Friends, Secrets, and AI: The Tension Between Digital Trade Secrets and Transparent AI in the Age of ChatGPT

3/2025 4.6.2025

Friends are an integral part of our lives, and one of the hallmarks of a good friend is their ability to keep our deepest secrets. By comparison, digital trade secrets are a good friend for ChatGPT because they keep its inner secrets (algorithms and source codes) legally under lock and key. The friendship is increasingly coming nder scrutiny as the public is now demanding a reasonable explanation of how this technology works to d trust in its outputs. This has ignited a debate regarding the balance between transparent AI and the

protection of digital trade secrets. The legal basis for digital trade secret protection derives from international agreements, such as the Agreement on Trade-Related Aspects of Intellectual Property Rights[i] ⚓ (TRIPS), as well as regional frameworks like the EU's Trade Secret Directive[ii] ⚓ (TSD). These frameworks provide for the protection of digital trade secrets while acknowledging the need for transparency in certain situations. Yet, attaining meaningful transparency in ChatGPT which operates on a closed source[iii] ⚓ policy, is a daunting task. However, the demands for transparency are only expected to grow with the coming on the market of DeepSeek[iv] ⚓ which purportedly operates based on open-source policy. [v] ⚓ At this point, two questions need to be addressed. What is meant by transparent AI, and is there such a "thing" as a "digital" trade secret?

Transparent AI

As you might have guessed, the concept of transparent AI is fluid and this is because it means different things to different people. For instance, some scholars are of the view that transparent AI refers to making the functionality of an AI system understandable to humans.[vi] ⚓ Yet others opine that it involves providing explanations for the system's decisions and behaviours.[vii] ⚓ From these views, it can be said that transparent AI represents two possible aspects. Firstly, humans must have a fair understanding of the architectural structure of an AI system and secondly, there must be a possibility of understanding or explaining the system's decisions. My view is that regardless of how transparent AI is understood, its goals remain uniform and include among other things; accountability and user trust.

Many people believe that AI systems should be accountable for their decisions and this means that there should be a way of tracking how decisions are made and to hold someone responsible for any harm caused.[viii] ⚓ From a public interest`s perspective, Transparent AI builds user trust by making it clear how it works and what its limitations are.[ix] ⚓ Majority of the people believe that this encourages users to feel more comfortable using AI systems like ChatGPT.[x] ⚓ Therefore, when jurisdictions develop regulations for AI systems, transparency is often a key component. For example, the EU's Artificial Intelligence Act[xi] ⚓ (AIA) in Article 53 and the General Data Protection Regulation[xii] ⚓ (GDPR) in Article 14 address transparency in context of personal data collection.[xiii] ⚓

Digital Trade Secrets

The concept of digital trade secret is not new, perhaps what makes it seem relatively new is the addition of the word "digital" to the phrase. This concept refers to confidential and commercially valuable information which is stored and transmitted in electronic formats.[xiv] ⚓ This information includes algorithms, codes, images, audio, and video data. On the other hand, "traditional" trade secrets refer to information with commercial value that is not generally known, and is kept secret through reasonable measures.[xv] ⚓ This can include formulas, strategies, devices, processes, and recipes. This information can be stored mentally or expressed in texts, figures and software code.[xvi] ⚓ Therefore, digital trade secrets are a subcategory of trade secrets and specifically refer to data or information stored and transmitted in electronic formats. This also means that the law applicable to trade secrets can generally be used on digital trade secrets. Consequently, I will use the terms interchangeably in this writing.

The Digital Objects that Build ChatGPT

From what has been discussed so far, my view which is also supported by other scholars is that digital objects can be protected as digital trade secrets if they meet the three time-honoured requirements for trade secret protection. [xvii] ⚓ But then what are digital objects? These electronic objects include among other things algorithms, and programming code. Programming code is the language used to create algorithms. It includes the specifics of how ¹gorithms are implemented and can provide important business insights into the handling and utilization of data.

[xviii] ⚓ What about algorithms? These are essentially a set of instructions or rules designed to solve a specific problem or complete a particular task.[xix] ⚓

Large Language Models (LLMs) like ChatGPT are nothing but a combination of these digital objects and from a logical point of view, should qualify for digital trade secret protection.[xx] ⚓ LLMs can analyse massive datasets, learn probability relationships and become proficient in the grammar of one or more languages.[xxi] ⚓ In particular, ChatGPT is based on a neural network architecture called a transformer model. This makes it so advanced that it can respond to human language by producing coherent text that is not easily differentiated from a text prepared by a natural human being.[xxii] ⚓ As a result, these models have amassed commercial value, and their creators are increasingly treating them as digital trade secrets to maintain a competitive advantage over their rivals. I will return to this issue later.

The protection of digital trade secrets is a complex issue in the context of ChatGPT. The vast datasets used to train ChatGPT and its probabilistic response generation make it challenging to determine which specific elements qualify as digital trade secrets. Also, the need for transparency may conflict with protecting underlying algorithms or training data as trade secrets. To ably analyse this collision, I will first spark a discussion demonstrating that ChatGPT and its building blocks can qualify for digital trade secret protection (and perhaps, OpenAI has kept it as a digital trade secret). Thereafter, I will analyse the tug-of-war between these two competing concepts within the EU and provide possible ways through which transparency can be enhanced in ChatGPT.

ChatGPT: A Digital Trade Secret?

There are several factors that show that OpenAI[xxiii] ⚓ treats ChatGPT as a digital trade secret. For example, and as I have explained above, the first requirement for obtaining a digital trade secret is to demonstrate that the digital object has been kept as a secret. How is this requirement fulfilled in the context of ChatGPT? OpenAI has not publicly disclosed the details of ChatGPT's algorithms or its full training dataset.[xxiv] ⚓ This information remains confidential, known only to a limited group within the company.[xxv] ⚓ There can only be one logical explanation, this controlled approach to information dissemination aligns with the need to maintain secrecy for digital trade secret protection.[xxvi] ⚓ Although some aspects of ChatGPT could be patentable, OpenAI has obtained very few patents for its technology. One possible explanation for this is that OpenAI is choosing to protect its technology as a trade secret which offer longer duration of protection as compared to a patent.[xxvii] ⚓ However, to be eligible for digital trade secret protection more is required than simply showing that the digital object has been kept as a secret. It must also be shown that it has commercial value.

As you may recall, demonstrating that a digital object holds commercial value is the second requirement for qualifying as a digital trade secret. Arguably, this is the easiest element to satisfy in the context of ChatGPT. The commercial value for this technology can be perceived from its worldwide use which potentially translate into revenue streams. These potential revenue streams likely include paid subscription plans for enhanced access to ChatGPT's features. To the plus side, developers and businesses can integrate ChatGPT into their own applications and services through paid API access.[xxviii] ⚓ Equally, OpenAI offers customized solutions for businesses, tailoring ChatGPT to their specific needs. Taken together, this demonstrates that the question of whether ChatGPT has commercial value has an obvious answer. However, does this automatically qualify ChatGPT for digital trade secret protection? No, the final requirement must also be met.

The last step in acquiring digital trade secret is met by demonstrating that positive steps have been taken to keep the digital object confidential. Is this true in the context of ChatGPT? It is common knowledge that developers of closed-source generative AI models, like ChatGPT, are putting in place strategies to keep their technology confidential. The reasons are obvious-they want to remain ahead of their competitors.[xxix] ⚓ For example, ChatGPT's terms of use include prohibitions against reverse engineering and confidentiality requirements for businesses that acquire an Enterprise License. [xxx] ⚓ It may be argued that the use of these terms in themselves may not be sufficient to conclude that OpenAI is trying to take positive steps to keep ChatGPT secret. However, when this position is considered in view of the other two requirements, the picture becomes complete: ChatGPT is ital trade secret, although in disguise. I hasten to say that eventually, whether ChatGPT qualifies for trade

secret protection would depend on how competent authorities like courts would assess the specific facts and circumstances.

The Tug of War

Treating ChatGPT as a digital trade secret by hiding its core technology form the public, offers OpenAI a significant competitive advantage over its competitors.[xxxi] ⚓ This secrecy creates a barrier to entry for potential rivals and helps OpenAI maintain its dominant position in the generative AI market. Additionally, the ability to protect its valuable technology as a digital trade secret makes OpenAI more attractive to investors and potential partners. For example, Microsoft's substantial investment in OpenAI is likely influenced by the perceived value of OpenAI's intellectual property, including its trade secrets.[xxxii] ⚓

Such investments by and large contribute to the economic and social emancipation of societies in general. However, limiting the understanding of ChatGPT decision-making processes by keeping it as a secret raises serious concerns about transparency.[xxxiii] ⚓ A thought that has baffled many people is that if we are benefiting from ChatGPT in many ways, should we be concerned about understanding its inner workings? The answer is the affirmative but why? The lack of transparency makes it challenging to build trust in the system's outputs. For example, in the EU, the GDPR emphasizes transparency in data processing regardless of the economic or societal benefits that come with such processing. Therefore, it should not surprise us that ChatGPT was temporarily banned in March 2023 in Italy for transparency issues.[xxxiv] ⚓

Legal Approaches to Moving ChatGPT Towards Transparency

In the EU, the TSD provides a framework for navigating the tension between transparency and digital trade secret protection in the context of AI systems like ChatGPT. This can be achieved through a careful consideration of what qualifies as a trade secret, exceptions to that protection for public interest reasons, and the existence of transparency obligations that enable access to information. The goal is to achieve a balance that promotes both innovation and public oversight of AI systems like ChatGPT. I now turn to discussing each of these balancing techniques in the paragraphs below.

I will start by arguing that not all information related to an AI system like ChatGPT qualifies for digital trade secret protection in the EU. This is possible thanks to the TSDs strict definition of what qualifies as digital trade secrets. As already mentioned, for a digital object or information to qualify for protection, it must be a Secret. Therefore, some information, such as the user interface or the outputs of a generative AI model like ChatGPT, may be self-disclosing and not eligible for trade secret protection.[xxxv] ⚓ Even if some information is strongly considered to have commercial value by OpenAI, it may not qualify for trade secret protection as the three time-honoured requirements for trade secret protection are cumulative in nature and thus must all be met.[xxxvi] ⚓ This means that some measure of transparency in ChatGPT maybe achieved to the extent that some of information does not qualify for digital trade secret protection.

Furthermore, the TSD recognizes exceptions to trade secret protection based on public interest grounds. However, what constitutes public interest is always a contentious matter. It is however, safe to mention that freedom of expression and information is considered a matter of public interest because it is specifically provided for under Article 19 of the TSD.[xxxvii] ⚓ This exception, is rooted in the Charter of Fundamental Rights of the EU which allows for the disclosure of trade secrets when it is necessary for exercising the right to freedom of expression and information. How can this exception move AI systems like ChatGPT towards transparency? The freedom of expression exception ensures that the public's right to receive and impart information is not overridden by digital trade secret protection.[xxxviii] ⚓ This means that even if certain details about ChatGPT's inner workings or training data are considered digital trade secrets, they can be disclosed if such disclosure is necessary for exercising the right to freedom of expression.

Related to the above is article 20 of the TSD which provides for whistleblowing.[xxxix] ⚓ The freedom of expression exception is closely linked to the protection of whistleblowers. Whistleblowers can reveal misconduct,

wrongdoing, or illegal activity related to AI, and this exception ensures that they are protected when their disclosures serve the public interest. This exception makes it clear that not all information related to AI can be shielded from public scrutiny. I must be quick to mention that when access to information is requested, public authorities are required to weigh the public interest in such disclosure against the trade secret holder's interest in confidentiality. The competent authorities in line with article 21 of the TSD which provides for the principle of proportionality, should consider factors like the value of a trade secret, the seriousness of the conduct resulting in its unlawful disclosure, and the impact of such conduct.[xl] Actually, proportionality is what OpenAI is claiming for being fined and tasked to educate the public about its inner workings for the March 20, 2023 technical glitch. I eagerly await to see how the authorities will strike this delicate balance.

Apart from the EU's TSD, the AIA includes several transparency obligations for different types of AI systems and those who develop or use them. For example, recital 101 of the AIA requires providers of general-purpose AI models to draw up and keep up to date technical documentation.[xli] The documentation envisaged under the AIA is one that provides information on the AI model's usage and enables downstream providers to understand its capabilities and limitations.[xlii] This is because the framers of the AIA recognize that trade secrets are important for encouraging innovation, but also that transparency is essential for building trust in AI and for ensuring that it is used safely. However, generating detailed technical documentation can be costly and time-consuming, particularly for complex AI systems like ChatGPT. These systems are dynamic and continuously evolve as they process new data. This makes it challenging to maintain accurate and up-to-date documentation.[xliii]

From the GDPR perspective, transparency can be enhanced in ChatGPT by providing users with an opt-out option for data collection which allows them to control their personal data.[xliv] This could make it in line with Article 13 of the GDPR which encompasses the principle of transparency and requires that users are informed about who is collecting their data and for what purpose.[xlv] Even when user data was collected from the internet via web scraping or from other sources to train ChatGPT, users should at least be informed if and how their data are used to train the system.[xlvi]

I must say that to move ChatGPT to full transparency is a daunting task. This stems from its complex architectural design, and the possibility to legally dodge scrutiny in the name of digital trade secret protection. These limitations may affect its compliance with laws like GDPR, AIA and TSD.[xlvii] While these laws may not provide the expected silver bullet in moving ChatGPT towards transparency in the EU, they provide a good starting point in regulating such complex LLMs systems.

Final Remarks

The tension between keeping ChatGPT as a digital trade secret and moving it towards transparency has been brought to the fore. Keeping it as a digital trade secret commercially benefits its proprietors and gives them a competitive advantage in the market. Also, digital trade secrets promote innovation and in that way benefit societies. On the other end of the spectrum, we, the users of this technology demand some measure of transparency so that trust can be built into its outputs. In the EU for example, I have demonstrated how some modicum of transparency can be achieved through various mechanisms, such as a stricter interpretation of what a digital trade secret is and public interest demands under the TSD.

Going back to the hypothetical friendship that exists between ChatGPT and digital trade secrets, I conclude by emphasising that the legally moving ChatGPT towards transparency at the expense of digital trade protection, should not terminate or sour this friendship. The reason is that even good friends are sometimes compelled by law, to reveal their friends' innermost secrets.

---

[i] 'WIPO Lex, Treaties, Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement)' <https://www.wipo.int/wipolex/en/treaties/details/231> accessed 28 January 2025.

[1] 'DIRECTIVE (EU) 2016/ 943 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL – of 8 June – on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) against

Their Unlawful Acquisition, Use and Disclosure'.

[iii] ⚓ Software whose source code is not publicly available is referred to as a closed source. You cannot copy, alter, or remove any element of the code without authorisation. This contrasts with open source. See https://encyclopedia.kaspersky.com/glossary/closed-source/ accessed 28 Jan. 25

[iv] ⚓ DeepSeek is the name of a Chinese free AI-powered chatbot, which looks, feels and works very much like ChatGPT.

[v] ⚓ Cade Metz, 'What Is DeepSeek? And How Is It Upending A.I.?' *The New York Times* (27 January 2025) <https://www.nytimes.com/2025/01/27/technology/what-is-deepseek-china-ai.html> accessed 28 January 2025.

[vi] ⚓ Naomi Aoki and others, 'Explainable AI for Government: Does the Type of Explanation Matter to the Accuracy, Fairness, and Trustworthiness of an Algorithmic Decision as Perceived by Those Who Are Affected?' (2024) 41 Government Information Quarterly 101965 <https://linkinghub.elsevier.com/retrieve/pii/S0740624X24000571> accessed 2 December 2024.

[vii] ⚓ Hans De Bruijn, Martijn Warnier and Marijn Janssen, 'The Perils and Pitfalls of Explainable AI: Strategies for Explaining Algorithmic Decision-Making' (2022) 39 Government Information Quarterly 101666 <https://linkinghub.elsevier.com/retrieve/pii/S0740624X21001027> accessed 2 December 2024.

[viii] ⚓ Ulla-Maija Mylly, 'Transparent AI? Navigating Between Rules on Trade Secrets and Access to Information' (2023) 54 IIC – International Review of Intellectual Property and Competition Law 1013 <https://link.springer.com/10.1007/s40319-023-01328-5> accessed 30 November 2024.

[ix] ⚓ Mylly (n 9).

[x] ⚓ Aoki and others (n 7).

[xi] ⚓ 'Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)Text with EEA Relevance.'

[xii] ⚓ 'Regulation – 2016/679 – EN – Gdpr – EUR-Lex' <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> accessed 27 January 2025.

[xiii] ⚓ F Gualdi and A Cordella, 'Theorizing the Regulation of Generative AI: Lessons Learned from Italy's Ban on ChatGPT' (2024).

[xiv] ⚓ 'WIPO Guide to Trade Secrets and Innovation – Part VII: Trade Secrets and Digital Objects' (*WIPO Guide to Trade Secrets and Innovation*) <https://www.wipo.int/web-publications/wipo-guide-to-trade-secrets-and-innovation/en/part-vii-trade-secrets-and-digital-objects.html> accessed 30 November 2024.

[xv] ⚓ 'Understanding the Uniform Trade Secrets Act' (*Freiberger Haber LLP*, 4 April 2018) <https://fhnylaw.com/understanding-uniform-trade-secrets-act/> accessed 2 December 2024.

[xvi] ⚓ 'WIPO Guide to Trade Secrets and Innovation – Part VII: Trade Secrets and Digital Objects' (n 18).

[xvii] ⚓ Hawraa Hammoud, 'Trade Secrets and Artificial Intelligence: Opportunities & Challenges' [2020] SSRN Electronic Journal <https://www.ssrn.com/abstract=3759349> accessed 30 December 2024.

[xviii] ⚓ 'WIPO Guide to Trade Secrets and Innovation – Part VII: Trade Secrets and Digital Objects' (n 18).

[xix] ⚓ Tiffany C Li, 'Algorithmic Destruction' (2022) 75 SMU Law Review 479 <https://scholar.smu.edu/smulr/vol75/iss3/2/> accessed 25 December 2024; Joshua A Goland, 'Algorithmic Disgorgement: Destruction of Artificial Intelligence Models as the FTC's Newest Enforcement Tool for Bad Data' [2023] SSRN Electronic Journal <https://www.ssrn.com/abstract=4382254> accessed 27 December 2024.

⚓ Hammoud (n 29).

[xxi] ⚓ 'Edpb_20240523_report_chatgpt_taskforce_en.Pdf' <https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf> accessed 20 December 2024.

[xxii] ⚓ 'Edpb_20240523_report_chatgpt_taskforce_en.Pdf' (n 33).

[xxiii] ⚓ OpenAI is an American company that owns ChatGPT.

[xxiv] ⚓ William (Bill) J Samore, 'Patent Landscape Report: Generative Artificial Intelligence' (*PatentNext*, 12 August 2024) <https://www.patentnext.com/2024/08/wipo-issues-a-patent-landscape-report-on-generative-artificial-intelligence-genai/> accessed 30 November 2024.

[xxv] ⚓ Samore (n 45).

[xxvi] ⚓ Aki Tomita, 'Open Technology Management for Maximizing the Public Value of Large Language Models', *2024 Portland International Conference on Management of Engineering and Technology (PICMET)* (2024) <https://ieeexplore.ieee.org/document/10652994/?arnumber=10652994> accessed 13 December 2024.

[xxvii] ⚓ Samore (n 45).

[xxviii] ⚓ 'WIPO Guide to Trade Secrets and Innovation – Part VII: Trade Secrets and Digital Objects' (n 18).

[xxix] ⚓ Tomita (n 47).

[xxx] ⚓ Steve (n 22).

[xxxi] ⚓ ChatGPT's dominance is doubtful with the advent of cheaper and more effective models like DeepSeek.

[xxxii] ⚓ Samore (n 45).

[xxxiii] ⚓ Steve (n 28).

[xxxiv] ⚓ Antonio Cordella and Francesco Gualdi, 'Regulating Generative AI: The Limits of Technology-Neutral Regulatory Frameworks. Insights from Italy's Intervention on ChatGPT' (2024) 41 Government Information Quarterly 101982 <https://www.sciencedirect.com/science/article/pii/S0740624X24000741> accessed 30 November 2024.

[xxxv] ⚓ Steve (n 22).

[xxxvi] ⚓ Mylly (n 9).

[xxxvii] ⚓ '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' (n 2).

[xxxviii] ⚓ Mylly (n 9).

[xxxix] ⚓ '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' (n 2).

[xl] ⚓ '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' (n 2).

[xli] ⚓ 'Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) Text with EEA Relevance.' (n 13).

[xlii] ⚓ Wang (n 59).

[xliii] ⚓ Sophia Worth and others, ‘AI Data Transparency: An Exploration through the Lens of AI Incidents’ <http://arxiv.org/abs/2409.03307> accessed 13 December 2024.

[xliv] ⚓ Wang (n 59).

[xlv] ⚓ Cordella and Gualdi (n 55).

[xlvi] ⚓ ‘Edpb_20240523_report_chatgpt_taskforce_en.Pdf’ (n 33).

[xlvii] ⚓ Luckett (n 62).

Kannen kuva: iStock / Shutter2U

Aiheet: Liikesalaisuus, Tekoäly

Kirjoittajat

Chisanga Mutale

Doctoral candidate, Bachelor of Laws, Master of Intellectual Property and New Technologies University of Turku