Transparency to Platform Observability in the Digital Services Act" (2024) 4 Weizenbaum Journal of the Digital Society 1.

[138] Judgment of 27 February 2025, *CK v Dun & Bradstreet Austria*, at [73]–[74].

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

Second, widening the scope of vetted third-party participation in standard setting and compliance assessment within the trade-secrets barrier could also bring elements of the public right to know inside the trade-secret barrier. In academic and civil society spheres, there is a considerable push for more public participation in AI governance, including the design of AI transparency and accountability processes.[139] At their broadest, these proposals are captured by concepts of AI democratisation, which embrace collective decision-making by creating rights of participation in AI use, development, revenues and governance as well as building technical and organisational capacities to make those rights effective.[140] AI democratisation, however, risks the unbounded populist tendencies discussed above.[141] Somewhat more narrowly, proposals for public participation have been advanced through ideas of participatory design and similar concepts.[142] As Corbett and Denton have explained: "[p]articipatory design is fundamentally about dismantling power and information asymmetries between designers and users [. . .] Participatory design can help achieve this by bringing people into the design process such that they can be empowered to discover the ends and means of transparency that are meaningful to them."[143]

The adoption of the EU AI Act raised expectations for public participation in AI transparency standard setting as well as subsequent compliance assessment and auditing. Yet, progress in public AI transparency methodologies has moved slowly in comparison to the surging pace of AI model development. AI documentation methods, such as model cards, data cards, risk labels and disclosure interfaces, which are essential to better AI public transparency, vary considerably and are often not fit for that purpose.[144] Disclosure practices, such as technical "data dumps", may not meet expectations for meaningful public explainability and

[139] E.P. Goodman, "NTIA Artificial Intelligence Accountability Policy Report", available at https://www.ntia.gov/sites/default/files/publications/ntia-ai-report-final.pdf (last accessed 14 August 2025).

[140] Seger et al., "Democratising AI", 715–22; U. Aytac, "Big Tech, Algorithmic Power, and Democratic Control" (2024) 86 The Journal of Politics 1431.

[141] J. Himmelreich, "Against 'Democratizing AI'" (2023) 38 AI and Society 1333.

[142] D. Zytko et al., "Participatory Design of AI Systems: Opportunities and Challenges Across Diverse Users, Relationships, and Application Domains" in S. Barbosa et al. (eds.), *CHI EA '22: CHI Conference on Human Factors in Computing Systems Extended Abstracts* (New York 2022), 1–4; F. Delgado et al., "The Participatory Turn in AI Design: Theoretical Foundations and the Current State of Practice" in *EAAMO '23: Equity and Access in Algorithms, Mechanisms, and Optimization* (New York 2023), 1–23.

[143] E. Corbett and R. Denton, "Interrogating the T in FAccT" in *FAccT '23: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency* (New York 2023), 1624–34.

[144] Ibid.; Liao and Wortman Vaughan, "AI Transparency in the Age of LLMs"; S. Huang and D. Siddarth, "Generative AI and the Digital Commons", available at https://arxiv.org/pdf/2303.11074 (last accessed 15 August 2025).

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

interpretability.[145] Commitments to disclosure are also restricted in practice by encryption and other barriers to access.[146]

The standardisation of AI transparency processes and outputs is widely seen as an essential foundation for improving AI public transparency, which will require novel substantive and procedural solutions to the blocking effects of trade-secrets claims.[147] There is, however, an evident lack of consensus on the aims of that transparency standardisation or who should participate in the standardisation processes.[148] For proponents of civil society participation in transparency governance, the objective is to put "the right information in the hands of the people with the legitimacy to make complex normative decisions at a local, context sensitive level".[149] The realisation of effective disclosure methods that are open to public contestation is certainly less likely where standardisation is dominated by technical experts selected through closed standard setting processes.[150]

External participation in compliance assessment and auditing processes is a potential avenue for building effective AI public transparency but would require considerable ingenuity at the trade-secrets barrier. AI auditing for security, fairness, reliability, data protection and other requirements is already a focus for potential public participation in operational oversight,[151] although unstandardised and idiosyncratic.[152] This developmental moment

[145] C. Norval et al., "Disclosure by Design: Designing Information Disclosures to Support Meaningful Transparency and Accountability" in M. Corbett-Davies et al. (eds.), *FAccT '22: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (New York 2022), 679–90.

[146] M. Veale, "Denied by Design? Data Access Rights in Encrypted Infrastructures" in J. Ausloos and S. P. de Souza (eds.), *Critical Perspectives on Data Access for Research* (Cambridge forthcoming), available at https://doi.org/10.31235/osf.io/94y6r (last accessed 6 July 2026).

[147] European Commission, "Commission Implementing Decision on a Standardisation Request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in Support of Union Policy on Artificial Intelligence", available at https://ec.europa.eu/transparency/documents-register/detail?ref=C%282023%293215&lang=en (last accessed 26 October 2025); IEEE SA Working Group, "How to Make Autonomous Systems More Transparent and Trustworthy", available at https://standards.ieee.org/beyond-standards/topic/artificial-intelligence-systems/how-to-make-autonomous-systems-more-transparent-and-trustworthy/#:~:text=IEEE%207001%20standard%20describes%20specific,engineering%20to%20enable%20societal%20benefit (last accessed 14 August 2025).

[148] G. Auld et al., "Governing AI through Ethical Standards: Learning from the Experiences of Other Private Governance Initiatives" (2022) 29 Journal of European Public Policy 1822; H. Pouget, "The EU's AI Act Is Barreling toward AI Standards that Do Not Exist", available at https://www.lawfaremedia.org/article/eus-ai-act-barreling-toward-ai-standards-do-not-exist (last accessed 14 August 2025).

[149] J. Laux et al., "Three Pathways for Standardisation and Ethical Disclosure by Default under the European Union Artificial Intelligence Act" (2024) 53 Computer Law & Security Review 1, 4.

[150] Ibid.; P. Nemitz and A. Oueslati, "How US Firms Are Weakening the EU AI Code of Practice", available at https://www.techpolicy.press/how-us-firms-are-weakening-the-eu-ai-code-of-practice/ (last accessed 20 August 2025).

[151] J. Mökander, "Auditing of AI: Legal, Ethical and Technical Approaches" (2023) 49 Digital Society 2; V. Ojewale et al., "Towards AI Accountability Infrastructure: Gaps and Opportunities in AI Audit Tooling" in N. Yamashita et al. (eds.), *CHI '25: Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems* (New York 2025); B. Faveri, G. Auld and S. Renckens, "AI Audit Objects, Credentialing, and the Race-to-the-Bottom: Three AI Auditing Challenges and a Path Forward", available at https://www.techpolicy.press/ai-audit-objects-credentialing-and-the-racetothebottom-three-ai-auditing-challenges-and-a-path-forward/ (last accessed 14 August 2025); A. Mantelero, "The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, Legal Obligations and Key Elements for a Model Template" (2024) 54 Computer Law & Security Review 106020.

[152] A. Birhane et al., "AI Auditing: The Broken Bus on the Road to AI Accountability", available at https://arxiv.org/pdf/2401.14462 (last accessed 15 August 2025).

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

in AI assessment and auditing offers an opportunity to increase the range of participant groups involved in the design and execution of audits,[153] such as civil society organisations.[154] So far, however, legal mandates for participation through stewardship models or the capacity and knowledge base needed to enable effective public participation are inadequate.[155]

Widening public participation in audits would undoubtedly help to bring a publicly defined right-to-know inquiry into the processes of AI oversight. Yet, that objective carries obvious hazards. Expanding the range of actors operating under the confidentiality obligations of auditors would, for example, increase risks of unauthorised disclosure through non-compliant parties or security failures. Conversely, while civil society presence may encourage more challenging audit inquiries and practices, that presence cannot resolve conflicts between trade secrets and public disclosure per se. Ensuring that audit reports are published and that only information that is legitimately protected by trade-secret claims is excluded is one option.[156] That route to better AI public transparency would require efficient adjudication processes for auditor assertions that a claim does not have a valid basis or, alternatively, should be disclosed for compelling public-interest reasons. It should also be recognised that making public disclosure an AI audit responsibility also puts auditors in a privileged position in the mediation of transparency.[157]

Third, developing public authority or agency responsibilities to report and disclose matters of public interest resulting from AI regulatory supervision and enforcement could be subject to duties to provide contestable, reasoned explanations.[158] Where full public disclosure could not be justified, there are strong precedents for more limited public disclosure, reporting on public-interest-based internal scrutiny without revealing essential protected information.[159] Yet, reliance on the state to satisfy public information needs is self-evidently an extreme form of mediated transparency, controlling the substance and form of public disclosure. Where state authorities disclose information according to internal conclusions about

[153] S. Costanza-Chock et al., "Who Audits the Auditors? Recommendations from a Field Scan of the Algorithmic Auditing Ecosystem" in Corbett-Davies et al. (eds.), *FAccT '22*, 1571–83.

[154] I. D. Raji et al., "Outsider Oversight: Designing a Third-Party Audit Ecosystem for AI Governance" in V. Conitzer and J. Tasioulas (eds.), *AIES '22: Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society* (New York 2022), 557–71.

[155] P. Terzis, M. Veale and N. Gaumann, "Law and the Emerging Political Economy of Algorithmic Audits" in *FAccT '24*, 1255–67.

[156] T. Zick et al., "AI Procurement Checklists: Revisiting Implementation in the Age of AI Governance, Computers and Society", available at https://arxiv.org/pdf/2404.14660 (last accessed 15 August 2025); E. Seger et al., "Democratising AI".

[157] J. Wong et al., "Key Challenges for the Participatory Governance of AI in Public Administration" in S. Giest et al. (eds.), *Handbook of Governance and Data Science* (Cheltenham 2023).

[158] Morten, "Publicizing Corporate Secrets".

[159] See e.g. IPCO, "Annual Report of the Investigatory Powers Commissioner 2022", available at https://www.ipco.org.uk/publications/annual-reports/ (last accessed 14 August 2025).

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

the extent of the public's need to know, as we note above, the dynamic, exploratory nature of a public exercised right to know is inevitably lost. Consequently, public disclosure mechanisms controlled by the state authorities or agencies, however independent, offer a significant but inadequate strand in AI public transparency.

In our view, these areas for further research are both preferable and potential alternatives to carving out public-transparency fields from trade-secret protections. In emphasising the need for innovations at the trade-secrets barrier, these suggested alternatives do, however, illustrate the ways in which civil society intermediaries, rather than the public at large, have become central to the exercise of the right to know in the AI era. Returning to our example of AI in the workplace, even if employees, who suspect that AI assessment or monitoring is discriminatory, possessed better explanations and/or access rights, very few would have the time and knowledge needed to use those rights effectively. On the other hand, aside from trade unions, which are absent or under-resourced in many work environments, there is an obvious shortage of specialist intermediaries equipped to articulate compelling cases for the public disclosure of AI-related trade secrets affecting conditions of employment and recruitment.

Yet, this gap in representation and capacity is plainly not confined to the employment sector. The integration of complex AI systems into human life presents an enormous challenge to liberal democratic ideals of informed public knowledge and action. While trade secrets present a genuine barrier to that knowledge and action, the other side of the right to know also needs urgent attention. Further innovations in public-transparency law will need to address the intermediary problem.

VII. Conclusions

In this article, we recognise that trade-secret claims pose a serious threat to the necessary public transparency of AI systems and that a publicly defined and pursued right to know is essential to meaningful AI transparency. Nonetheless, in our view, the established model of public disclosure rights, protected types of trade secrets and recognition of context-specific compelling public interests in disclosure can be adapted to address that threat. The alternative of transparency carve-outs to trade-secrets protections would create substantial uncertainties and risk disproportionate commercial harms, while not addressing the ways in which trade-secret claims are embedded in complex and evolving AI transparency processes. Finding more effective ways to resolve conflicts between trade-secret claims and public-interest disclosure in AI contexts is, consequently, inseparable from the complicated challenges of

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press

achieving public knowledge of AI systems for essential democratic, economic and risk-prevention purposes.

The evolution of public-transparency regimes towards forms of targeted transparency offers a potentially effective route to meaningful transparency for defined purposes and, to a degree, can manage trade-secret and public-transparency conflicts. However, targeted transparency also undermines the right to know, with wider implications for the public's capacities to contest the ordering of the public information sphere by state and private power. Securing the right to know in AI transparency processes is therefore critically important to the survival of liberal democracies and market economies in the AI era.

The enduring conflict between public transparency and trade secrecy can only be navigated through innovations in transparency that are fair, effective and efficient. We suggest three promising areas for potential innovation that are worthy of further research and development: (1) developing right-to-know transparency challenge rights that incorporate third-party review of trade-secret claims to remove trade-secret holders' unilateral advantages; (2) developing more diversity in vetted third-party access to compliance assessment within the trade-secrets barrier; and (3) developing public authority or agency responsibilities to report and disclose matters of public interest in the course of AI regulatory supervision and enforcement. These areas do not provide a "quick-fix" solution, but they do have the potential to grapple meaningfully with the complexities and demands of public transparency and trade secrets.

https://doi.org/10.1017/S0008197325101086 Published online by Cambridge University Press