

Trade secrecy in automated decisions: against the myth of irreconcilability and the imposition of patents

Asress Adimi Gikay*

Asress Adimi Gikay is Senior Lecturer in AI, Disruptive Innovation and Law, Brunel University of London, Kingston Ln, Uxbridge UB8 3PH, United Kingdom.

*Email: asress.gikay@brunel.ac.uk

Abstract

- Trade secrecy has been widely recognised as an obstacle to transparency in automated decision-making. In multiple cases involving automated decisions impacting individuals, the disclosure of decision-making processes has been restricted to safeguard proprietary information.
- This limitation to transparency has prompted scholars to question the appropriateness of trade secrecy in the age of algorithms including calling for the complete removal of trade secret protection for algorithms in some cases. While some scholars have proposed an unconditional disclosure of the data used in automated decision systems as well as of their source code, others have favoured the use of patents for certain software programmes.
- In this article, based on extensive analysis of existing law including judicial decisions, we discuss how to achieve a balance between these two conflicting positions. Furthermore, we contend that neither abolishing trade secrecy nor mandating patent-based protection for algorithms is necessary or justifiable. Lastly, we assert that, although patenting software and artificial intelligence (AI) is possible, businesses are likely to prefer trade secret protection over patents for their inventions due to the practical challenges of obtaining patents for AI systems.

1. Introduction

'Life would be intolerable in personal and commercial terms, if information could not be given or received in confidence and the right to have the information respected by the force of law'.¹ This is Sir John Donaldson's remark in the appellate judgment in *Attorney General v Guardian Newspapers* (1990). The case involved the disclosure in a book, by a retired MI5 agent, of alleged irregularities and illegal activities within MI5.² Sir Donaldson's remark highlights the need to uphold the protection of confidential information, for personal or commercial life as well as governments to function. Nevertheless, he recognised that this protection is not absolute as '... there will be just cause or excuse for breaking confidence when there are countervailing public interests supporting publication which outweigh those supporting the right to confidentiality'.³ So the law should protect secrecy and facilitate disclosure when there is a compelling interest. In the era of advanced algorithms used for automated decision-making (ADM) impacting the rights of individuals and public interest at large, the extent to which commercial secrets should be protected has been a matter of longstanding controversy.

Trade secret protection of algorithms as a limiting factor in ensuring transparency in algorithmic decisions has been widely

analysed.⁴ The dilemma arises from two potentially conflicting but legitimate interests. On the one hand, businesses have a legitimate interest in safeguarding their proprietary algorithm potentially giving them a competitive advantage over rival firms.⁵ On the other hand, the members of the public that allege to be unfairly impacted by an algorithmic decision may wish to understand how the decision was made, requiring some level of transparency, including potential rights to examine the data involved in the decision-making as well as the decision-making process itself. The law must strike a delicate balance between these two opposing expectations.

On several occasions where disclosure of information regarding algorithmic decisions was demanded, trade secret has been invoked as a defence to limit disclosure.⁶ This has caused

⁴ Rebecca Wexler, 'Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System' (2018) 70 *Stanford Law Review* 1344–429, Céline Castets-Renard, 'Accountability of Algorithms in the GDPR and Beyond: A European Legal Framework on Automated Decision-Making' (2019) 30 *Fordham Intell. Prop. Media & Ent. L. J.* 91, 96. Available at <https://ir.lawnet.fordham.edu/jipl/vol30/iss1/3> (accessed 21 March 2020) and I Mendoza and LA Bygrave, 'The Right Not to Be Subject to Automated Decisions Based on Profiling' in T Synodinou et al. (eds), *EU Internet Law: Regulation and Enforcement* (Springer 2017).

⁵ Kurt M Saunders, 'The Law and Ethics of Trade Secrets: A Case Study' (2006) 42 *California Western Law Review* 209, 247.

⁶ In *State v Loomis*, 881 N.W.2d, [769], a Wisconsin Circuit court used COMPAS recidivism risk assessment (algorithm), which evaluated the probability of the offender reoffending. The prediction was based on an interview with the offender and comparison of the offender's criminal history with other offenders' data. The exact methodology of COMPASS was protected by trade secrets. The Supreme Court of Wisconsin upon appeal concluded that the risk assessment method was based on data available to the

¹ *Attorney General v Guardian Newspapers* (n 2) [1990] (Sir John Donaldson M.R.), [177]–[178].

² *Ibid* at 109.

³ *Ibid* at 178.

concerns among scholars, advocacy groups and policy makers, as the combination of opaque algorithmic decision systems and trade secret law might lead to relevant actors making decisions for which they are not held accountable.

In the European Union (EU), the conflict between transparency in ADM and trade secret protection has been addressed by the General Data Protection Regulation (GDPR)⁷ and the Trade Secret Directive.⁸ Recently, the EU Artificial Intelligence (AI) Act and the now-withdrawn Draft AI Liability Directive have introduced some provisions dedicated to trade secret protection in the context of AI. However, these recent legal developments have not brought about significant changes in addressing the concerns raised in academic literature and policy papers. In the USA, both the legal basis for trade secret protection and the rule for balancing disclosure and secrecy have largely been established by state and case laws.⁹ The US Congress passed the first federal trade secret legislation, the Defend Trade Secret Act (DTSA), in 2016.¹⁰ Neither the EU's relatively tailored system, nor the US's sparse legal regime contain hard and fast rules on how judges could reconcile the conflict between transparency in ADM and trade secret protection of proprietary information in concrete cases.

There are two primary problems with the existing literature. The first one is the call for abolishing trade protection for algorithms that impact individuals and the public.¹¹ Such a call, unsupported by a robust analysis of the existing legal frameworks, is unrealistic. Second, while moderate positions recognised the need for a balancing exercise, they fail to provide guidance on how such exercise can be done in practical terms.¹² This article first articulates the conflict between the demand for transparency and maintaining trade secret protection for algorithms. More importantly, it argues for the first time that the existing legal literature

that advocate for the abolition of trade secrecy for certain ADM is erroneous due to the lack of strong legal reasoning justifying such a prescription. To that effect, the article analyses how balancing exercises introduced by courts in the USA can aid in applying the existing laws to allow the enforcement of trade secret protection in such a way that the individual rights and public interests are also protected. The article also analyses why patent protection for algorithms, especially in the age of AI, is an unattractive method of protection, giving businesses little incentive to pursue it as an alternative. Thus, the call for removal of trade secret protection for algorithms or for its replacement by patent protection is neither justifiable, nor necessary.

The remaining part of the article is divided into three sections. Section 2 provides a brief overview of the preference for trade secrecy over other IP rights for software. Section 3 analyses the conflict between trade secrecy and algorithmic transparency by focusing on ADM under the GDPR. It also discusses judicial decisions from the USA to exemplify how judges have tried to balance the two interests in concrete cases. Section 4 investigates the possibility and feasibility of mandating patent protection for computer programmes including AI, as this is one of the solutions presented as an alternative in the existing literature. It discusses the economic arguments against patenting computer programmes as well the legal challenges to obtaining patents for them. This section highlights that the combination of legal and practical challenges makes patenting computer programmes a difficult choice, strongly supporting the argument that businesses should not be forced to make that choice by law. Section 5 provides concluding remarks.

2. Trade secrecy in ADM and its appeal to businesses

A report published in 2017 by the European Union Intellectual Property Office shows companies prefer trade secret over patents to protect innovation.¹³ There are several reasons for this, but first it will be useful to start with the definition of trade secret to understand its unique features that might appeal to businesses. The EU Trade Secret Directive defines trade secret as follows:

'trade secret' means information which meets all of the following requirements: (a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) it has commercial value because it is secret; (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.¹⁴

The definition has three crucial components. These are (a) secret information, which can encompass business information, technological information and know-how, excluding 'trivial information or experience and skills gained by employees during the normal course of their employment'¹⁵; (b) potential or actual commercial

defendant and thus the proprietary nature of COMPAS did not violate the defendant's due process of law. See generally, Han-Wei Liu, 'Beyond State v Loomis: Artificial Intelligence, Government Algorithmizing, and Accountability' (2019) 27 *International Journal of Law and Information Technology* 122, 133. In credit scoring, the German Federal Court of Justice has given a similar judgment where it allowed a limited disclosure due to trade secret protection of the algorithm. See Hunton Andrews Kurt, Federal German Court Rules on Credit Scoring and Data Subject Access Rights (29 January 2014). Available at <https://www.huntonprivacyblog.com/2014/01/29/federal-german-court-rules-credit-scoring-data-subject-access-rights/> (accessed 11 September 2018).

⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJEU, L119/1, Recital 63.

⁸ Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJEU, L157/1.

⁹ Brian T Yeh, 'Protection of Trade Secrets: Overview of Current Law and Legislation, Congressional Research Service' (22 April 2016). Available at <https://fas.org/spp/crs/secretary/R43714.pdf> (accessed 1 April 2019).

¹⁰ Defend Trade Secret Act, Public Law 114-53—11 May 2016.

¹¹ For instance, Citron and Pasquale argue that disclosure of the logic involved in scoring algorithm are guarded by trade secret, but they do not engage in examining the issue in detail other than asserting that the default rule should switch from assumption of secrecy to the right of the consumers to know the system of scoring that impacts them. Danielle Keats Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2016) 89 *Washington Law Review* 1, 6. Similarly, Hurley and Adebayo argue that 'While total trade secrecy could allow certain scorers to maximize their business advantage, we maintain that this interest does not outweigh the need to ensure that consumers are informed and can challenge inaccurate, biased, and potentially predatory models.' Mikella Hurley and Julius Adebayo, 'Credit Scoring in the Era of Big Data' (2017) 18 *Yale Journal of Law and Technology* 146, 198. But their work on this particular aspect of algorithmic credit scoring is not detailed enough to provide the basis for policy or legal reform.

¹² The GDPR presents a unique opportunity to examine the relationship between trade secrets and algorithms. One of the comprehensive works from the EU is Gianclaudio Malgieri, 'Trade Secrets v Personal Data: A Possible Solution' (2016) 6 *International Data Privacy Law* 102. Although Malgieri's analysis is insightful, he does not provide a satisfactory answer to the question.

¹³ Dugie Sandeford 'Companies Prefer Trade Secrets to Patents to Protect Innovation, EUIPO Finds' IP Watch (27 July 2017). Available at <https://www.ip-watch.org/2017/07/27/companies-prefer-trade-secrets-patents-protect-innovation-euipo-finds/> (accessed 16 August 2020).

¹⁴ Trade Secret Directive Art. 2(1).

¹⁵ Rembert Niebel, Lorenzo de Martinis and Birgit Clark, 'The EU Trade Secrets Directive: All Change for Trade Secret Protection in Europe?' (2018) 13(6) *Journal of Intellectual Property Law and Practice* 445, 448.

value causally linked to the secrecy of the information¹⁶ and (c) reasonable steps—‘protective measures’—being taken by the business to keep the information secret.¹⁷ The EU Trade Secret Directive does not define essential notions such as reasonable steps,¹⁸ but these are issues to be addressed through judicial interpretation. For the purpose at hand, it suffices to highlight that trade secrecy can be an attractive form of protecting commercial information for five key reasons: (i) wider scope of subject matter, (ii) lack of specific legal formality for securing protection, (iii) secrecy, (iv) unlimited duration and (v) absence of public interest use exception. Since these characteristics make trade secrets more attractive to companies than other IP rights, in particular in the field of algorithms, it is necessary to analyse them in more detail.

As note earlier, the subject matter of a trade secret is any information that is secret and valuable, subject to reasonable steps by the owner to preserve its secrecy.¹⁹ A valuable information could be anything including technical information (eg a formula or a method) or business information (eg customer pricing list).²⁰ The information in question does not need to meet a substantive requirement such as the novelty requirement of patent law²¹ or the originality standard of copyright law.²² It only needs to be valuable, not publicly accessible and subject to reasonable steps to preserve the *status quo*.

The second important aspect of trade secrecy is the lack of a formal procedure to secure the protection of proprietary information. To obtain a patent, the prospective patentee should file an application at the patent office, which investigates whether the invention qualifies as patentable subject matter. Among others, the applicant must define the scope of the invention (draw up a claim)²³ and disclose the invention to enable a person having ordinary skill in the art to be able to reproduce it.²⁴ Sometimes, an invention may not meet the requirements of patentability, for instance due to lack of an inventive step.²⁵ This creates legal uncertainty, which may deter computer programme developers/owners from seeking patent protection. By contrast, trade secret protection permits the holder to prevent the disclosure of an invention which may not be worthy of protection under patent law by keeping it secret through contractual mechanisms, mainly, non-disclosure agreements. In this sense, while the law provides protection for trade secrets by enforcing contractual agreements guarding proprietary information, it does not require an arduous procedure to protect the information.

The most obvious and defining feature of trade secret law is protection through secrecy. In a patent regime, the prospective patentee must meticulously describe the invention to enable its reproduction by a person having ordinary skill in the art.²⁶ The

disclosure of the invention is a prerequisite for granting the patent and is aimed at allowing the public, including other inventors, to have access to the invention after the expiry of the patent. It is a *quid pro quo* for the exclusive right the law grants to the patentee.²⁷

The fact that trade secret protection could last indefinitely makes it an attractive legal tool for companies in contrast with patent and copyright that have limited durations.²⁸ A company could exploit the value of its proprietary information for a reasonably long period of time (eg Coca Cola has been keeping its formula secret for over a century).²⁹

Finally, trade secret law does not have an exception for public interest uses. Copyright law allows a justified unauthorized use under the fair use doctrine, while patent law grants mandatory licensing in cases where public interest requires it. These exceptions are aimed at limiting proprietary right to serve public interest. A fair use of a copyright work and the non-enforceability of a patent in case of medical emergencies provide cases where IP law creates limits to advance public interest.³⁰ Trade secret law accepts no such cases of general public interest disclosure sanctioned by law.

In ADM, as this article demonstrates, companies are frequently using the opaque nature of trade secret law to limit the disclosure of information in a legal dispute. Nonetheless, first, an in-depth analysis of the conflict between trade secrecy and transparency in ADM is provided.

3. ADM and trade secrecy

3.1. Transparency in ADM, the GDPR and the Trade Secret Directive

This section provides an overview of how transparency in ADM and trade secrecy conflict and the mechanism available for reconciling the two. The focus is on how a conflict might arise and what the law says as to reconcile the conflict. Although the central focus of this article is the European legal framework, we also briefly review relevant US judicial decisions to obtain useful insights.

Under the GDPR, generally, the data subject has ‘the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her’.³¹ In cases where an automated decision is authorized by way of exception, it ‘should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain

by a person skilled in the art.’), see also Robert G. Bone, ‘The (Still) Shaky Foundations of Trade Secret Law’ (2014) 92 Tex. L. Rev. 1803, 1807–10.

²⁷ Katherina Pistor, *The Code of Capital: How the Law Creates Wealth and Inequality* (Princeton University Press 2019) 126. ‘As a *quid pro quo* for obtaining a patent the patentee must disclose the core features of the invention, which implies that some information about the product will be leaked to others.’

²⁸ EPC Art. 63(1) establishes 20 years from the date of filing as the term for a European Patent. See 35 U.S.C. § 154(a)(1) (2012) which establishes that patent right has the duration of 20 years from the date on which the application for the patent was filed. See also 17 U.S.C. § 106(1)–(5) (2012). § 302(a) establishes that generally ‘copyright in a work created on or after 1 January 1978 subsists from its creation and ... endures for a term consisting of the life of the author and 70 years after the author’s death.’

²⁹ Deepa Varadarajan (n 19) 1412.

³⁰ Rebecca Tushnet, ‘Intellectual Property as a Public Interest Mechanism’ in Rochelle Dreyfuss and Justine Pila (eds) *The Oxford Handbook of Intellectual Property Law* (OUP 2018) 5.

³¹ GDPR Art. 22(1). Para 2 recognises exceptions, namely automated processing when necessitated for entering into or performance of contract between the data subject and the data controller and when allowed by the union’s law and based on the data subject’s consent. In all cases, adequate safeguards to protect the freedom and legitimate interest of the data subject must be put in place.

¹⁶ Ibid.

¹⁷ Ibid., 449.

¹⁸ Ibid.

¹⁹ Trade Secret Directive Art. 2(1). See also Deepa Varadarajan, ‘Trade Secret Fair Use’ (2014) 83 *Fordham Law Review* 1401, 1403.

²⁰ Ibid., 1403.

²¹ Tun-Jen Chiang, ‘Defining Patent Scope by the Novelty of the Idea’ (2012) 89 *Wash. U. L. Rev.* 1211, 1217.

²² T. Margoni, ‘The Harmonisation of EU Copyright Law: The Originality Standard’ in M. Perry (ed) *Global Governance of Intellectual Property in the 21st Century* (Springer International Publishing 2016) 85–105.

²³ EPC Art. 84. ‘The claims shall define the matter for which protection is sought. They shall be clear and concise and be supported by the description.’

²⁴ EPC Art. 56. See also Deepa Varadarajan (n 19), 1419, 1421.

²⁵ EPC Art. 56. ‘An invention shall be considered as involving an inventive step if, having regard to the state of the art, it is not obvious to a person skilled in the art.’

²⁶ See EPC Art. 83 (‘The European patent application shall disclose the invention in a manner sufficiently clear and complete for it to be carried out

an explanation of the decision reached after such assessment and to challenge the decision'.³² The data subject has therefore the right to explanation, including to obtain meaningful information about the logic involved in the automated ADM.³³ This right is aimed at enabling individual to effectively exercise the rights conferred on them by Article 22(3) of the GDPR, 'namely the right to express his or her point of view on that decision and to contest it'.³⁴ In this context, the GDPR states that such 'right, should not adversely affect the rights or freedoms of others, including trade secrets or IP and in particular the copyright protecting the software'.³⁵ This principle, embodied in recital 63, is the only instance in which trade secret is mentioned under the GDPR. Since the GDPR requires the explanation of the logic involved in ADM, it raises a question as to how the logic of ADM could be explained without infringing trade secrecy, where proprietary information is involved.

The lack of clear understanding on the provision of meaningful information about the logic involved in ADM has previously been emphasised by scholars.³⁶ In addition to the ambiguity in the notion of the logic involved in automated decision, the trade secret rights of the decision maker (data controller or the party providing the ADM service) pose an added challenge to ensuring algorithmic transparency.

The EU Trade Secret Directive, whose aim is to encourage innovation through protecting the trade secrets of businesses,³⁷ also places limitations on trade secret protection. In particular, 'this Directive should not affect the application of Union or national rules that require the disclosure of information, including trade secrets, to the public or to public authorities'.³⁸ Further, the Directive pledges to respect fundamental rights and observe the principles recognised in particular by the Charter of Fundamental Rights of the EU, including personal data protection.³⁹ Although respect for fundamental rights is expected to limit trade secrets, the extent to which trade secrets may suffer from limits due to data protection rights is not clear from the Directive.⁴⁰

3.2. A balancing test

Ensuring algorithmic transparency, in particular the right to explanation in automated decisions while protecting trade secrecy, requires a delicate balancing. As discussed above, the corresponding provisions in the GDPR⁴¹ and the Trade Secret Directive provide only general guidance. Investigating the relationship between trade secret and data protection under the GDPR, Gianclaudio Malgieri argues that the prevalence of one or the other legal regime, ie whether the right to explanation or the protection of trade secrecy prevails, should be determined on a

case-by-case basis.⁴² This is in line with the way in which these potentially inconsistent legal regimes should operate. However, no statutory rule or judicial decisions provided an insight into how the case-by-case balancing act should be conducted, in particular identifying specific factors that might be considered in the analysis.

In a recent judgment, the Court of Justice of the European Union (CJEU) had the opportunity to consider this issue in the *Dun and Bradstreet (D&B) Austria* case.⁴³ There, a mobile telephone operator refused to conclude or extend a mobile telephone contract which would have required a monthly payment of EUR 10 on the ground that, according to an automated credit assessment, carried out by D&B, the complainant CK did not have sufficient financial creditworthiness.⁴⁴ D&B had not provided the complainant with sufficient explanations to enable her to understand how the prognosis on the probability of her future behaviour ('score') had been established other than stating that, to obtain the scoring, 'certain socio-demographic data concerning CK had been "given equal weighting"'.⁴⁵

Based on expert advice on the minimum information required to meet the obligation to provide meaningful information regarding the logic involved in the automated decision under the GDPR, the referring Administrative Court of Austria believed the following information to be necessary to satisfy the requirement 'meaningful information about the logic involved'.⁴⁶

- the personal data concerning CK which have been processed in order to formulate a 'factor';
- the mathematical formula on which the calculation that led to the score at issue in the main proceedings is based;
- the specific value attributed to CK for each of the factors concerned;
- the precise intervals within which the same value is attributed to different data for the same factor (interval or discrete evaluation or index/land-register-based evaluation) and
- a list of scoring for the period covering the 6 months preceding and the 6 months following the establishment of CK's score, as obtained using the same calculation rule.

The referring court asked several questions in its preliminary reference, the most pertinent being the following:

Can the tension between the right of access guaranteed by Article 15(1)(h) of the GDPR and the right to non-disclosure of a trade secret protected by [Directive 2016/943] be resolved by allowing the information to be disclosed as a trade secret within the meaning of [point 1 of Article 2 of Directive 2016/943] be disclosed to the authority or the court only, so that the authority or the court must independently verify whether it must be assumed that a trade secret within the meaning of [point 1 of Article 2 of Directive 2016/943] exists and whether the information provided by the controller within the meaning of Article 15(1) of the GDPR is accurate?

In this regard, it is interesting to observe that the referring court referred to article 9 of the Trade Secret Directive.⁴⁷ Article 9, which

³² GDPR Art. 22(2) and Recital 71.

³³ Ibid, Recital 63.

³⁴ Case C-203/22, *Dun & Bradstreet Austria*, CLI:EU:C:2025:117 at [55].

³⁵ GDPR, Recital 63.

³⁶ Lilian Edwards and Michael Veale, 'Slave to Algorithm? "Why a Right to Explanation Is Probably Not the Remedy" You Are Looking for' (2017), 16 *Duke Law & Technology Review* 19–84. See also David Lehr and Paul Ohm, 'Playing with the Data: What Legal Scholars Should Learn About Machine Learning' (2017), 51 *University of California Davis* 653.

³⁷ The Trade Secret Directive Recital 1.

³⁸ Trade Secret Directive Recital 11.

³⁹ Ibid, Art. 34.

⁴⁰ Maja Brkean and Grégory Bonnet, 'Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: Of Black Boxes, White Boxes and Fata Morganas' (2020) 11 *European Journal of Risk Regulation* 18, 40. 'From a legal perspective, it therefore remains rather unclear which set of rules should take precedence in case of conflict of trade secrets with data subjects' rights.'

⁴¹ GDPR Recital 63.

⁴² Gianclaudio Malgieri, 'Trade Secrets v Personal Data: a Possible Solution for Balancing Rights' (2016) 6 *International Data Privacy Law* 102, 104.

⁴³ Case C-203/22, *Dun & Bradstreet Austria*, CLI:EU:C:2025:117.

⁴⁴ Ibid at [6].

⁴⁵ Ibid at [20].

⁴⁶ Ibid at [24–25].

⁴⁷ Ibid at [31].

pertains to the preservation of confidentiality of trade secrets in the course of legal proceedings, requires Member States to ensure that parties involved in legal proceedings related to the unlawful acquisition, use or disclosure of a trade secret, including lawyers, court officials, witnesses and experts, are prohibited from using or disclosing confidential trade secret accessed during the judicial proceeding.⁴⁸ The provision does not apply to cases where unlawful acquisition, use or disclosure is not involved, for instance where the controversy relates to a data subject exercising their right, as in the case at hand. Therefore, it is unclear why the referring court mentioned article 9. Similarly, the CJEU did not express its view on the relevance of that provision. However, it concluded that although a balance must be struck between the right to access of the data subject and the rights or freedoms of others including trade secret, such a process should not lead to a full refusal to provide any information, as stated in recital 63 of the GDPR.⁴⁹ It recognised that:

... in particular in so far as it contains personal data of third parties protected by that regulation or trade secrets, within the meaning of point 1 of Article 2 of Directive 2016/943. In that case too, that information must be disclosed to the competent supervisory authority or court, which must balance the rights and interests at issue with a view to determining the extent of the data subject's right of access to personal data concerning him or her. In that regard, it should be borne in mind that a Member State cannot definitively prescribe the result of a case-by-case balancing of the rights and interests at issue imposed by EU law ...⁵⁰

Therefore, it is for the national courts to balance the rights of individuals in the case of ADM *v* trade secret by considering proportionality on a case-by-case basis.⁵¹ This position has support in the reading of the GDPR provisions as well as the Trade Secret Directive. More importantly, it ought to be acknowledged that, fundamentally, the law in this area is reasonably workable with appropriate judicial interpretation.

Recent legislative developments also tend to do nothing more than provide a general principle in addressing the conflicting interests of algorithmic transparency and trade secrecy. For instance, the EU AI Act,⁵² and the now-withdrawn Draft AI Liability Directive,⁵³ highlight the need for balancing the protection of individual rights and public interest to the disclosure of information on the one hand and the trade secret rights on the other, with relatively more detailed provisions. A caveat here would be that the EU AI Act covers a slightly broader notion of algorithmic transparency, which involves potential disclosure of information to entities involved in the application of the act rather than to individuals affected by an ADM. However, the general idea behind the prevailing rules under the EU AI Act, the GDPR and the AI Liability Directive remains that transparency and trade secrecy require a balancing act.

Article 78 of the EU AI Act reiterates that legal or natural persons that engage in the application of the regulation must protect the confidentiality of information obtained in the relevant activities, including the trade secrets of the businesses, in accordance with article 5 of the Trade Secret Directive.⁵⁴ Under article 5 of the directive, trade secret could be divulged for the following reasons:

- (i) for exercising the right to freedom of expression and information as set out in the Charter, including respect for the freedom and pluralism of the media;
- (ii) for revealing misconduct, wrongdoing or illegal activity, provided that the respondent acted for the purpose of protecting the general public interest;
- (iii) disclosure by workers to their representatives as part of the legitimate exercise by those representatives of their functions in accordance with Union or national law, provided that such disclosure was necessary for that exercise and
- (iv) for the purpose of protecting a legitimate interest recognized by Union or national law.

The EU AI Act therefore assumes that information protected by trade secrets can be disclosed for instance to regulatory entities or conformity assessment bodies obtaining technical documentation. Such information cannot be disclosed further, except under article 5 of the Trade Secret Directive. This provision is slightly different from article 3 of the AI Liability Directive, which allows a court, 'upon a duly reasoned request of a party or on their own initiative, to take specific measures necessary to preserve confidentiality when that evidence is used or referred to in legal proceedings'.⁵⁵ Both the EU AI Act and the AI Liability Directive are based on the notion that the disclosure of information, including trade secrets, should be limited and proportionate to what is necessary, ie to risk assessment in the case of the AI Act or 'to support a potential claim or a claim for damages and the preservation to that which is necessary and proportionate to support such a claim for damages' in the case of the AI Liability Directive.⁵⁶

Thus, while the method of striking a balance between trade secret protection and the protection of transparency interest is not comprehensively addressed in the legislation, there are some rules scattered around different laws that can aid judges in achieving such a balance in practice.

3.3. Trade secrecy and ADM in the USA: some insights on the balancing exercise

While this work is not concerned with providing a detailed account of the US experience on trade secrecy in the context of algorithmic transparency, we highlight below some insightful cases that suggest how the balancing exercise can be carried out in practice.

In the USA, neither the Constitution nor any other federal law regulated trade secret protection. Thus, the protection of trade secret has traditionally been based on case law.⁵⁷ In 1979, the Uniform Trade Secrets Act (UTSA)⁵⁸ was adopted by the Commissioners of Uniform State Laws with a view to harmonizing diverse state trade secret laws.⁵⁹ The UTSA was adopted by all states

⁴⁸ Trade Secret Directive Art. 9(1).

⁴⁹ Case C-203/22, *Dun & Bradstreet Austria*, CLI:EU:C:2025:117, para 73.

⁵⁰ *Ibid* at [74] and [75].

⁵¹ *Ibid* at [73].

⁵² Regulation (EU) 2024 of the European Parliament and the Council laying down harmonized rules on artificial intelligence and amending Regulations (EC) 300/2008, (EU) 167/2013, (EU) 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

⁵³ Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM (2022) 496 final.

⁵⁴ EU AI Act Art. 78(1)(a).

⁵⁵ EU AI Liability Directive Art. 3(4).

⁵⁶ See EU AI Act Art. 78(2) and the EU AI Liability Directive Art. 3(4).

⁵⁷ Brian T. Yeh (n 9).

⁵⁸ Uniform Trade Secrets Act, 14 U.L.A. 539–40.

⁵⁹ Ramon A. Klitzke, 'The Uniform Trade Secrets Act' (1980) 64 *Marq. L. Rev.* 277.

except New York and Massachusetts.⁶⁰ In 2016, Congress enacted the DTSA, which became the first federal trade secret law.⁶¹

The DTSA has no specific provision on the balancing of trade secret protection and disclosure. However, it does recognise that in court proceedings (civil or criminal), 'the court may not authorize or direct the disclosure of any information the owner asserts to be a trade secret unless the court allows the owner the opportunity to file a submission under seal that describes the interest of the owner in keeping the information confidential'.⁶² Hence, any party that is compelled to disclose its secret information may do so under confidentiality. In the USA, there is a comprehensive system of law that permits disclosure of information to be made to limited parties, including to attorney only at the exclusion of the opposing party.⁶³ These rules can be used to disclose proprietary information with the necessary protection from further disclosure in place. Nevertheless, in many cases, excluding the party seeking transparency is likely to defeat the very purpose of the disclosure. When an aggrieved suspect in a criminal proceeding challenges an algorithmic decision-making system on the basis of the right to question the evidence used in the decision-making system (due process of law), or where a consumer wishes to understand how he/she is denied credit, disclosing the required information only to the attorney is likely to be considered unjust as the parties themselves have the right to engage in their own trial.

Trade secret is as powerful in the USA as it is in the EU in the field of ADM, as it has limited disclosure in multiple cases. In *State v Loomis*, the specific method used by a software known as COMPAS for the determination of sentencing and parole by a court was protected by trade secret.⁶⁴ In 2006, the US Department of Justice filed for subpoena to compel Google to provide millions of user search queries and unlimited number of URLs from Google search index in an effort to uphold online pornography law.⁶⁵ Google argued, among others that 'the disclosure of statistically significant sample of Google's search index or query log may permit competitors to estimate information about Google's search indexing method or Googles users'.⁶⁶ Google's motion to dismiss the subpoena led the Department of Justice to modify its request to compel google to disclose only 50 000 URLs from Google search index and 5000 user queries. The District Court of California ordered Google to produce a list of 50 000 URLs under protective order reasoning that the risk that the disclosure of smaller sample of URLs would lead to a disclosure of trade secrets was low.⁶⁷

Notwithstanding the fact that legal rules are scant on the balance to be struck between disclosure and secrecy, some insights on the factors that can be considered to require disclosure can be gathered from otherwise unsystematic statutory rules and judicial decisions. Many of these factors ultimately determine

whether and how much a trade secret-protected information should be disclosed.

One of the factors to be considered in forcing disclosure include the indispensability of the information whose disclosure is sought. When algorithmic transparency is sought, whether in the context of a consumer wishing to challenge an adverse decision, an opposing party seeking disclosure in court of law or a public authority seeking disclosure of information related to its duties, the court should consider whether the information in question is indispensable to resolve the controversy. If the dispute at hand can be resolved by evidence obtained from other sources, the court should not compel disclosure of trade secret-protected information or information that may lead to reverse engineering of the underlying proprietary technology.

Google has argued in the 2006 subpoena case that the disclosure of similar information by other service providers, including Yahoo and Microsoft, was sufficient for the US Department of Justice to achieve its goal of developing an enforcement of online pornography law.⁶⁸ In the USA, a disclosure of information for the purpose of trial is restricted if 'the discovery sought is unreasonably cumulative or duplicative or can be obtained from some other source that is more convenient, less burdensome, or less expensive'.⁶⁹ Although this should be applied carefully and it may not always be a readily available, it is one of the factors that could be considered.

Another factor is whether limited disclosure achieves the objective. This reduces the likelihood of trade secret infringement while allowing the underlying objective of disclosure to be achieved. In *US AG v Google Inc.*, the court emphasised that the disclosure of 50 000 URLs from Google's search index is less likely to lead to inferences on the function of Google's search indexing as opposed to the disclosure of millions of URLs.⁷⁰

Last, the significance of the interests at stake could determine whether and to what extent disclosure of proprietary information could be compelled. For instance, it is easier to make the case for the disclosure of proprietary information used to prosecute an accused crime suspect than to compel disclosure in case of payment of higher interest rate for a loan. Clearly, it is difficult to create a hard and fast rule; the courts could put the various competing interests at stake on a scale of balance in compelling disclosure on a case-by-case basis. In the USA, some precedent exists in this regard, although slightly contradictory. In *Nebraska v Kuhl*, the appellate court held that defendant could not compel the disclosure of the source code of a breathalyser called MasterData that is used in his prosecution of driving under influence (DUI) cases, agreeing with the state that MasterData is a trade secret of the manufacturer.⁷¹ In a similar case, a Kentucky appellate court took a slightly different position holding that the source code of Intoxylizer 5000, a breathalyser manufactured by CMI Inc. could be disclosed to the parties of the case with a protective order preventing expert witnesses and parties from sharing the source code to persons outside the case.⁷² Both cases involve a prosecution for DUI where the interest involved is the right of confrontation (six amendments).

It is difficult to imagine a world where disagreements on this issue would not exist. In a similar vein, it is conceivable that the European courts could work out how a balance between competing interests could be struck in dealing with practical cases. Some

⁶⁰ Trade Secrets Laws and the UTSA—A 50 State and Federal Law Survey Chart (updated for Massachusetts), Fair Competition Law (2018). Available at <https://www.faircompetitionlaw.com/2018/08/10/trade-secrets-laws-and-the-utsa-a-50-state-and-federal-law-survey-chart-updated-for-massachusetts/> (accessed 13 February 2020).

⁶¹ Defend Trade Secret Act, Public Law 114-53—11 May 2016.

⁶² Ibid, section 3(b).

⁶³ Robert Timothy Reagan, 'Confidential Discovery: A Pocket Guide on Protective Orders' (Federal Judicial Center 2012) 6-7. Available at <https://www.fjc.gov/sites/default/files/2012/ConfidentialDisc.pdf> (accessed 6 August 2020).

⁶⁴ *State v Loomis*, 881 N.W.2d 749 (Wis. 2016).

⁶⁵ Katie Hafner and Matt Richtel, 'Google Resists U.S. Subpoena of Search Data' NY Times (20 January 2006). Available at <https://www.nytimes.com/2006/01/20/technology/google-resists-us-subpoena-of-search-data.html> (accessed 17 August 2020).

⁶⁶ *US AG v Google Inc. The United States District Court of California*, San Jose (CV-06-8006 MISC JV) 14.

⁶⁷ Ibid at [17].

⁶⁸ Ibid at [16].

⁶⁹ Federal Rules of Civil Procedure (US), Rule 26(b)(2)(i).

⁷⁰ Ibid.

⁷¹ 741 N.W.2d 701 (Neb. App. 2007), aff'd, 755 N.W.2d 389 (Neb. 2008).

⁷² No. 07-417, 2008 Ky. App. LEXIS 19 (Ken. 18 January 2008).

calls for reforming the law to provide better guidance have been made. However, some scholars have also called for a complete eradication of trade secret protection in the field of ADM.

3.4. The call for legislative reform

There is a potential conflict between algorithmic transparency and trade secrecy which needs to be addressed. In the EU, a soft approach to encourage transparency in ADM without jeopardizing trade secrets is adopted, without providing detailed guidelines on how to weigh the different competing interests.⁷³ In the USA, case law provides better guidance on how to reconcile the conflict between trade secrecy and algorithmic transparency. Regardless, some scholars emphatically argue that algorithmic transparency requires doing away with trade secret protection for algorithms,⁷⁴ albeit without offering an alternative method of protecting proprietary algorithms. Alluding to the lack of effort in reforming the law in this area, a study supported by the European Parliamentary Research Service concluded:

In legal terms, there is still no satisfactory mechanism that obliges companies to disclose their algorithms, without harming competitive strategies while ensuring public scrutiny. There is little discussion around changing IP Law in the sense of pressing for disclosure of algorithms in confidentiality agreements, though there is important literature demanding the auditability and transparency of algorithms.⁷⁵

A relatively small amount of literature advances theories under which trade secret protection could be carved out. The most important theory is the safe harbour theory, where a statutory exclusion of trade secret protection for certain subject matters is proposed. David S. Levin argues, in the context of breathalysers and voting machines, in favour of abandoning trade secret protection for proprietary assets of private companies providing services related to public infrastructure.⁷⁶ The theory of eliminating trade secret law for public infrastructure relies on the public's legitimate interest in the disclosure of information that affects fundamental values such as democracy and justice. David S. Levin argues for patent-based protection of information related to public infrastructure.⁷⁷

Nevertheless, to the extent that disclosure provides meaningful information to the public, regulators and other interested

stakeholders, is it possible to create a system where proprietary information no more enjoys trade secret protection? Could patenting algorithms be mandated at least in limited instances where it is believed that the cost of reconciling transparency and secrecy would be so high that companies should disclose the functioning of their algorithms from the get-go? The next section explores these questions.

4. Patenting algorithms

4.1. A theoretical analysis of patenting algorithms

The opaque nature of some algorithmic decisions exacerbated by trade secret law has created the sentiment that protecting algorithms through trade secret law is undesirable from a social justice and innovation point of view. If this is justified, an alternative legal regime for the protection of algorithms must be presented as feasible and reasonable, because it is unrealistic to argue for the elimination of trade secret protection of algorithms without offering such an alternative to protect commercial assets in which companies invest large sums of money to get a competitive edge over their rivals.⁷⁸ Patent is the most readily available alternative; but is it justifiable and feasible to impose it?

Patent law requires the disclosure of an invention as a prerequisite to granting the inventor an exclusive right.⁷⁹ Upon the expiry of a certain period of time, the patented invention becomes part of the public domain that is available for others to use.⁸⁰ The most obvious but important distinguishing feature of patent law relative trade secret law is that, under the former, secrecy is neither permitted, nor necessary. It is only trade secret law that protects commercial information of value by ensuring that it is hidden from competitors.⁸¹

The existing literature calling for the removal of trade secret protection for algorithms does not discuss alternative systems of protection,⁸² with the exception of a few scholars that suggest the elimination of trade secret in the public sector.⁸³ Daniele Citron and Frank Pasquale appeal to the inherent soundness of disclosure of algorithms in encouraging innovation and the public's interest in ensuring that consumers have adequate disclosure of systems that deeply impact them, to plea for the removal of trade secret protection for algorithms, although they do not explicitly recommend its replacement with the patent system.⁸⁴ In the context of credit scoring algorithms, they argue that:

The benefits of secrecy are murkier than these costs. Moreover, the secrecy of credit scoring can impede incremental innovation: how can outsiders develop better scoring systems if they have no way of accessing current ones? Secret credit scoring can undermine the public good, since opaque methods of scoring make it difficult for those who feel—and quite possibly are—wronged to press their case.⁸⁵

⁷³ 'In 2016 and 2018, the USA and the European Union each adopted trade secret protection laws that fail to clarify exemptions for algorithms and other digitized processes used by governments but built by private companies.' Marietje Schaake 'Trade secrets shouldn't shield tech companies' algorithms from oversight' (Brookings, 4 May 2020). Available at <https://www.brookings.edu/techstream/trade-secrets-shouldnt-shield-tech-companies-algorithms-from-oversight/> (accessed 6 August 2020).

⁷⁴ Danielle Keats Citron and Frank Pasquale (n 11) 31. 'The benefits of secrecy are murkier than these costs. Moreover, the secrecy of credit scoring can impede incremental innovation: how can outsiders develop better scoring systems if they have no way of accessing current ones? Secret credit scoring can undermine the public good, since opaque methods of scoring make it difficult for those who feel—and quite possibly are—wronged to press their case.'

⁷⁵ Ansgar Koene, 'A governance framework for algorithmic accountability and transparency' EPRS Scientific Foresight Unit, Study PE 624.262 (2019) 26.

⁷⁶ David S. Levin, 'The Impact of Trade Secrecy on Public Transparency' in Rochelle C. Dreyfuss and Katherine J. Strandburg (eds) *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research* (Edward Elgar Publishing 2010) 435.

⁷⁷ Ibid, 433. 'Nonetheless, there are some possible solutions to consider, the most extreme being eliminating trade secrecy protection for public infrastructure. If democratic transparency is the public's primary goal, the law might simply require those whose activities are of public concern to find proper protection in another intellectual property law doctrine, such as copyright or, more likely, patent, if possible. At least from a theoretical standpoint, if not from the purely practical perspective, the idea of patents as the primary substitute for trade secrecy has appeal' (citation omitted).

⁷⁸ Michael Risch 'Why Do We Have Trade Secrets?' (2007) 11 *Intellectual Property Law Review* 3, 39.

⁷⁹ Jeanne C. Fromer 'Patent Disclosure' (2009) 94 *Iowa Law Review* 539–606.

⁸⁰ See 35 U.S.C. § 154(a)(1) (2012) which establishes that patent right has the duration of 20 years from the date on which the application for the patent was filed. See also 17 U.S.C. § 106(1)–(5) (2012). Under Article 63(1) of the European Patent Convention, the term of a patent is 20 years subject to extension by a contracting party as provided under para 2 of this provision.

⁸¹ Michael Risch (n 78) 6–7.

⁸² Danielle Keats Citron and Frank Pasquale (n 11) 31.

⁸³ David S. Levin (n 76).

⁸⁴ Ibid and Danielle Keats Citron and Frank Pasquale (n 11) 31.

⁸⁵ Danielle Keats Citron and Frank Pasquale (n 11) 31.

Although a patent regime could possibly enhance transparency in algorithmic decision-making, in a legal system based on market economy, a strong policy justification should be found to compel businesses to protect their valuable innovations only through patents. So far, no such justification has been offered in the existing literature. On the contrary, there is a strong economic argument against patenting software. Based on empirical and anecdotal evidence, Andrew Nieh argues that patenting software is bad for the software industry because it deters innovation.⁸⁶ He argues that when software is patented, there is high probability of patent disputes. As patent examiners do not have the sufficient resource to examine prior art, they could also grant patents for inventions that do not make the required level of improvement to the state of the art,⁸⁷ while defensive patents deter modification of existing technological innovations.⁸⁸ Finally, patenting software discourages investment in research and development⁸⁹ and therefore it has a detrimental effect on the software industry overall.

Despite the strong assertion of the incompatibility of patenting software with innovation culture, the US Patent Office has granted patents for software in many instances. Although US Patent Act section 101 does not specify software as a patentable subject matter and hence software is not a statutory subject matter, various judicial decisions upheld the patentability of software.⁹⁰

As a vocal critic of patentability of software, Andrew Nieh claims that software is more appropriately protected by copyright.⁹¹ While software can indeed be protected under copyright law, this does not provide a valid alternative to trade secret from an economic perspective. Indeed, since copyright protects only expressions of ideas, and not ideas per se, there are no effective remedies against reverse engineering with copyright protection.

Since Andrew Nieh's main goal was to make the case that patent is unsuitable means of protecting software, he does not argue against trade secret-based protection, a subject matter to which he dedicates no comprehensive discussion. He also argues that from legal point of view, software should be excluded from patent law based on the non-patentability of abstract ideas.⁹²

The economic argument against patenting software is strong. Nevertheless, it is by no means sufficient to rule out patents as a viable alternative for protecting software. What it does highlight nevertheless is the fact that choosing patents as a means of protecting software-related inventions involves high costs. The choice to bear such costs should not be imposed by a legal system which requires patents as an exclusive means to protecting software. As demonstrated below, the legal and practical challenges in patenting software in Europe provide compelling evidence for why it is unjustifiable to remove trade secrecy in favour of patents for software and AI in particular.

4.2. Patenting AI software: legal and practical challenges

The patentability of software programmes in Europe is a matter of longstanding controversy and considerable legal disputes.

Article 52(2)(c) of the European Patent Convention (EPC) establishes that programmes for computer as such are not patentable subject matters.⁹³ The exclusion has been interpreted to mean that patenting software per se is excluded because the wording of article 52(2)(c) excludes computer programmes as such.⁹⁴ Hence, a software with technical effect, meaning that makes technical contribution to the art, is still patentable.⁹⁵

The practical application of article 52(2)(c) poses significant challenges, particularly entailing legal costs as a result of frequent and lengthy litigation. A few examples from the UK illustrate this challenge. In the UK, the relevant provision of the EPC is implemented in the Patents Act 1977, section 1(2)(c).⁹⁶ A number of cases decided by the UK Intellectual Property office (UKIPO) and the courts showcase the difficulty in obtaining patents for software, practically disincentivizing patents as an IP regime for software.

In *Emotional Perception AI Ltd v Comptroller-General of Patents, Designs and Trade Marks*,⁹⁷ Emotional Perception AI Ltd had applied for a patent for an artificial neural network (ANN), an AI system used '... to provide an improved system for providing media file recommendations to an end user, including sending a file and message in accordance with the recommendation'.⁹⁸ The invention in question involved an ANN trained to recognize files including music of similar characteristics and categorize them based on this similarity and ultimately recommend them to users.⁹⁹ As the decision used music as a good use case scenario for the invention, this article follows the same approach here. Through natural language processing, the ANN recognizes similarities between music files, using a semantic description given by humans and creates coordinates (notional spaces) between the two music files depending on how close they are in terms of similarity.¹⁰⁰ The ANN is also trained to characterize the similarity in the physical properties of the two music files based on physical characteristics such as loudness, tone and speed.¹⁰¹ By combining the semantic and physical similarities between two music files, the ANN categorizes similar music files and provides recommendations to users. In simple terms, the AI software in question is an advanced file recommender that is able, for instance, to recommend songs that users are likely to enjoy by comparing the similarity between their preferred songs and other songs in a database. 'Once trained, the ANN can then be used to identify, swiftly and accurately, files from a database which correspond semantically to a target file, and to provide—against [sic] swiftly and accurately—file recommendations to a user device (over a communication network)'.¹⁰²

The UKIPO refused to grant a patent for this invention, treating the ANN as excluded subject matter under section 1(2)(c). The Hearing Officer concluded that an ANN falls squarely within the excluded subject matter as it fails to meet the criteria of technical effect. The ANN was therefore treated as a computer programme as such within the meaning of section 1(2)(3).

⁹³ European Patent Convention Art. 52(2)(c).

⁹⁴ Klaus H Offermann (ed) 'The Patentability of Computer Programs Discussion of European-Level Legislation in the Field of Patents for Software' European Union Directorate-General for Research, Working Paper, JURI 107 EN (2002) 9–10.

⁹⁵ See for instance *Vicom*, T208/84, and *Official Journal of the EPO* 1987, 14.

⁹⁶ UK Patent Act 1977 s. 1(2)(c).

⁹⁷ *Emotional Perception AI Ltd v Comptroller-General of Patents, Designs and Trade Marks* [2023] EWHC 2948 (Ch) (21 November 2023).

⁹⁸ *Ibid* at [4].

⁹⁹ *Ibid*.

¹⁰⁰ *Ibid* at [8].

¹⁰¹ *Ibid* at [9].

¹⁰² *Emotional Perception AI Limited*, BL O/542/22 (22 June 2022) (UK IPO [53]).

⁸⁶ Andrew Nieh, 'Software War: The Patent Menace' (2010) 55 *New York Law School Law Review* 295–327.

⁸⁷ Andrew Nieh (n 86) 313.

⁸⁸ *Ibid*, 309–310.

⁸⁹ *Ibid*, 308.

⁹⁰ 45 F.3d 943 (Fed. Cir. 2008), *aff'd sub nom. Bilski v Kappos*, 130 S. Ct. 3218 (2010). Defines the contours of patenting software. See also *State Street Bank & Trust Co. v Signature Fin. Group*, 149 F.3d 1368, 1370 (Fed. Cir. 1998).

⁹¹ Andrew Nieh (n 86) 325–26.

⁹² *Ibid* at 320. 'But there is also a legal justification as to why software should not be patented. A basic principle under patent law is that "laws of nature, natural phenomena, and abstract ideas" cannot be patented. Algorithms fall under this exception as well.'

The decision of the UKIPO was overturned on appeal. The difference in the decision at the UKIPO and at High Court was in the application of the requirements of EPO Article 52(2)(c)/section 1(2)(c) of the UK Patent Act.

*Aerotel Ltd v Telco Holdings Ltd*¹⁰³ introduced a four-stage assessment to determine the eligibility of computer programmes under section 1(2)(c). These four steps are '(1) properly construe the claim; (2) identify the actual contribution; (3) ask whether it falls solely within the excluded subject matter; and (4) check whether the actual or alleged contribution is actually technical in nature'.¹⁰⁴ In summary, once the claim is identified, the assessor or judge should examine if the invention for which the patent is claimed makes a contribution different from the existing state of the art.¹⁰⁵ The fact that the invention makes some contributions does not necessarily mean that it is automatically eligible for a patent. The contribution must not be within one of the excluded subject matters. Thus, if the contribution is a computer programme, that is potentially an excluded subject matter. Nevertheless, the mere fact that a contribution is a computer programme in itself does not conclude the assessment. A computer programme could still be eligible if it makes a technical contribution, because what is excluded is a computer programme as such. Requests for patents for software fail usually at the third or fourth steps, where the biggest challenge lie.

Whether a contribution is technical in nature or if so, whether the technical contribution itself is an eligible subject matter, has been difficult to determine in practice. UKIPO and the courts use the AT&T signposts to determine whether a contribution is technical.¹⁰⁶ The AT&T lays out the following five non-exhaustive factors that would suggest that a computer programme has a technical effect:¹⁰⁷

- (a) whether the claimed technical effect has a technical effect on a process which is carried on outside the computer;
- (b) whether the claimed technical effect operates at the level of the architecture of the computer; that is to say whether the effect is produced irrespective of the data being processed or the applications being run;
- (c) whether the claimed technical effect results in the computer being made to operate in a new way;
- (d) whether there is an increase in the speed or reliability of the computer;
- (e) whether the perceived problem is overcome by the claimed invention as opposed to merely being circumvented.

The AT&T signposts provide clarity in assessing technical effect, but do not completely remove controversies. In *Protecting Kids*, the hearing officer at the UKIPO refused to grant a patent for a computer programme that monitors electronic communications on a device, creates a score of the communication based on the risk of inappropriate communications and sends a message to a user with alternative course of action, concluding that the actual contribution of the invention constitutes a computer programme as such or a method of performing mental act, thus failing to meet

the requirement of technical contribution.¹⁰⁸ This was reversed on appeal where Mr Justice Floyd (as he then was) found that there was a technical effect, arguing:

The effect here, viewed as a whole, is an improved monitoring of the content of electronic communications. The monitoring is said to be technically superior to that produced by the prior art. That seems to me to have the necessary characteristics of a technical contribution outside the computer itself.¹⁰⁹

Similarly, in *Halliburton*, a decision to refuse a patent for a computer programme used to simulate the designing of drilling equipment for wells,¹¹⁰ was reversed on appeal. The patent examiner had concluded that the invention was 'excluded from patentability as a scheme or method for performing a mental act and as a computer programme as such'.¹¹¹ On appeal, Mr Justice Birss (as he then was) concluded that:

Designing drill bits is obviously a highly technical process, capable of being applied industrially. Drill bit designers, I am sure, are highly skilled engineers. The detailed problems to be solved with wear and the ability to cut rocks and so on are technical problems with technical solutions. Accordingly, finding a better way for designing drill bits in general itself is a technical problem. This invention is a better way of carving that out. Moreover, the detailed ways in which this method works—the use of finite element analysis—is itself highly technical.¹¹²

A series of decisions in patenting computer programmes demonstrate that patent examiners generally reject applications, which leads to litigation. *Emotional Perception* is one of a series of cases where the patent examiner found that the invention in question was a programme for computer as such and thus fell within the exclusion, due to lack of technical effect.¹¹³ The hearing officer argued in particular that:

However, where it may represent something specific and external to the computer is in the provision to a user of an improved file recommendation. It is not the mere sending of a file over a network which makes this a process external to the computer—this transmission process is achieved in a standard fashion and operates wholly within the conventional computer network. It is external to the computer in the sense that there is a beneficial effect on the end user in being provided with a better recommendation, such as a song they are likely to enjoy. However, such a beneficial effect is of a subjective and cognitive nature and does not suggest there is any technical effect over and above the running of a programme on a computer.¹¹⁴

On appeal, Sir Anthony Mann disagreed, concluding that:

The correct view of what happened, for these purposes, is that a file has been identified, and then moved, because it fulfilled certain criteria ... So the output is of a file that would not

¹⁰³ *Aerotel Ltd v Telco Holdings Ltd* (EWCA Civ 1371 (2006)).

¹⁰⁴ *Ibid* at [40].

¹⁰⁵ *Ibid* at [43]. 'The second step—identify the contribution—is said to be more problematical. How do you assess the contribution? Mr Birss submits the test is workable—it is an exercise in judgment probably involving the problem said to be solved, how the invention works, what its advantages are. What has the inventor really added to human knowledge perhaps best sums up the exercise. The formulation involves looking at substance not form—which is surely what the legislator intended.'

¹⁰⁶ *AT&T Knowledge Ventures* [2009] EWHC 343, [40] Pat, Lewison J.

¹⁰⁷ *Ibid*.

¹⁰⁸ *Protecting Kids, the World Over (PKTWO) Limited*, BL O/439/10 (23 December 2010) (UK IPO) [34].

¹⁰⁹ *Protecting Kids, The World Over (PKTWO) Ltd* [2011] EWHC 2710 (Pat) [34].

¹¹⁰ *Halliburton Energy Services Inc*, BL O/170/11 (19 May 2011) (UK IPO) [5–8].

¹¹¹ *Ibid* at [18].

¹¹² *Halliburton Energy Services Inc* [2011] EWHC 2508 (Pat) (5 October 2011) [74].

¹¹³ *Emotional Perception AI Limited* (UK IPO) at [69] and [83].

¹¹⁴ *Ibid* at [69].

otherwise be selected. That seems to me to be a technical effect outside the computer for these purposes, and when coupled with the purpose and method of selection it fulfils the requirement of technical effect in order to escape the exclusion.¹¹⁵

Sometimes, even if the invention is considered to have technical effect and therefore not 'a programme for computer as such', it could be excluded because the technical effect itself is not patent eligible. This was the case in *Macrossan* involving an application for 'a patent for an automated method of acquiring the documents necessary to incorporate a company', which was considered patent ineligible because the programme only enabled a method of doing business.¹¹⁶

The overview of various cases involving patenting software suggests that there are significant legal challenges to obtaining patents, leading to litigation. The process has not only cost implications but also implications in terms of potential disclosure of new inventions without having secured the patent or having put in place non-disclosure agreements during lengthy litigation. Thus, it would not be unreasonable if businesses preferred trade secrecy to protect software programmes as opposed to patent. From the perspective of transparency, relying on patents as a means of getting disclosure of information on the functioning of the software seems to ignore the fact that computer programmes are frequently updated and the decisions or predictions they make in a particular case might not necessarily correspond to any other variation in similar circumstances. In machine learning AI, this is particularly the case, as the very essence of the programme is for the system to update its decision-making model through experience. Therefore, the suggestion of removing trade secrecy, and imposing patent under any circumstance with the view to promoting transparency in ADM does not appear to be justifiable and as helpful as imagined. Instead, a measured disclosure system that balances conflicting interests, on a case-by-case basis should be adopted. The current legal framework would be sufficient to allow that with additional guidelines.

5. Conclusion

This article examined the implications of replacing trade secret protection with mandated patent protection for algorithms,

aiming to enhance transparency in decision-making processes. Through a comprehensive analysis, it has demonstrated that the conflict between algorithmic transparency and trade secrecy are reconciled through a balancing exercise. Although the EU lacks detailed guidance in the context of ADM, the CJEU has recently reaffirmed that it is up to the national courts to consider the rights and freedoms of individuals, including data protection rights, and the trade secrecy of businesses in making the balancing test. The analysis of case law from the USA also shows how this can be achieved. The article therefore argued that there is no need for major legislative reform to address the challenge.

The existing literature also advocated for the partial or complete abolition of trade secret protection of algorithms that can be used to make automated decisions. This article demonstrated the complexities of patenting software and AI, identifying legal and practical challenges that must be taken into consideration, both from the perspective of protecting the rights of individuals, the public's interest in transparency as well as the perspectives of business, particularly in relation to competitiveness and legal certainty. The inherent uncertainties associated with patenting AI pose significant risks to investment in the field, potentially stifling innovation and growth. Furthermore, even if these uncertainties were to be mitigated, trade secret protection remains a viable alternative for businesses pursuing different strategic objectives or aiming to protect specific information and/or business models. Consequently, advocating for the total elimination of trade secret protection for algorithms is unrealistic.

The article recognises the necessity of striking a delicate balance between trade secret protection and algorithmic transparency requirements, but submits that existing judicial decisions and legislation could be used to engage in such a balancing exercise without major legislative changes.

In conclusion, while patenting AI is possible and should remain one of the available options, trade secret should still be considered a viable solution that can be appropriately coordinated with other competing interests requiring only the disclosure of information that is necessary for achieving algorithmic transparency proportionately.

Conflict of interest. None declared.

¹¹⁵ *Emotional Perception AI Ltd v Comptroller-General of Patents, Designs and Trade Marks* [2023] EWHC 2948 at [76].

¹¹⁶ *Aerotel Ltd v Telco Holdings Ltd, Aerotel* [58]–[74].