

Keeping Secrets in Orbit.

A Preliminary Study of Trade Secret Protection in Outer Space and in the LEO Commercial Ecosystem

by

Marco Franzoso*

J.D., Adv. LL.M., PhD (Cand.)

Abstract

International space law, through Article XI of the Outer Space Treaty (OST), obliges states to inform the international community "to the greatest extent feasible," a transparency mandate now in tension with the commercial space economy's need to protect sensitive information as trade secrets. This structural unease sharpens once terrestrial assumptions about secrecy, access control, and physical containment are carried into orbit. This paper offers a preliminary study of that tension, mapping the doctrinal terrain rather than proposing a definitive solution, built around a redefinition of "reasonable measures" in orbital contexts. First, it examines whether Article XI's "feasible and practicable" qualifier leaves normative space for confidentiality, or instead imposes a transparency logic at odds with trade secret protection. Second, it surveys domestic trade secret regimes and their reach in non-territorial, multi-jurisdictional orbital operations. Third, it considers the outer limits of trade secret protection, terrestrial and orbital alike. The paper argues that "reasonable measures" cannot remain a static terrestrial standard: across satellite communications, commercial space stations, private astronauts, and space-sector employment, Earth-based protective measures often become impracticable, disproportionate, or legally incomplete in orbit. Trade secret law, properly calibrated, functions as a conditional shield: flexible enough to coexist with OST Article XI's disclosure duty, yet bounded by outer limits rooted in data protection, AI transparency, and constitutional law.

Keywords: Trade Secrets, OST, LEO, Reasonable Measures, AI Transparency

Word count (excl. Abstract, Cover Page, Table of Contents, Footnotes, Main Title): **7.415**

Marco Franzoso, J.D. (University of Padova), Adv. LL.M. (Leiden University), is a PhD Candidate under the Marie Skłodowska-Curie Actions (MSCA) Doctoral Network SPARE, jointly hosted by Ludovika University of Public Service (Budapest, Hungary) and Thales Alenia Space France (Toulouse, France). He is a legal consultant and researcher specialized in international law, space law, and intellectual property, and previously served as Research Co-Lead at the Space Generation Advisory Council (SGAC) and Legal Counsel at Studio Legale Veronese, Italy. He is a Prospective Member of the International Institute of Space Law (IISL) and an Alumnus of the International Institute of Air and Space Law (IIASL). ORCID: 0009-0000-1818-9671.

marco.franzoso@thalesalieniaspace.com; m.franzoso21@gmail.com.

KEEPING SECRETS IN ORBIT. A PRELIMINARY STUDY OF TRADE SECRET PROTECTION IN OUTER SPACE AND IN THE LEO COMMERCIAL ECOSYSTEM

1	INTRODUCTION. VINEYARDS AND ANTENNAS.....	3
2	TRADE SECRET LAW: A GLOBAL OVERVIEW AND ITS TERRESTRIAL CONSTRAINTS.	4
2.1	DEFINITION AND VARIATION: THE THREE-PART TEST.....	5
3	THE INTERNATIONAL OBLIGATION REGARDING SPACE TRANSPARENCY AND INFORMATION SHARING.....	7
3.1	THE CONTENT OF THE OBLIGATION AND ITS CURRENT STATUS.	8
4	HOW TO KEEP SECRETS IN ORBIT. A RETHINKING OF “REASONABLE MEASURES” IN OUTER SPACE.	10
4.1	PROTECTING SECRETS DURING SATELLITE COMMUNICATION.....	11
4.2	PROTECTING SECRETS ON COMMERCIAL SPACE STATIONS.....	13
4.3	BALANCING TRADE SECRET PROTECTION AND EMPLOYERS’ RIGHTS IN THE SPACE SECTOR	13
5	OUTER SPACE AND OUTER LIMITS: THE BOUNDARIES OF TRADE SECRETS PROTECTION IN ORBIT.....	15
5.1	THE FIRST OUTER LIMIT: GDPR AND THE RIGHT TO INTELLIGIBLE EXPLANATION	16
5.2	THE SECOND OUTER LIMIT: THE EU AI ACT AND TRAINING DATA TRANSPARENCY.....	17
5.3	THE THIRD OUTER LIMIT: AB 2013 AND THE FAILURE OF THE FIRST AMENDMENT SHIELD.....	17
5.4	PRIVACY-BY-DESIGN AS A STRUCTURAL RESPONSE	18
6	CONCLUSION	18

1 Introduction. Vineyards and Antennas.

Camblanes-et-Meynac is a quiet village of approximately 3,000 inhabitants in the Gironde, south of Bordeaux, France. A pleasant, unhurried place, immersed in the green of its trees and fields, surrounded by vineyards that produce some of the finest Bordeaux wines in the world. A place that, as its mayor once remarked, "*tend[s] to get artists*."¹ Among the trees and the low rooftops, however, something was disrupting the view of Camblanes-et-Meynac's inhabitants: a very large antenna. Installed in the garden of a rented house, the device attracted the attention not only of the villagers, but of the French authorities, who discovered - after a thorough investigation - that it had been erected by foreign nationals to capture data from the world's largest satellite constellation, orbiting above the village. The ultimate purpose, according to the prosecution (which remains pending), was to retransmit that information back to their country of origin.² In the twenty-first century, information is the essential fuel of industrial competition, and the race to obtain it, by any means available, is neither metaphorical nor victimless.³

In such a competitive environment, technological innovation and advantage, being the most important assets of any knowledge-intensive business, must be protected from competitors in order to preserve the firm's competitive edge.⁴ Yet the current norms governing such protection are based solely on terrestrial precedents and scenarios, having never been required to interact with extraterrestrial environments before today. When that information derives its value from remaining undisclosed, and is actively protected as such, it qualifies as a "trade secret." Trade secrets constitute a category of industrial property whose protection is conditioned on the holder's active conduct: unlike patents or copyright, no registration is required, but the holder must demonstrate that the information was subject to "*reasonable steps under the circumstances*" to maintain its secrecy - the standard common to TRIPS Art. 39(2)(c), EU Directive 2016/943 Art. 2(1)(c), and UTSA §1(4), as well as DTSA.⁵ The standard is neither absolute nor perfectionist: courts assess proportionality, industry custom, and cost-benefit balance, not the ultimate success of the protective measures.⁶ Critically, the reasonable measures inquiry and the liability inquiry operate independently: a successful breach does not retroactively negate the reasonableness of prior protective conduct,⁷ just as a bank robbery does not render a vault unreasonable. The accused may escape liability by demonstrating independent development, lawful reverse engineering, or - most powerfully - that the information was never properly protected at all, and therefore never qualified as a trade secret in the

¹ Hugh Schofield, 'Suspected Chinese spies arrested in quiet French town' *BBC News* (6 February 2026) <https://www.bbc.com/news/articles/cwy8yw98l2xo>.

² Ibid.

³ Claudia Ray, Joseph Loy and Josh Berlowitz, 'Trade secrets laws are more relevant than ever' in Claudia Ray and Joseph A Loy, *Trade Secrets 2026* (Chambers Global Practice Guide 2026) 5.

⁴ Ibid 6.

⁵ Agreement on Trade-Related Aspects of Intellectual Property Rights (adopted 15 April 1994, entered into force 1 January 1995) 1869 UNTS 299, art 39(2)(c); 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 OJ L 157/1, art 2(1)(c); Uniform Trade Secrets Act § 1(4) (1979); Defend Trade Secrets Act 18 USC § 1839(3)(a) (2016).

⁶ For the US: *Rockwell Graphic Systems, Inc v DEV Industries, Inc*, 925 F 2d 174 (7th Cir 1991); *Yellowfin Yachts, Inc v Barker Boatworks, LLC*, 898 F 3d 1279 (11th Cir 2018). For the EU: Corte di Cassazione, Sez I, no 698/2023 [Italy]; Bundesgerichtshof (BGH), 16 December 2021, I ZR 186/20 [Germany]. For China: Shenzhen Intermediate People's Court, Case No 3843 (2021), *Yue 03 Min Chu*.

⁷ *Religious Technology Center v Netcom On-Line Communication Services, Inc*, 907 F Supp 1361 (ND Cal 1995).

first place.⁸ It is precisely this last defense that becomes structurally acute in space operations, where the physical, jurisdictional, and technical assumptions underlying terrestrial "reasonable measures" are systematically unavailable.

Factually, today's contestants for the supremacy of outer space, and in particular of Earth's orbits, are wealthy individuals, public-private entities, and even startups.⁹ These entities must obtain a licence from their state of residence, build a space object that is subsequently launched, and then the authorizing state registers that object in the international registry maintained at the United Nations (UN) level.¹⁰ The jurisdiction and control of the authorizing state then extend to that registered object - its own law becomes the applicable law on board. This is the spatial counterpart of the flag principle in admiralty law, subject to the necessary distinctions.¹¹ Here, however, the apparent clarity of the framework begins to dissolve. Outer space activities are so varied and commercially expensive that interactions between operators are essential for any adequate return on investment. When two "foreign" operators (authorized by different states) interact in space, as during the refueling of a rocket or an on-orbit servicing encounter, the primary applicable law is the contract they have previously signed, drafted to address the requirements of an extraterritorial engagement. On one side, jurisdiction (per Article VIII of the OST); on the other, contract law. Where the two may align or diverge lies in cross-references to principles and rules that are inherent in one legal system but absent in another (i.e., the law of tort in the UK differs substantially from its Italian equivalent). International, harmonized private law is therefore of considerable practical utility, filling possible gaps through established norms and commercial custom. Some gaps, however, are still too new and too wide to be addressed by pre-existing instruments. The present paper accordingly proposes a rethinking - a reset - of what constitutes "*reasonable measures*" for trade secret protection in outer space (which, in the opinion of the author, are structurally different from their terrestrial counterparts), advancing an international dialogue on lines of action that may be harmonized, implemented rapidly, and applied consistently across the sector. Only through cooperation and a clear set of rules may a level playing field be ensured, one that sustains healthy competition, encourages innovation, and preserves the long-term sustainability of space activities. And perhaps, in doing so, ensures that places such as Camblanes-et-Meynac are no longer troubled by unwanted antennas among their ancient vineyards.

2 Trade Secret Law: A Global Overview and Its Terrestrial Constraints.

Trade Secrets law is more relevant than ever.¹² The rapid and pervasive expansion of Artificial Intelligence (AI) across virtually every aspect of human endeavour has underscored the need for

⁸ Nathalie Dreyfus, 'Reference Guide: Trade Secrets in 2026' (*Dreyfus*, 10 Dec 2025) <https://www.dreyfus.fr/en/2025/12/10/complete-reference-guide-trade-secrets-in-2026/>; *Courtesy Temporary Service, Inc v Camacho*, 222 Cal App 3d 1278, 272 Cal Rptr 352 (1990).

⁹ Charles Albert, 'The New Space Economy: Trends, Growth & Opportunity' (*VivaTech*, 28 May 2026) <https://vivatech.com/news/the-new-space-economy-trends-growth-and-opportunity>.

¹⁰ Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (opened for signature 27 January 1967, entered into force 10 October 1967) 610 UNTS 205 ('OST'), Article VIII OST; Convention on Registration of Objects Launched into Outer Space (opened for signature 14 January 1975, entered into force 15 September 1976) 1023 UNTS 15 ('REG').

¹¹ Doris König, 'Flag of Ships', *Max Planck Encyclopedias of International Law* (Apr 2009).

¹² n 3, 5.

firms to protect their commercially sensitive information.¹³ Most practitioners and scholars working in this field are currently focused on precisely that intersection (trade secrets and AI) alongside alternative dispute resolution mechanisms.¹⁴ What appears to have received no sustained attention, however, is the intersection of trade secret law with outer space. The present research therefore cannot draw on any sector-specific doctrine, nor on a meaningful body of case law, given the scarcity of both at this stage. Exploring and defining such uncharted territory requires firm doctrinal foundations, and that is the purpose of this chapter, which is descriptive in nature but necessary for the analysis that follows. The focus is placed on the definition of trade secrets, the requirements for qualifying information as such, and the reasonable measures required to maintain that status, across a selection of legal frameworks - both regional and national - currently most relevant to space activities. These include the United States of America (USA), the European Union (EU) and select Member States (France, Italy, Germany, Belgium, and Poland), as well as jurisdictions in the Asia-Pacific region, namely Australia, Japan, India, and China. Given that the general structure and requirements of trade secret law are broadly similar across these systems, the approach taken is to identify and define the constituent elements of the law and to flag differences and jurisdiction-specific variations where relevant. Remedies, criminal liability, and litigation procedures have been excluded from the inquiry as falling outside the scope of the research.

2.1 Definition and Variation: The Three-Part Test

In essence, trade secrets law is part of the broader “family” of Intellectual Property (IP) law, alongside copyright, patents, and trademarks.¹⁵ It also has strong connections with unfair competition norms, given that the misappropriation of trade secrets can generate unlawful competitive advantages (particularly evident in the Chinese framework).¹⁶ At the foundational level, Article 39(2) of the TRIPS Agreement establishes that information qualifies for protection only if it meets three cumulative conditions:¹⁷

- a) it is secret;
- b) it has commercial value because it is a secret;
- c) it has been subject to reasonable steps, under the circumstances, to keep it secret.

These are general, internationally agreed, standards, around which the various frameworks have developed their own variation of it.¹⁸ Particularly, the EU, through the Directive 2016/943 Art. 2(1)(c),¹⁹ has regionally harmonized trade secret protection, and further refined the “secret”

¹³ Marc Zao-Sanders, ‘How People are Really Using AI in 2026’, *Harvard Business Review* (1 Jun 2026), <https://hbr.org/2026/06/how-people-are-really-using-ai-in-2026>.

¹⁴ Makoto Hattori, Rikita Karakawa, Wataru Takagishi, and Taku Shibazaki, ‘Japan. Trends and Developments’ in Claudia Ray and Joseph A Loy, *Trade Secrets 2026* (Chambers Global Practice Guide 2026) 126.

¹⁵ WIPO, ‘Trade Secrets’ (WIPO.int) <https://www.wipo.int/en/web/trade-secrets>.

¹⁶ In the People’s Republic of China, trade secrets protection is based on the Anti-Unfair Competition Law (AUCL), as amended on the 15 Oct 2025 (中华人民共和国反不正当竞争法).

¹⁷ n 5.

¹⁸ *Wright v Gaseweld Pty Ltd* (1991) 22 NSWLR 317 [Australia]; *Beyond Dreams Entertainment v Zee Entertainment Enterprise* (2016) 5 Bom CR 266 [India]; *Calcutta High Court in Tata Motors v State of WB*, No 1773 (2008) [India]; *Saltman Engineering v Campbell Engineering* (1963) 3 All ER 413 [India]; *Bombay Dyeing v Mehar Karan Singh* (2010) 112 BomLR375 [India]; *PepsiCo, Inc v Redmond*, 54 F 3d 1262 (7th Cir. 1995) [US].

¹⁹ 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 OJ L 157/1.

requirement, stating 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.*”²⁰ Accordingly, information is not secret merely because it is obscure or complex to the general public; it must also be inaccessible to the specialist or expert operating in the relevant field (a common requirement also in Japan and in the USA).²¹ Examples of what can be considered trade secrets are: formulas and methods,²² process technologies,²³ marketing research,²⁴ source code,²⁵ internal design,²⁶ software architecture,²⁷ customer lists,²⁸ suppliers list,²⁹ technical patterns,³⁰ know-how,³¹ algorithms,³² and so on.

The other common requirement is that the information has some sort of commercial value, either actual or potential,³³ derived directly: “*from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.*”³⁴ In short, that specific information has a specific value (which can eventually be assessed during litigation, to establish eventual damages) *because* it is a secret; it gives a commercial advantage to its owner.³⁵

Finally, the third criterion is the one that is central for the present research, as well as one of the most litigated. The “reasonable measures” refer to that series of steps, precautions, and adjustments, either active or passive, that the owner of a trade secret has to take in order to maintain the protection of its information.³⁶ Now, these “measures” need not be absolute or perfect, only “reasonable.”³⁷ This adjective is the thorny issue that originated this paper, because it opens the door to an inquiry that is strongly fact-specific to the case at hand. The test is whether the measures are reasonable at the time of the misappropriation, not whether they are ultimately successful;³⁸ whether they are

²⁰ Ibid, art 2(1)(a).

²¹ Unfair Competition Prevention Act (UCPA) (不正競争防止法) 1993 (Japan), art. 2(6). For the US: *Ashland Management Inc v Janien*, 82 NY 2d 395, 407; 624 NE 2d 1007, 1013 (1993).

²² n 16, Article 10, par. 4 [China]; *Arxada Holdings NA v Harvey*, 351 A 3d 519, 557 (Del Ch 2026) [US].

²³ *Walker Manufactory Inc v Hoffman Inc*, 261 F Supp 2d 1054, 1080, (ND Iowa 2003) [US].

²⁴ Industrial Property Code (Legislative Decree n. 30 of 10 Feb 2005), Art. 98 [Italy]; Article 2(6) of the UCPA [Japan]; *Whyte v Schlage Lock Co*, 101 Cal App 4th 1443, 1455-56 (2002) [US].

²⁵ Supreme People’s Court IP Civil Final No. 539 (2024) [China]; *Wellogix Inc v Accenture, LLP*, 716 F 3d 867, 875 (5th Cir 2013) [US].

²⁶ Suprema Corte di Cassazione, Ord No 18958/2023 [Italy].

²⁷ *TouchPoint Solutions Inc v Eastman Kodak Co*, 345 F Supp 2d 23, 28 (D Mass 2004) [US]; Article 2(7) of the UCPA, regarding “Shared Data with Limited Access” [Japan]; Supreme People’s Court IP Civil Final No 1592 (2022) [China].

²⁸ *New Aim Pty Ltd v Leung (No 4)* (2025), FCA 747 [Australia]; *Fireworks Spectacular Inc. v Premier Pyrotechnics Inc*, 86 F Supp 2d 1102, 1106 (D Kan 2000) [US]; *Kevlaer BV v KDV, Elano and others*, Business Court Brussels (2020) [Belgium].

²⁹ *New Aim Pty Ltd v Leung*, n 28. [Australia]; Article 2(6) of the UCPA, [Japan];

³⁰ Supreme People’s Court IP Civil Final No 1667 (2020) [China];

³¹ *X v Aéroports de Paris*, 18/04573, Cour d’Appel de Paris (2020) [France].

³² CJEU C-203/22, *CK v Magistrat der Stadt Wien*, ECLI:EU:C:2025:117, 27 Feb 2025 [EU].

³³ Shenzhen Intermediate People’s Court, Case No 5073 (2020) *Yue 03 Min Chu* [China]; *Tata Motors v State of West Bengal*, n 18 [India].

³⁴ 18 USC §1839 (3)(B).

³⁵ *Sadepan Chimica s.r.l. and Sadepan Chimica NV v [two natural person]*, Tribunale di Milano (2021) [Italy].

³⁶ European Union Intellectual Property Office, *Trade Secrets Litigation Trends In The EU* (EUIPO 2023) 66, https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2023_Trade_Secrets_Litigation_Trends_in_the_EU/2023_Trade_Secrets_Litigation_Trends_Study_FullR_en.pdf.

³⁷ n 7.

³⁸ Ibid.; Tribunale di Bologna, Sez Imprese, No 733/2017, 24 Apr 2017 [Italy].

reasonable in light of costs and benefits, not simply optimal precaution *per se*;³⁹ whether they meet the industry's best practices, in a specific field, at a specific moment in time.⁴⁰

It is, in fact, a thorny issue; even more so when paired with the space sector, which is new, rapidly evolving, lacking a set of established industry best practices, and still heavily reliant on countries' involvement.⁴¹ Earth-focused practitioners, courts, and industries have developed a long and detailed list of what measures are considered reasonable, as will be presented further (§4); however, some of these mostly fail in outer space because of the inherent "nature" of this location. To give some anticipatory examples, on an orbital space station, installing safes or locking components is not advisable, both for weight reasons and safety reasons. This means that, in (a near) future,⁴² when industries thrive in our orbit as well as on celestial bodies, information cannot simply be stored in an Earth-style floating vault; a different measure must be found. Similarly, it would be very difficult for a commercial operator of a space station to keep its supplier list a secret, given the presence of "private astronauts" who can inspect the whole facility and acquire that information. Even more immediate is the problem of possible competitors eavesdropping on commercially valuable information during a satellite communication, as already shown in the *Introduction* (§1) with the Camblanes-et-Meynac case. The introduction of this new sector-specific "reasonable measure" will be the focus of Chapter 4.

3 The International Obligation Regarding Space Transparency and Information Sharing.

Information sharing is not an accessory feature of international space law; it is one of its structural pillars. Article XI of the Outer Space Treaty (OST) gave early and explicit form to this idea by requiring States to inform the United Nations (UN) Secretary-General, the public, and the international scientific community, to the *greatest extent feasible and practicable*, of the nature, conduct, locations, and results of their space activities. Article IX adds another layer, through the duty of due regard and consultation where harmful interference may be caused. The logic is simple: where activities are carried out in a domain without sovereignty, and where those activities may affect others beyond the launching state, information becomes a necessary condition for coordination, ensuring also that the use of outer space would remain peaceful, predictable, and open to international scrutiny. What matters here, however, is not only the existence of that international obligation, but also its structure. Space transparency was designed in a state-centric legal environment, for a world in which the relevant actors were public authorities and the relevant information was intended to support inter-State coordination. That is no longer the whole picture. Today, the space environment is increasingly shaped by private operators, commercial constellations, and technically sensitive activities whose competitive value may depend on secrecy. The chapter therefore begins from the international duty to share information, but immediately moves to the more difficult question: how that duty interacts with the protection of commercially valuable information in a space economy that is no longer exclusively public.

³⁹ n 6, *Rockwell Graphic Systems, Inc v DEV Industries, Inc.*

⁴⁰ *Yellowfin Yachts Inc v Barker Boatworks*, n 6.

⁴¹ n 9.

⁴² Chris Martin, 'Space station developer Axiom Space closes \$525M+ funding round' (*ECIKS.org*, 5 Jun 2026), <https://eciks.org/7332-37592-space-station-axiom-funding-525-million>.

3.1 The Content of the Obligation and Its Current Status.

In April 2026, during the 65th session of the United Nations Committee on the Peaceful Uses of Outer Space's (UN COPUOS) Legal Sub-committee, the International Institute of Space Law (IISL) presented an expert analysis of the current status of the obligation *sub iudice*, clarifying open questions and essential terminology that had remained, for the most part, in obscurity, despite extensive scholarly attention.⁴³ In essence, Article XI of the Outer Space Treaty requires "State Parties" - a group of subjects that must be understood according to a distinction discussed below - to inform the international community at large, including the UN Secretary-General and the scientific community, as well as the "public," of the "*nature, conduct, location, and results*" of the activities they carry out in space, to the "*greatest extent feasible and practicable*."⁴⁴ Following the "expert analysis" interpretation, the subjects of this obligation are, in essence, States. However, as the analysis points out, "*reliance solely on States may delay or otherwise affect information. [...] A balanced approach therefore involves collecting relevant information from non-governmental operators through national licensing and supervision regimes*."⁴⁵ What the IISL is correctly stating is that, in the current context, the information-sharing obligation concerning space activities, albeit relying on States, cannot disregard the role of private operators; thus, in order to comply with the obligation, private players should be required to report all relevant information regarding their activities in space through national systems of licensing and supervision. Moreover, the notion of "activities" is understood broadly, encompassing civil, commercial, and dual-use missions ("*.../ the provision encourages transparency across all types of activities*").⁴⁶ Now that the subjects are clearer, the focus must move to the objects: what kinds of information ought to be shared? And how?

Starting from the "*nature*" component, the expert analysis defines it as the type or purpose of the activity, which seems unproblematic in the broader context of trade secrets protection.⁴⁷ The same can be sustained about the "*location*" requirement, which is defined as "*where the operation occurs*", together with what frequency bands have been used, as previously reported at the International Telecommunication Union.⁴⁸ Thus, the most critical points of friction between the information sharing obligations and trade secrets protection are embodied by the "*conduct*" and "*results*" components. Technical approach, timeline, identity, as well as operational safety and even payload information fall within the definition of "*conduct*." The "know-how" of how a space operation is carried out certainly can trigger trade secret protections by private operators. The same can be said about the "*results*" requirement, which encompasses, according to the expert analysis, the various outcomes of a mission, such as scientific findings or data, operational achievements, and even lessons learnt from the activity.⁴⁹ Based on what has just been described, it seems that there is not much room for trade secrets protection in space; however, the implied methodology for sharing information may "save" that essential IP. In fact, the whole transparency system is based on flexibility, allowing each State to: "*determine what information can reasonably be shared [...] while*

⁴³ United Nations Office for Outer Space Affairs, A/AC.105/C.2.2026/CRP.19; Franziska Knur, Scarlet O'Donnell, and Neha Dagley and others, *An Expert Analysis of Article XI of the Outer Space Treaty* (International Institute of Space Law, Vienna, 15 Apr 2026).

⁴⁴ n 10, Article XI OST.

⁴⁵ n 43, 4.

⁴⁶ Ibid.

⁴⁷ Ibid, 3.

⁴⁸ Ibid, 3-4.

⁴⁹ Ibid.

recognizing the challenges raised by sensitive and complexities of space operations. Interpreting the provision today requires considering developments such as commercial operators."⁵⁰ States, as the ultimate and direct subjects, have a large margin of flexibility regarding what information ought to be shared; many may consider this to undermine the purpose of Article XI OST, but practice has demonstrated it is not the case. In 2024, the United States reaffirmed, before the UN COPUOS Legal Sub-Committee, its commitment to Article XI OST, lending further weight to the ongoing work of international groups on the subject.⁵¹ The same venue witnessed a comparable development just two years later: in 2026, the European Union, speaking in its own voice, credited the United States for having undertaken the agreed coordinated approach (under the Artemis Accords)⁵² with respect to data sharing for a scientific payload aboard a commercial spacecraft project.⁵³ On that occasion, the EU has also further specified the categories of information (data access, technical training, and institutional development), as well as the scope of this cooperation, oriented toward addressing social challenges, climate change, food security, and emergency management.⁵⁴ Even the United Kingdom, no stranger to data sharing obligations, presented a comprehensive account of what kind of data (such as orbital parameters, general function, launch vehicle used, etc.) it reports at the international level - although the scenarios were limited to change in ownership of a satellite and change in orbital positioning.⁵⁵

An additional layer of complexity is introduced by the absence of a standardized reporting methodology,⁵⁶ a challenge that is further compounded when dealing with reports from private and commercial operators that States are obliged to collect (pursuant to the supervisory duty under Article VIII OST) and subsequently transmit internationally. In this latter context, it would be immediately advisable to standardize national reporting systems and to introduce a dedicated provision allowing private and commercial operators to withhold specific information by designating it as a trade secret. The outer limits of this practical solution, designed to prevent private actors from invoking trade secret protection as a means of circumventing international obligations or gaining undue competitive advantage, will be examined in Chapter 5.

Entrenching upon a restrictive and overly literal interpretation of the OST would risk frustrating its overarching purpose: the expansion of human knowledge and presence in outer space. It is therefore the author's view that the "expert analysis" approach is both sound and appropriate in all the respects described, equipping the international community with an indispensable interpretive tool for a norm that has long been the subject of debate.

⁵⁰ Ibid.

⁵¹ United States, Statement as Prepared for U.S. Representative Emily Pierce, Agenda Item 8, UN COPUOS Legal Sub-Committee (Vienna, 21 Jun 2024).

⁵² The Artemis Accords: Principles for Cooperation in the Civil Exploration and Use of the Moon, Mars, Comets, and Asteroids for Peaceful Purposes, (NASA, 13 Oct 2020), [Artemis-Accords-signed-13Oct2020.pdf](#).

⁵³ European Union, Statement at COPUOS Legal Sub-Committee 65th session on status and application of the five UN treaties on outer space (Vienna, 16 Apr 2026).

⁵⁴ Ibid.

⁵⁵ UNOOSA, A/AC.105/C.2.2024/CRP.21, 'Sharing approaches of the United Kingdom to Article XI implementation and notifications' (Vienna, 15 Apr 2024).

⁵⁶ UN COPUOS Scientific and Technical Subcommittee, 66th session, 'Dedicated Tools and Practices for Enhanced Information Sharing', DRAFT Non-Paper submitted by Luxembourg and Germany (Vienna, 2023).

4 How to Keep Secrets in Orbit. A Rethinking of “Reasonable Measures” in Outer Space.

According to a consolidated jurisprudence - international, regional, and national - to satisfy the "reasonable measures" requirement, at least on Earth, a trade secret owner has to adopt a series of expedients, such as:⁵⁷

- Physical steps
 - a) Building access controls
 - b) ID checks
 - c) Visitors logs
 - d) Labelling confidential information
- Technological protection
 - a) Dedicated VPN
 - b) Password protection and update
 - c) Encryption
 - d) Multifactor authentication
- Personnel
 - a) Pre-employment screening
 - b) Training
 - c) Instructions on policies and confidentiality
 - d) Non-Disclosure agreements, both for employees, suppliers, and visitors
 - e) Non-compete clauses

And many others, to be assessed on a case-by-case basis. At first sight, it appears possible to apply them to the space environment *sic et simpliciter*, without any specific variation. It is not the case; not for some of them, at least. As already stated *supra* (§2.1), it is not advisable to "store" sensitive information in an orbiting locker, both for safety reasons and cost concerns. A different solution must therefore be found. Moreover, encryption must be implemented in any case; however, the appropriate level of protection can only be determined based on the specific technology deployed in each scenario. Additionally, non-compete clauses for personnel are being challenged - not only in the space sector - by some of the most influential legal systems (such as the US), and they pose additional constraints on workers and employees who also have to navigate export control and national security limitations. As stated, the goal of this research is to advance the discussion on this emerging area of law, but also to provide actionable solutions: tools that can serve as guidance for practitioners, judges, arbitrators, regulatory officials, and academics. Currently, Low Earth Orbit (LEO) is the most suitable (and profitable) for a series of operations that would otherwise be impossible, or prohibitively expensive, making it the current oil of space activities. Earth observation, remote sensing, telecommunications, and even In-Space Assembly and Manufacturing (ISAM) and On-Orbit Servicing (OOS) all take place in outer space,⁵⁸ beyond the reach of any territorial sovereignty, per Article II of the Outer Space Treaty,⁵⁹ cornerstone of the *Corpus Iuris*

⁵⁷ Claudia Ray, Joseph Loy, Josh Berlowitz, and Andrew Lee, ‘USA. Law and Practice’ in Claudia Ray and Joseph A Loy, *Trade Secrets 2026* (Chambers Global Practice Guide 2026) 160.

⁵⁸ Referring, respectively, to the in-space manufacturing of new items, the repair of existing ones, and the provision of ancillary services such as refuelling.

⁵⁹ n 10.

Spatialis.⁶⁰ These orbits are today's Klondike, in which gold is substituted for orbital slots. Thus, the following paragraphs will discuss some of the scenarios already unfolding in LEO, that may trigger trade secret protection, before the chapter closes with a brief reflection on the current trends and developments in this area of law that would benefit most from international harmonization, namely employment rights and export control policies in the space sector.

4.1 Protecting Secrets During Satellite Communication.

A satellite “downlink” is a procedure that consists of a transmission of data from the satellite (the sender) back to a ground station (the receiver) on Earth.⁶¹ The reverse procedure is called an “uplink,” and communication between satellites is defined as a “crosslink” (or “inter-satellite link”).⁶² These kinds of transmission may be carried out using radio frequencies (RF), through various-sized antennas, installed on both the satellite and the ground station, or by means of optical transmission (also referred to as laser communications, lasercom, or Free Space Optical (FSO)),⁶³ whereby light signals are converted into electric signals (hence, information) by a receiver. As illustrated in Figure 1 below, the physical distinction between the two is stark, and for the present inquiry, it is the threshold question that determines not whether encryption is required, but how much of it is. RF systems broadcast information on electromagnetic waves through antennas, spreading broadly as they travel: more floodlight than torch.⁶⁴ This wide divergence means that a sufficiently equipped receiver, positioned anywhere within the beam's extensive footprint, may intercept the transmission without the knowledge of either party. The antenna in Camblanes-et-Meynac was, precisely, such a receiver. Given the structural exposure of RF transmissions to eavesdropping, state-of-the-art encryption is not merely advisable for operators transmitting commercially sensitive data via RF downlink;⁶⁵ it is, in the author's view, what the reasonable measures standard demands. NASA already requires that propulsive spacecraft within two million kilometres of Earth protect their command uplink with FIPS 140-3 Level 1-compliant encryption;⁶⁶ for trade secret purposes, that benchmark offers a sensible reference point for commercial operators as well, at least for highly sensitive commercial data. Critically, however, an operator transmitting under an amateur FCC licence cannot encrypt at all - a constraint that would make any trade secret claim over that data very difficult to sustain.⁶⁷

⁶⁰ Tanja Masson-Zwaan, Mahulena Hofmann, *Introduction to Space Law*, (4th edn, Kluwer Law International 2019) 6.

⁶¹ Bruce D. Yost, Brian C. Kempa, Craig D. Burkhard, *et al* , *State-of-the-Art of Small Spacecraft Technology*, NASA (18 May 2026) 224.

⁶² *Ibid*.

⁶³ *Ibid*, 245.

⁶⁴ *Ibid*, 249-250.

⁶⁵ *Ibid*.

⁶⁶ National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules* (Federal Information Processing Standard 140-3, NIST). ISO/IEC 19790:2012; ISO/IEC 24759:2014.

⁶⁷ 47 CFR § 97.113 (a)(4) [US].

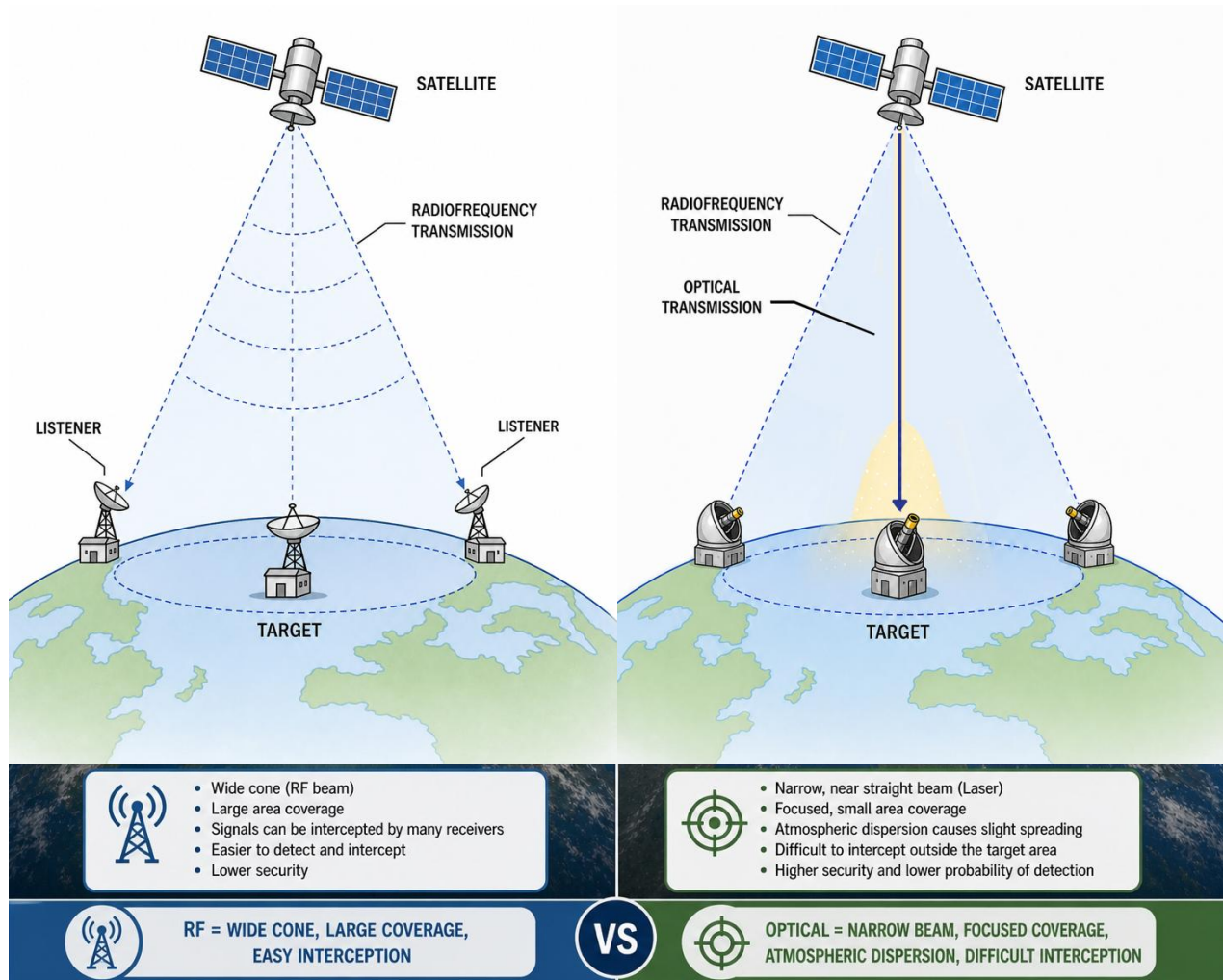


Figure 1: RF vs Optical space transmission. Note: in the image on the right, the optical transmission does not originate from an antenna © Marco Franzoso

Lasercom operates on an entirely different physical logic. As Figure 1 illustrates, the optical beam is narrow to the point of near-surgical precision: its divergence is much smaller than that of the RF beam.⁶⁸ A lasercom transmission does not flood surrounding space with recoverable data; it delivers it to a specific terminal and nowhere else. The probability of interception is structurally low, not as a matter of good fortune, but of physics.⁶⁹

This distinction has a direct consequence for the reasonable measures inquiry, which, as established above, is calibrated to costs and benefits rather than the absolute best precaution *per se*. Where the risk of interception is high (as with RF), the standard demands correspondingly robust encryption. Where that risk is structurally reduced by the transmission technology itself (as with lasercom), a proportionally lighter encryption standard may still satisfy the reasonableness threshold. The law does not require a bank vault, where a secure room will do.

⁶⁸ n 61, 268.

⁶⁹ *ibid.*

4.2 Protecting Secrets on Commercial Space Stations

As already noted (§2.1), commercial space stations are no longer a speculative hypothesis but a foreseeable operational setting of the next phase of the LEO economy.⁷⁰ Their very architecture, however, makes the terrestrial logic of secrecy difficult to transplant: there is no room for ordinary vaults, and no practical way to “lock away” every component, label, or supplier trace without introducing weight, safety, and cost concerns that would be disproportionate to the mission itself. In this setting, the status of private or commercial astronauts becomes crucial.⁷¹ They are not fully assimilated to state astronauts, yet they are not simple passengers either;⁷² existing ISS practice and NASA’s more recent private-astronaut framework already show that they may be subject, from the outset, to dedicated conduct rules, safety requirements, and mission-specific obligations, including those relating to crew behaviour, training, and compliance on board.⁷³

Against that background, one possible response would be to reconfigure the commercial astronaut, at least for the duration of the mission, as a *visitor* rather than as a mere customer, and to make station access conditional upon the execution of NDAs, confidentiality undertakings, and access agreements. Given the general trend toward extending national jurisdiction to the extraterritorial misappropriation of trade secrets wherever a demonstrable link to a specific national jurisdiction can be shown, and given the quasi-territorial jurisdiction that Article VIII OST confers over registered space objects, the eventual enforceability of these covenants is not, in fact, the intractable problem it might first appear: the space station itself supplies the jurisdictional anchor while the visitor is aboard, and the extraterritorial reach of national trade secret regimes supplies it once they return to Earth.⁷⁴ That solution would not eliminate the practical exposure of trade-secret material - supplier lists, component labels, internal layouts, and other commercially sensitive details may still be visible to anyone on board - but it would at least provide a contractual basis for disclosure control where physical segregation is not realistically attainable. Even then, however, confidentiality cannot operate in a vacuum. The same visitor would still have to comply with the mandatory safety, security, and operational rules applicable to the station and its crew, and those rules may in turn require disclosure, training, or access to information that cannot be withheld without jeopardizing mission integrity.

4.3 Balancing Trade Secret Protection and Employers’ Rights in the Space Sector

Non-compete agreements between employer and employee are a standard instrument of trade secret protection across virtually all the jurisdictions surveyed, though their scope, enforceability, and conditions vary considerably.⁷⁵ In the European Union, post-contractual non-compete clauses are

⁷⁰ n 42.

⁷¹ Marco Franzoso, “‘Fly Me to the Moon... & Back’: the Intricate Interplay Between Copyright and Space Law” (2025) XXXV Fordham IP, Media, and Entertainment L. J. 4, 985, 987.

⁷² Bin Cheng, *Studies in International Space Law* (Oxford University Press 1997), 416-417.

⁷³ Code of Conduct for the International Space Station Crew, 14 CFR § 1214.403 (1992); Artemis Accords, n 52.

⁷⁴ 18 U.S.C. § 1837 [US]. Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) OJ L 351, 20.12.2012, p. 1-32; CJEU C-832/21, *Beverage City & Lifestyle GmbH e.a. v Advance Magazine Publishers Inc*, ECLI: ECLI:EU:C:2023:635, 7 Sep 2023 [EU]. Claudia Ray, Joseph Loy and Josh Berlowitz, *Trade Secrets 2026* (Chambers Global Practice Guide 2026) 13, 39, 73, 92, 112, 135, 158.

⁷⁵ *Liberty Financial Pty v Jugovic* (2021), FCA 607 [Australia].

permissible but tightly circumscribed: they must be limited both territorially and temporally, and - critically - they must be compensated. In France and Italy, the obligation to pay the employee for the duration of the restriction is not a matter of good practice but of legal requirement;⁷⁶ an uncompensated clause is simply void. In India, the position is considerably more restrictive: Section 27 of the Indian Contract Act 1872 renders agreements in restraint of trade void as a general rule, and courts have consistently declined to enforce post-employment non-competes, leaving only intra-contractual restrictions on solid ground.⁷⁷ In China, the Labour Contract Law provides a more structured framework: non-competes are enforceable for up to two years, but only against senior management and technical personnel, and only where monthly compensation is paid throughout the restriction period.⁷⁸

In the United States, the picture is one of deliberate fragmentation. The Federal Trade Commission's attempt to impose a near-total federal ban on non-compete agreements (in April 2024) was struck down by federal courts before it could take effect, leaving the field to a patchwork of state regimes.⁷⁹ Minnesota,⁸⁰ California and,⁸¹ to a significant extent, Delaware sit at one end of the spectrum,⁸² with non-competes largely unenforceable as a matter of public policy; Texas and Florida sit at the other,⁸³ where such clauses are routinely upheld provided they are reasonable in scope and duration. The result is a system that provides no consistent national answer and, for a sector as geographically diffuse as the space industry, no reliable legal infrastructure. That inconsistency alone would be a sufficient reason for caution. But there is an additional layer of complexity that is specific to the space sector and largely absent from any other industry: employees working in space-related activities are already subject to some of the most stringent restrictions on occupational mobility that any legal system imposes. Export control regimes - and in particular the US International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations⁸⁴ - require that personnel with access to controlled space technologies either hold US person status or obtain specific government authorization.⁸⁵ In practice, ITAR functions as a structural filter on who may work in this sector at all, regardless of any contractual arrangement. Nor is this phenomenon uniquely American. Several other jurisdictions with significant space industries have adopted equivalent deemed-export doctrines that produce direct hiring restrictions: giving a foreign national access to controlled space technology on domestic soil is treated as an export to that person's country of nationality, requiring a licence or being outright prohibited. In Australia, the Defence Trade Controls Amendment Act 2024 expressly criminalises the supply of technology listed on the Defence and Strategic Goods List (DSGL) to a "non-exempt foreign person" within Australia,⁸⁶ a provision deliberately modelled on

⁷⁶ Codice Civile, Articles 2125, 2596 [Italy]; Cass soc, July 10, 2002, No 00-45.135 [France].

⁷⁷ *Krishan Murugai v Superintendence Co*, AIR 1979 Delhi 232.

⁷⁸ Fani Li and Tingli Huan, 'Recap: Navigating China's Evolving Non-Compete Landscape' (*Freshfields* 23 Mar 2026), <https://www.freshfields.com/en/our-thinking/blogs/risk-and-compliance/recap-navigating-chinas-evolving-non-compete-landscape-102mnkz>.

⁷⁹ Dawn Martineit, Michael Wexler, Marcus Mintz, 'USA. Trends and Developments' in Claudia Ray and Joseph A Loy (eds), *Trade Secrets 2026* (Chambers Global Practice Guide 2026) 173.

⁸⁰ Minnesota Statutes § 181.988.

⁸¹ California Business and Professions Code § 16600.1; *Edwards v Arthur Andersen LLP* (2008) 44 Cal 4th 937.

⁸² *Hub Group Inc v Knoll*, 2024 WL 3453863 (Del Ch, 18 Jul 2024); *Kodiak and Sunder Energy LLC v Jackson and others*, 305 A 3d 723, 746 (Del Ch 2023).

⁸³ Texas Business and Commerce Code § 15.50; *Galderma Laboratories LP v Brenner* (Tex 8th 2026); *Alex Sheshunoff Management Services LP v Johnson and Strunk & Associates LP*, 209 SW 3d 644 (Tex 2006). Florida Contracts Honoring Opportunity, Investment, Confidentiality, and Economic Growth (CHOICE) Act (24 Apr 2025).

⁸⁴ 22 CFR § 120-130 (ITAR); 15 CFR § 730-774 (EAR).

⁸⁵ 22 CFR § 120.14 – 120.62.

⁸⁶ Defence Trade Controls Amendment Act 2024 (Cth) s 10A [Australia].

ITAR's deemed-export logic and enacted as a precondition for Australia's admission to the AUKUS ITAR exemption framework. In Japan, a 2021 clarification issued by the Ministry of Economy, Trade and Industry (METI) under Article 25 of the Foreign Exchange and Foreign Trade Act (FEFTA)⁸⁷ explicitly requires employers to screen foreign national employees and verify whether they fall within "Specific Categories" before granting access to controlled technology on Japanese soil,⁸⁸ producing an employment filter that is functionally indistinguishable from the US model. Superimposing a non-compete obligation on top of this pre-existing web of restrictions risks compounding an already constrained labour market to a degree that, in several jurisdictions, may engage constitutionally protected rights to freedom of employment and occupational choice. The space industry employee is not a typical worker: before any contractual restriction is even considered, their nationality, residency status, and security clearance have already determined the outer limits of where they may work and what they may touch. A non-compete clause, in this context, does not add a layer of protection; instead, it adds a layer of constraint onto a person who is, by operation of law, already among the most constrained workers in any modern economy.

It is therefore the author's view that, in the specific context of the space sector, non-compete clauses should be treated with considerable scepticism as a component of the reasonable measures inquiry. A measure that is legally contested, jurisdiction-dependent, financially burdensome, and potentially disproportionate when layered onto existing export control obligations is a fragile foundation for trade secret protection; and fragile foundations, as the case law has consistently reminded us, do not satisfy the standard of reasonableness.

5 Outer Space and Outer Limits: The Boundaries of Trade Secrets Protection in Orbit.

Now that the meaning of "reasonable measures" in outer space has been established, the focus must shift to the outer limits of this category of intellectual property; limits that apply not only on Earth, but in space as well. The essential caveat is to strike a balance between trade secret protection and the information-sharing obligation discussed in §3, and in particular, how private and commercial space operators can navigate that duty without infringing current space law. It was already advised (§3.1) to introduce standardized national reporting systems and to permit the withholding of specific information by designating it as a trade secret. The risk embedded in that system, however, is that private operators would use it as a shield, labelling everything a "trade secret" to circumvent their disclosure obligations entirely, thereby hampering the collective human endeavour in outer space. It is therefore essential to identify the outer limits: the scenarios in which commercially valuable information cannot seek trade secret protection because a different, and more fundamental, value is at stake. Three such limits emerge from current law (two rooted in EU frameworks, one in US constitutional litigation), and all three converge on the same structural point: trade secret protection is not an absolute right capable of functioning as a blanket refusal to disclose. It is, at most, a conditional shield, one that yields when fundamental rights, regulatory transparency obligations, or constitutional limits step into the frame.

⁸⁷ Foreign Exchange and Foreign Trade Act (外国為替及び外国貿易法), Act No. 228 of 1949, as amended, Art. 25.

⁸⁸ Ministry of Economy, Trade and Industry (METI), 'Clarification on Transactions or Acts of Transferring Technology Requiring Permission pursuant to Article 25(1) of the Foreign Exchange and Foreign Trade Act' (November 2021).

5.1 The First Outer Limit: GDPR and the Right to Intelligible Explanation

The first limit is drawn on privacy protection regulation, as interpreted by the Court of Justice of the European Union (CJEU) in its judgment *CK v Magistrat der Stadt Wien*.⁸⁹ The case arose from the refusal of a credit-scoring company - relying on automated algorithmic systems - to disclose meaningful information about the logic of its creditworthiness assessment, invoking Directive 2016/943. The CJEU was unequivocal: the existence of trade secrets cannot ground a blanket refusal to provide the information required under Article 15(1)(h) of the General Data Protection Regulation (GDPR).⁹⁰ Where a controller invokes trade secrecy, the allegedly protected information must be disclosed to the competent supervisory authority or court, which then balances the competing rights and determines the extent of the data subject's access.⁹¹ Confidentiality is preserved procedurally, not by denying the right altogether. The Court further specified that the informative duties under Article 15(1)(h) cannot be satisfied by the mere communication of a complex mathematical formula or algorithm, none of which constitutes an information "*sufficiently transparent and intelligible to inform the data subject*."⁹² The explanation must describe the procedure and principles actually applied in such a way that the data subject can understand which of their personal data were used, and how, in the automated decision at issue. Algorithmic complexity, the Court held, does not relieve the controller of this obligation.⁹³ Therefore, when private operators licensed in an EU Member State comply with the duty of information sharing and complete the requested form, they must take into account a specific constraint: in disclosing the "*results*" or the "*conduct*" of their operations (§3.1), they cannot withhold information whose disclosure would nonetheless be prohibited by the protection owed to personal data, as understood under Regulation (EU) 2016/679.⁹⁴ Such information may include geographic locations, movements, banking data, timestamps, and the like. The flexibility otherwise granted by the disclosure duty thus meets an insurmountable limit in the protection of sensitive personal data.

Ad abundantiam, for space operators using space-based raw data or AI systems that process the personal data of identifiable individuals (and the scenarios are already real, from satellite-based movement profiling to space-derived agricultural assessments),⁹⁵ Article 15(1)(h) GDPR and *CK v Magistrat der Stadt Wien* apply in full. The trade secret shield does not defeat the disclosure obligation; it merely channels it through a procedural mechanism that a court or supervisory

⁸⁹ *CK v Magistrat der Stadt Wien*, n 32.

⁹⁰ 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), OJ L 119, 4.5.2016, p. 1-88, art. 15(1)(h).

⁹¹ n 32 [72-78].

⁹² Ibid [62].

⁹³ Ibid [56-59].

⁹⁴ n 90, article 1.

⁹⁵ European Space Agency, 'Space-based radar reveals the hidden movements of the Bernabéu stadium' (*ESA-Earth*, 6 May 2026), <https://earth.esa.int/eogateway/success-story/space-based-radar-reveals-the-hidden-movements-of-the-bernabeu-stadium>; Francesca Spagnoli, Noemi Caiazza and Alex ChUNET and others, How Can Data From Space Shape the Future of Agriculture? (*World Bank Blog*, 1 Dec 2025), <https://blogs.worldbank.org/en/opendata/how-can-data-from-space-shape-the-future-of-agriculture->.

authority controls. Whatever is eventually disclosed must be genuinely intelligible: not a formula, but an explanation a natural person can understand and, if necessary, contest.

5.2 The Second Outer Limit: The EU AI Act and Training Data Transparency

The second limit is drawn by the EU AI Act.⁹⁶ Article 53(1)(d) requires General Purpose AI (GPAI) providers to publish a sufficiently detailed summary of the content used to train their models, according to a mandatory template issued by the AI Office.⁹⁷ A GPAI is defined by Article 3(63) of the EU AI Act as a model that: “[...] *displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market.*”⁹⁸ In this framework, trade secrets are acknowledged, per 53(1)(b), which expressly states that disclosure shall be made without prejudice to the need to protect intellectual property rights and confidential business information; however, they are not exempted from the obligation. The Regulation shapes how the disclosure is structured, without extinguishing the obligation. Transparency is the rule, where confidentiality is the exception.⁹⁹

For a space operator whose AI is trained on proprietary satellite imagery, orbital observation data, or geolocation patterns, this provision bites with particular force. They - most likely - fell into the “high-risk” category, given the dual nature of outer space, and therefore they “*must meet the specific requirements set out for high-risk AI systems, including transparency, robustness, and human oversight provisions.*”¹⁰⁰ Unlike a general AI company whose training data consists largely of internet-scraped content, the space operator's training data and core commercial asset are frequently the same thing: the proprietary orbital observation dataset that it sells and licences is also the dataset on which its AI is trained. A sufficiently detailed summary of that training data is, in substance, a description of the commercial asset itself, and the AI Act requires it. Thus, for these specific operators, being asked to disclose their “conduct” is, in effect, being asked to disclose their own most valuable asset. A reasonable balance ought to be found here, since the exact contours of this particular outer limit have yet to be drawn.

5.3 The Third Outer Limit: AB 2013 and the Failure of the First Amendment Shield

The third limit emerges from US constitutional litigation. California's Artificial Intelligence Training Data Transparency Act (AB 2013), which entered into force on 1 January 2026, requires generative AI developers to post a high-level summary of their training datasets.¹⁰¹ X.AI LLC, a

⁹⁶ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act), OJ L, 12.7.2024, Art. 53(1)(d).

⁹⁷ Ibid.

⁹⁸ Ibid., Art. 3(63).

⁹⁹ Giulia Maienza, Pietro Pouché, ‘Trade Secrets in the AI Era: Navigating Transparency under the EU AI Act’ (*Herbert Smith Freehills Kramer*, Nov 2025), <https://www.hsfkramer.com/insights/2025-10/trade-secrets-in-the-ai-ere-navigating-transparency-under-the-eu-ai-act>.

¹⁰⁰ Leila Debiasi, ‘Understanding General Purpose AI’ (*European Institute of Public Administration*, 11 Mar 2025), <https://www.eipa.eu/blog/understanding-general-purpose-ai/>.

¹⁰¹ Artificial Intelligence Training Data Transparency Act 2024 (AB 2013), Cal Civ Code § 3111.

company behind one of the main AI models, sought to enjoin enforcement, raising a First Amendment compelled speech claim alongside a trade secrets defence.¹⁰² In its order of 4 March 2026, the Central District of California denied the preliminary injunction, applying intermediate scrutiny under *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*.¹⁰³ AB 2013 requires disclosure of factual commercial information, not ideological statements, and directly advances a substantial government interest in consumer information. X.AI demonstrated a "distinct possibility" of success on the merits but not the "likelihood" required for emergency relief, leaving the law in effect while the constitutional challenge proceeds.¹⁰⁴

The implications for space operators accessible to California markets, which encompass virtually every significant commercial operator, are direct. The First Amendment shield, as it stands, does not block training data transparency obligations. The *Central Hudson* analysis would, moreover, be no more favourable to a space operator whose AI is consumer-facing, precisely because the government's interest in informing consumers is strongest where ordinary persons interact with the system directly. What has been argued at the end of the previous paragraph (§5.2) applies here as well, albeit under a different rationale (privacy protection for the EU, freedom of speech in the USA).

5.4 Privacy-by-Design as a Structural Response

The three outer limits described converge on a common prescription: if trade secret protection cannot defeat GDPR intelligibility obligations, cannot block training data transparency under the EU AI Act, and cannot rely on the First Amendment to void comparable US requirements, then the rational design response is not to resist disclosure but to architect systems that can satisfy it without exposing the proprietary core. GDPR Article 25 already mandates data protection by design and by default,¹⁰⁵ *CK v Magistrat der Stadt Wien* gives that principle a specific operational meaning in the AI context. For space operators, simultaneously facing EU GDPR obligations, EU AI Act requirements, AB 2013 compliance demands, and ITAR/EAR export control constraints, privacy-by-design is not merely a compliance strategy.¹⁰⁶ It is the architecture that best navigates all three outer limits at once: a system designed from the outset to be explainable at the required level of intelligibility, without being technically revealing, satisfies each limit without surrendering the commercial asset that the trade secret framework was designed to protect in the first place.

6 Conclusion

The present research has moved through genuinely uncharted territory. At current knowledge, no sustained doctrinal work has been done on this specific intersection of the law with outer space. The coordinates offered here are therefore necessarily preliminary, but they are also precisely what allow subsequent expeditions to set out with confidence rather than speculation.

¹⁰² *X.AI LLC v Rob Bonta*, No 2:25-cv-12295 (CD Cal, 4 Mar 2026).

¹⁰³ *Central Hudson Gas & Electric Corp v Public Service Commission of New York*, 447 US 557, 561-62 (1980).

¹⁰⁴ *X.AI LLC v Rob Bonta*, n 100, 11.

¹⁰⁵ n 90, Article 25.

¹⁰⁶ Marco Franzoso, *The "Third Way" to Space Power: Europe's Digital Sovereignty Advantage* (Stanford Space L & Pol Perspectives, Jan 2026) 3.

The argument has unfolded in three stages, where the first established the doctrinal foundations: the framework behind trade secrets protection, their commercial value, and the reasonable steps to protect them, interpreted across a selection of legal systems currently most relevant to space activities. The second identified the structural tension between this branch of the law and the international obligation of information sharing under Article XI OST - a tension that the flexibility built into the transparency regime partially alleviates, but does not dissolve. The third and central contribution was the rethinking of what "*reasonable measures*" actually demands in the space environment, and the identification of its outer limits. Regarding the latter, the analysis has yielded three concrete conclusions. For satellite communications, the choice of transmission technology is not an engineering decision but a constitutive element of the reasonable measures inquiry: state-of-the-art encryption is what the reasonable measures standard demands for RF communication, where the beam spreads broadly and any sufficiently equipped receiver may intercept it; a proportionally lighter standard may satisfy the reasonableness threshold for lasercom (optic), where the probability of interception is structurally low, as a matter of physics. For commercial space stations, physical segregation of sensitive material is largely impractical, and the most workable solution lies in reconfiguring visitors (commercial astronauts) as conditional entrants, bound by NDAs and access agreements executed prior to boarding. For employees of the space sector, non-compete clauses should be treated with considerable scepticism: a measure that is legally contested, jurisdiction-dependent, financially burdensome, and layered on top of export control regimes already functioning as structural filters on occupational mobility is not a reasonable protective measure but an unreasonable burden.

On the question regarding where the outer limits lie, again, three convergent boundaries emerge from current law. The GDPR, as interpreted by the CJEU, establishes that trade secrecy cannot function as a blanket refusal to explain the logic of automated decisions affecting individuals: confidentiality is preserved procedurally, not by denying the right altogether. This limit reaches beyond the AI context: even outside automated decision-making, the disclosure duty under Article XI OST meets an ally in the protection owed to personal data, meaning that a space operator cannot invoke trade secrecy to withhold information that GDPR independently prohibits disclosing in the first place. Moreover, the EU framework requires GPAI companies to publish meaningful summaries of the data they use to make automatic decisions; a disclosure obligation that trade secrets may shape, but cannot defeat. In the USA, the First Amendment does not provide a constitutional shield against factual commercial disclosure requirements under intermediate scrutiny, reaching the same result as the EU AI Act under a different rationale: privacy protection on one side of the Atlantic, freedom of speech on the other. For space operators implementing AI systems and whose training data and core commercial assets are frequently the same thing, all three limits hit particularly hard. The structural response, it has been argued, is privacy-by-design, a system architected from the outset to be explainable at the required level of intelligibility, without being technically revealing.

Additionally, several national and regional trends and developments would be of great benefit for trade secrets protection if internationally harmonized. Confidentiality rings - procedural mechanisms allowing commercially sensitive information to be disclosed to courts and regulators without entering the public domain - are already established in the EU, India, China,¹⁰⁷ and represent the most immediately transposable tool, also for the space context. Specialized IP courts or chambers with space-sector expertise, an emerging feature of several national systems,¹⁰⁸ would provide the

¹⁰⁷ Claudia Ray, Joseph Loy and Josh Berlowitz, *Trade Secrets 2026* (Chambers Global Practice Guide 2026) 42, 75, 97.

¹⁰⁸ Ibid, 104, 116, 149, 233.

technical literacy that general commercial courts currently lack when assessing the reasonableness of a space-specific measure. The shift of the burden of proof in trade secret litigation (a distinctive feature of the Chinese system under the amended Anti-Unfair Competition Law, and increasingly relevant)¹⁰⁹ is a development that international harmonization efforts can neither ignore nor defer. In conclusion, trade secret protection in outer space must be interpreted through a *holistic* prism, taking into consideration not just the ultimate end - the protection of commercially valuable information - but also the environment where the necessary protective steps must unfold. Only under this approach, an equitable system can be created.

This paper has given coordinates and a map. What it has not built is the destination, and it has done so deliberately. The space economy is moving faster than any single piece of scholarship can follow, and the honest contribution of a preliminary study is precisely to establish the doctrinal perimeter within which more targeted research can subsequently operate. If it has succeeded in demonstrating that the problem is real, the existing frameworks are insufficient, and actionable solutions are available, it will have served its purpose.

In the meantime, the antenna in Camblanes-et-Meynac has been dismantled. A measure, decidedly, reasonable.

Funding disclosure

This research has received funding from the European Union's Horizon Europe research and innovation programme under the Marie Skłodowska-Curie Actions Doctoral Network SPARE - Resiliency, Sustainability, and Competitiveness in Future Satellite Systems, Grant Agreement No. 101227584. The views and opinions expressed are those of the author only and do not necessarily reflect those of the European Union or the granting authority; neither the European Union nor the granting authority can be held responsible for them.

AI-assistance disclosure

During the preparation of this work, the author used Claude Sonnet 4.6 (Anthropic) for research assistance and citation formatting. The author reviewed and edited the content as needed and takes full responsibility for the content of the published article.

¹⁰⁹ Supreme People's Court ZhiMinZhong No1669 [China].