

India-EU Free Trade Agreement: Implications of Source Code Rules

Amitendu Palit and Atyantika Kothuri Mookherjee

Summary

Provisions restricting government access to software source code have become a standard feature of digital trade agreements. Because artificial intelligence (AI) systems are software, these provisions now sit at the boundary between trade law and AI governance. This working paper examines draft source code rules in the India-European Union (EU) Free Trade Agreement (FTA) from a comparative perspective for understanding their potential implications on Indian digital exports. While the source code rules are largely identical in the FTA with those in the EU's other major recent Asian FTAs, like those with Korea and Indonesia, the perceived disadvantages for Indian exporters arise from a lack of domestic regulations for AI. The absence of these regulations subjects Indian source codes to the possibility of pre-market reviews in the EU, while no such provisions exist for checking EU source codes in India, except for sensitive sectors like critical infrastructure.

This working paper, however, argues that this imbalance does not constitute the ground for revisiting the source code rules for making them more specific to safeguard against the downsides of high-risk AI systems. On the contrary, it argues for India speeding up the growth of sectoral regulations impacting the use of externally developed frontier AI systems in the country and working closely with the EU in this regard.

Introduction

India and the European Union (EU) concluded negotiations on a bilateral free trade agreement (FTA) on 27 January 2026, with the provisional text of the FTA becoming available soon after. Both sides aim to sign the FTA following the finalisation of the legal text by the end of 2026 and operationalise it by early 2027.¹ The FTA has been widely proclaimed as the 'mother of all deals' for creating one of the world's largest common markets; and the faith of two of the world's largest economic actors – with historically divergent views on trade – in a comprehensive rules-based framework for advancing mutual trade.²

The FTA includes digital trade rules agreed upon by India and the EU. Among India's new-generation FTAs signed in the current decade, the EU FTA will join those signed by India with the United Arab Emirates (UAE) and the United Kingdom (UK) as agreements containing

¹ Piyush Goyal, "India-EU trade pact to be signed by end of this year", *Business Standard*, 16 July 2026, https://www.business-standard.com/economy/news/india-eu-trade-pact-to-be-signed-by-end-of-this-year-piyush-goyal-126071601216_1.html.

² Amitendu Palit, "India-EU's 'mother of all deals' is much more than just a trade pact", *Channel NewsAsia*, 29 January 2026, <https://www.channelnewsasia.com/commentary/india-european-union-trade-deal-significance-5888286>.

digital trade rules. Salience of these rules in India's FTAs is significant, given the global growth in digital trade and its growing prominence in India's external trade.

A critical enabler of bilateral digital trade is the rules regarding disclosure of source code. These provisions in the draft India-EU FTA have generated interest in their potential impact on digital trade. The impact extends to cross-border usage of artificial intelligence (AI) in bilateral trade between India and the EU, along with their capacities to regulate such use.³ Given the rapid adoption of AI by Indian enterprises in cross-border digital service deliveries, India's ability to frame effective domestic regulations for AI, and their alignment with similar regulations in major global markets such as the EU, have significant implications for its long-term digital trade prospects.

This paper explores the wider implications of source code rules in the India-EU FTA through a comparative lens. These implications are significant for an economy like India, as it figures among those economies where externally developed AI systems operate at scale across various regulated sectors, with domestic firms often lacking ownership of proprietary software. The comparative lens employed in the paper entails studying a few more major trade agreements with source code provisions. Apart from the India-EU FTA, these include the India-UK Comprehensive Economic and Trade Agreement (CETA), signed in July 2025, which, till now, is India's only other FTA with source-code commitment. Two other major EU trade agreements are also studied. These are the EU-Korea Digital Trade Agreement (DTA)⁴ signed on 10 June 2026, and the EU-Indonesia Comprehensive Economic Partnership Agreement (CEPA), signed and concluded in September 2025.⁵ The paper also studies the source code rules in the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP), which set the precedent for 21st-century digital trade rules.⁶

The paper is divided into five sections. Section 1 examines source code rules in the draft EU-India FTA text and the need for domestic regulatory catch-up for India. Section 2 studies similar rules across the five mentioned trade agreements. Section 3 discusses India's disadvantages arising from lesser protection for software exports. Section 4 discusses asymmetry between the EU's domestic laws and FTA provisions. Section 5 summarises and concludes.

³ Shweta Kushe, "How India's New Free Trade Agreement with the EU Limits AI Governance", *Tech Policy Press*, 30 April 2026, <https://www.techpolicy.press/how-indias-new-free-trade-agreement-with-the-eu-limits-ai-governance/>.

⁴ European External Action Service, "EU And Republic of Korea Sign Landmark Digital Trade Agreement at Summit", *EEAS*, https://www.eeas.europa.eu/delegations/south-korea/eu-and-republic-korea-sign-landmark-digital-trade-agreement-summit_en?s=179.

⁵ EU-Indonesia Comprehensive Economic Partnership Agreement, Chapter 10 (Digital Trade), Article 10.13 (Transfer of or Access to Source Code) and footnote 10. The provisional text was published following the Ministerial Announcement of 23 September 2025 and is available via the European Commission, https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/indonesia/eu-indonesia-agreements/text-agreements_en.

⁶ Comprehensive and Progressive Agreement for Trans-Pacific Partnership, signed 8 March 2018, incorporating by reference the Trans-Pacific Partnership text, Article 14.17 (Source Code); official documents via the Australian Department of Foreign Affairs and Trade, <https://www.dfat.gov.au/trade/agreements/in-force/cptpp/official-documents/Pages/official-documents>.

Section 1: Source Code Rules in EU-India FTA

Source code rules in FTAs commit signatory states to not demand transfer of, or access to, the source codes of other members' software products as a condition of market entry. Source code is among the most valuable assets of firms providing software services. It's compelled disclosure, whether demanded directly or extracted through certification and testing requirements, amounts to forced technology transfer, and surrender of proprietary knowledge of the source code owning firm. These rules began featuring in global trade agreements after their formalisation by the CPTPP, with the EU gradually adopting these rules in its own FTAs.⁷

Disclosure conditions for source codes have implications for firms using AI applications in cross-border delivery of services. AI systems are considered software. Trade rules drafted in the past for pre-AI packaged software programmes now apply to algorithms that price credit, screen job applications, and manage power grids. Countries agreeing to source-code provisions in FTAs accept these as conditions governing their AI-embedded cross-border digital trade with other members of the FTAs.

Source code rules are critically important for India, given the importance of the EU as a market for its technology exports. According to the National Association of Software and Service Companies, India's information technology (IT) exports were at around US\$250 billion (S\$319 billion) in FY2026.⁸ Europe, including the UK, was the second largest global market for Indian software exports, after the US, accounting for 33 per cent of these exports.⁹ Indian IT service exporters, especially software exporters, would be eyeing enhanced export prospects following the FTA with the EU. Source code rules will be key determinants of these prospects. EU technology businesses are also looking closely at these rules, given that European software and AI systems are expected to extend deeper in various sectors of the Indian economy.

Article 9.9 of the EU-India FTA sets out the source code rules. It prohibits "the transfer of, or access to, the source code of software owned by a natural or legal person of the other Party as a condition for the import, export, distribution, sale or use of such software, or of products containing such software, in or from its territory".¹⁰ The rule will enable software exporters from India and the EU to access each other's markets without disclosing the proprietary source codes. However, regulatory, law-enforcement, judicial and conformity-assessment bodies might ask for disclosure of codes. Courts, administrative tribunals and competition authorities might also demand access to codes ostensibly for addressing violations in competition laws and other domestic laws. Such access might be asked for operations in critical infrastructure sectors also.

⁷ CPTPP, op. cit. The European Union's earlier agreements with Japan and the United Kingdom also contain source-code provisions.

⁸ India Brand Equity Foundation, "Information Technology", <https://www.ibef.org/industry/information-technology-india>.

⁹ Ibid.

¹⁰ Chapter 9, Article 9.9. EU-India: Text of the Agreements, https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/india/eu-india-agreements/text-agreements_en.

Do these rules impact prospects of digital trade using AI applications? Rules prohibiting transfer of, or access to, source code are broad and sweeping without specifically identifying AI features like algorithms. Indeed, rules addressing cross-border algorithmic interoperability are yet to feature in most global FTAs. By accepting non-disclosure of source codes, neither India nor the EU can insist on pre-market testing of AI algorithms. Given that risks associated with products and services comprising AI algorithms can only be judged post-facto, it might be considered rather short-sighted, especially for India, since Indian-origin algorithms will have to undergo prior testing in the EU market following the EU's domestic AI regulations.¹¹ The imbalance in this regard arises from India not having any domestic regulations like the EU mandating prior scrutiny of AI algorithms.

However, notwithstanding the absence of specific rules on algorithmic audit authority, the India-EU FTA text does emphasise ensuring safe and trustworthy use of AI as a legitimate objective justifying exceptions for access to source codes.

Whether absence of domestic regulations in India for checking foreign AI algorithms prior to their market entry, vis-à-vis those that may require Indian algorithms to be checked in the EU, amount to a comparative disadvantage for India's digital exports to EU, will depend on the sincerity of both India and EU in ensuring safe and trustworthy use of AI by employing appropriate contextual exceptions in the FTA, for source code disclosure. Moving forward, however, the FTA's rules must be complemented and aligned with respective domestic regulations. The EU has been far ahead of India in this regard, leaving the latter to work on regulatory 'catch-up'. Domestic regulations mostly develop independently of FTAs. To that extent, how those of the EU, and the upcoming ones for India, might influence the working of the FTA on AI governance, is very much a hypothetical issue at this stage.

Section 2: Comparable Source Code Rules in other FTAs

Source code rules of the five major FTAs are summarised in Table 1 for comparison. These include three of the EU's recent agreements: the India-EU FTA,¹² the EU-Korea DTA¹³ and the EU-Indonesia CEPA.¹⁴ Comparable rules are also noted for the India-UK CETA¹⁵ and the CPTPP.¹⁶

¹¹ Shweta Kushe, "How India's New Free Trade Agreement with the EU Limits AI Governance", *Tech Policy Press*, 30 April 2026, <https://www.techpolicy.press/how-indias-new-free-trade-agreement-with-the-eu-limits-ai-governance/>.

¹² India-EU FTA, Chapter 9, Article 9.9, op. cit.

¹³ Agreement on Digital Trade between the European Union and the Republic of Korea, Article 11 (Source Code) and Article 5(3), footnote 1; Council of the European Union document ST 13085/25, Brussels, 17 November 2025, <https://data.consilium.europa.eu/doc/document/ST-13085-2025-INIT/en/pdf>.

¹⁴ EU-Indonesia CEPA, Chapter 10, Article 10.13, op. cit.

¹⁵ India-UK CETA, Chapter 12, Article 12.15, op. cit.

¹⁶ CPTPP, Article 14.17, op. cit.

Table 1: Key FTAs and Source-code Rules

Provision	EU FTAs with India, Korea, Indonesia	India-UK FTA and CPTPP
1. Prohibition on requiring transfer of or access to source code	Present in all three with nearly identical wording: each prohibits transfer of or access to source code as a condition of import, export, distribution, sale or use.	India-UK FTA focuses on broader prohibition, not conditioned on market access. CPTPP's rules are limited to mass-market software.
2. Regulatory access for investigation, enforcement and judicial proceedings	All three allow access for investigation, inspection, examination, enforcement action or judicial proceeding purposes, subject to safeguards. The EU-Korea and EU-Indonesia FTAs mention before/ after market entry.	India-UK FTA preserves access without a public-policy-objective qualifier. CPTPP has no equivalent purpose-based access clause.
3. AI as a legitimate public policy objective	Yes, in all three. Footnotes list "safe and trustworthy artificial intelligence" among legitimate public policy objectives justifying access.	India-UK FTA: no reference to AI; preserves requirements for promoting algorithmic accountability tied to proceedings. CPTPP doesn't have such provisions
4. Competition-law access to source code	All three permit proportional and targeted access to address barriers to entry in digital markets.	Neither India-UK FTA nor CPTPP includes a competition law access provision.
5. Critical-infrastructure provision	Only in India-EU FTA.	CPTPP excludes critical-infrastructure software from the prohibition's scope entirely.
6. Scope limitations and exclusions	All three exclude voluntary commercial transfers and preserve requirements to modify code for legal compliance. EU-Indonesia FTA also excludes public procurement.	India-UK FTA excludes from "source code" the expression of an algorithm leaving documentation unprotected. CPTPP prohibition is limited to mass-market software.

Source: Compiled by the authors from the primary treaty texts cited in the footnotes earlier.

Provisions hardly vary between the India-EU, EU-Korea and EU-Indonesia FTAs. Access is conditioned upon specific purposes (such as investigation, judicial) (Table 1), with the India-EU FTA adding access for critical infrastructure (Table 1). The treatment of AI, too, is similar in being a legitimate public policy objective and is part of a broader list of similar objectives

in all three FTAs.¹⁷ Across all three FTAs, the template for source code rules remains the same and is applied with minor adjustments.

Both the EU-Korea and the EU-Indonesia texts allow regulatory access to source code before or after market entry (Table 1), while the India-EU FTA text permits it for import, export, distribution, sale or use. While allowing for a broad scope of when access to source code may be demanded, the grounds for such demand are unspecified. In the specific instance of the India-EU FTA, this can be considered to allow sufficient room for safeguarding domestic interests if untested AI applications are considered inimical. The India-UK FTA, however, underscores broader prohibition as it doesn't qualify public policy objectives (Table 1). The CPTPP, negotiated a decade earlier, is the outlier in scope, confined to mass-market software. From a wider perspective, the India-EU FTA on source code access scope doesn't really suggest any aspect that is strikingly unusual from other FTAs of the EU, as well as the India-UK FTA. Furthermore, the critical-infrastructure provision in the India-EU FTA text is a notable inclusion. The CPTPP reaches a comparable result by a different route, excluding critical-infrastructure software from the prohibition's scope, but no other EU-template signatory obtained the provision India did.

Section 3: India's Comparative Disadvantage: Less-protected Software Exports and Absence of Domestic Regulations

While the uniform clause across three EU FTAs implies consistent application, there are, however, country-specific implications. In India's case, this becomes clear from the nature of its exports to the EU, as well as the depth of domestic regulatory capacity, or the lack of it, for utilising exceptions to access.

A country's source-code embedded software exports eventually reflect the worthiness of the access clause's protections in its various FTAs. Its domestic regulatory capacity determines its ability to exercise exceptions. It is important to identify these issues from an Indian perspective in the India-EU FTA. It's necessary to note, though, that all the EU FTAs discussed here are recent, with no evidence yet of a party invoking or being obstructed by a source-code clause. The analysis identifies the determinants likely to influence prospective outcomes.

Rules in FTAs prohibiting disclosure of source code protects a highly significant and intangible revenue-generating asset of software-exporting firms. Disclosing the code as a precondition for accessing the market of the FTA partner can erode firm-specific comparative advantages in exports. The implication matters much for India, which has several firms exporting software with proprietary content. Indeed, the potential comparative disadvantage of Indian software exporters in this regard is asymmetric to those of their European counterparts. The asymmetry becomes evident given that the Indian IT industry's dominant exports are IT services delivered under client contract, with services

¹⁷ The India-EU, EU-Korea and EU-Indonesia footnotes materially carry the same enumerated list of legitimate public policy objectives: public security, public morals, human, animal or plant life or health, public order, cybersecurity, safe and trustworthy artificial intelligence, and protection against disinformation. The EU-Indonesia text omits "online safety" from the list, and the India-EU text adds "and related challenges" as a closing phrase.

accounting for over 65 per cent of technology exports.¹⁸ Codes written to a client's specification are usually the client's property on delivery, as opposed to being Indian intellectual property stemming from innovative capacities of local software developers. The ability of Indian source code developers to protect their key asset in the EU market, therefore, is significantly low, as non-disclosure rules for source code are not matched by IP rights.

South Korea is a contrasting example. Korean-manufactured exports to Europe comprise embedded software of precisely the kind the source code rules protect. These primarily include chips – both latest generation advanced AI-chips as well as older legacy chips. The same text in two FTAs – EU- India and EU- Korea - ostensibly has different implications for exporters impacted by rules on source code access due to variations in export baskets. Both FTAs, though, will shield the growing stock of EU-owned AI systems operating within the other party's regulated sectors.

As mentioned earlier, FTA rules permit access to source codes for investigation, inspection, examination and enforcement. However, a state can investigate or enforce against an AI system only to the extent that its own laws define violations and authorise its regulators to act accordingly. Regulatory capacities in South Korea and India diverge sharply in this regard. Korea's Framework Act on the Development of Artificial Intelligence and Establishment of Trust statutorily empowers Korean regulators, while defining high-impact and generative AI, and administrative powers applicable to AI systems generally.¹⁹ India doesn't have a comparable domestic regulatory framework. Its domestic AI governance, till now, is confined to sectoral proposals that are yet to be developed into enforceable rules. These include the Reserve Bank of India's (RBI) FREE-AI Committee Report of August 2025²⁰ and the Securities and Exchange Board of India's (SEBI) June 2025 consultation paper on AI in securities markets.²¹

Without statutory authority for investigating AI systems, the capacity of domestic regulators to enforce exceptions to non-disclosure of source code rules in the EU-India FTA, is distinctly limited. The exception negotiated by India is ahead of the domestic law required to exercise it.

¹⁸ NASSCOM, Strategic Review 2025, op. cit.

¹⁹ Republic of Korea, Framework Act on the Development of Artificial Intelligence and Establishment of Trust (AI Basic Act), Act No. 20676, promulgated 21 January 2025, in force 22 January 2026. See International Trade Administration, United States Department of Commerce, 'South Korea Artificial Intelligence (AI) Basic Act', <https://www.trade.gov/market-intelligence/south-korea-artificial-intelligence-ai-basic-act>. Enforcement is being phased in behind a grace period of at least one year for most administrative fines.

²⁰ Reserve Bank of India, *Report of the Committee on Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE-AI)* (Mumbai: Reserve Bank of India, 13 August 2025), <https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/FREEAIR130820250A24FF2D4578453F824C72ED9F5D5851.PDF>.

²¹ Securities and Exchange Board of India, *Consultation Paper on Guidelines for Responsible Usage of AI/ML in Indian Securities Markets* (Mumbai: SEBI, June 2025), https://www.sebi.gov.in/reports-and-statistics/reports/jun-2025/consultation-paper-on-guidelines-for-responsible-usage-of-ai-ml-in-indian-securities-markets_94687.html.

Section 4: Implications of Asymmetry between the EU’s Domestic Law and the FTA Rules

The EU AI Act is the most fully elaborated market-surveillance framework for AI currently in force, applied to the same class of systems the EU FTAs cover when deployed within the EU. How the framework ranks its own instruments is instructive evidence of which instruments perform the substantive work of oversight.

Article 74 (Section 3, Chapter IX) of the EU’s AI Act ranks these explicitly. Paragraph 12 grants market surveillance authorities “full access” to “the documentation as well as the training, validation and testing data sets used for the development of high-risk AI systems”, including, where appropriate, remote access through application programming interfaces.²² Paragraph 13 treats source code separately and on stricter terms. It mandates access to source code ‘necessary to assess the conformity of a high-risk AI system’ and “testing or auditing procedures and verifications based on the data and documentation provided by the provider have been exhausted or proved insufficient”.²³ The framework clearly specifies documentation and data as the usual tools of oversight. In this regard, it is noteworthy that all the EU FTAs discussed in this paper regulate source code and none of them creates a right to documentation or to training, validation or testing data. This is in contrast to the emphasis on oversight instruments in the EU’s AI Act.

What kind of issues might arise from this inconsistency? The India-EU FTA regulates the prohibition of the source code of software. However, the understanding of ‘source code’ is subject to interpretation. For example, software exporters using AI can argue that source code protection extends to the protection of algorithmic logic in any form. Whether it is indeed so is debatable.

The India-UK CEPA provides greater clarity in this regard by excluding the expression of algorithms in any form. For the India-EU FTA, establishing the interpretation of source code to documentation would rest on the party asserting it, from either side. From an Indian perspective, however, even the most favourable source-code protection interpretation under the EU FTA might not provide its exporters with the cushion that the EU’s domestic laws provide its own regulators and businesses with. This is due to the difference between instruments of routine oversight vis-à-vis instruments of last resort, as discussed earlier.

Section 5: Summary and Concluding Thoughts

The EU’s FTA with India, at least in its draft text form, doesn’t imply a weaker source-code clause than the EU-Korea and EU-Indonesia FTAs. Furthermore, declaring AI as a legitimate public policy objective underscores an important regulatory goal. By way of comparison, the emphasis is missing from India’s FTA with the UK.

²² Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), Article 74(12) and 74(13). Text available via the European Commission’s AI Act Service Desk, <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-74>.

²³ Ibid.

The scope of obtaining access to source code used in critical infrastructure is also exclusive to the India-EU FTA, vis-à-vis the EU-Korea and EU-Indonesia FTAs. The provision safeguards apprehensions that India (or even the EU) might have in allowing access to ‘unchecked’ software in various critical infrastructure. The interpretation of critical infrastructure, again, is subjective but should include almost all areas with potential national security concerns, such as telecom, finance, healthcare, transportation, critical manufacturing and defence.

There are, of course, as discussed earlier, specific implications for the source code rules on EU partners like India and Korea, depending on their export profiles, as well as domestic regulatory capacities for oversight. Indeed, source code rules in the EU’s various FTAs will come up for more scrutiny as the EU enters more FTAs with developing and emerging market economies, especially from Asia, such as Malaysia, the Philippines and the UAE. Any decisive conclusion on the normative quality of these rules is not appropriate till a significant number of FTAs signed by the EU with various partners are available for study. It is also worth noting that several of the EU’s FTAs, including the one with India, while being adopted or ratified, are undergoing legal scrubbing of the texts. The final texts are those that should be compared for conclusive decisions.

At this stage, it is impertinent to describe the source code provisions in the EU-India FTA as contradictory to India’s larger strategic and economic aspirations on developing frontier AI and adapting AI applications for economic and developmental purposes. Pragmatic adaptation through incremental capability building is considered an optimal approach for India.²⁴ The EU can be an effective partner for India in this regard.

The European Commission’s AI Office, in July 2026, published a report aggregating the views of more than 100 experts convened under the European Frontier AI Initiative. The findings record that frontier AI development is concentrated largely outside the EU. Its own capacity to audit, evaluate and verify frontier AI systems deployed in its jurisdictions “is only emerging”.²⁵ In this regard, the Union’s market size, regulatory strength, industrial base and positions in the AI stack are considered leverage for accessing frontier models; choosing among their providers; controlling operation of the models within the EU, and sharing the value they generate. For the EU, sovereign audit and evaluation capacity are considered strategic choices. The coupling of domestic capability-building combined with regulatory leverage, as proposed by the report, resonates for India, too. Indeed, the report considers India a trusted partner for the EU for pooling leverage over developing and deploying frontier AI, including in treaty negotiations.

²⁴ Amitendu Palit and Kanika Kaur, 2026, “India’s Foundational Artificial Intelligence and Large Language Model Ambitions”, *ISAS Scan*, 26 March 2026, https://www.isas.nus.edu.sg/wp-content/uploads/2026/03/SouthAsiaScan-26_p3.pdf.

²⁵ European Commission, AI Office, *Enhancing Competitiveness, Sovereignty and Security of the European Union in Frontier AI: Key Insights from the First Meeting of the European Expert Forum on Frontier AI* (Luxembourg: Publications Office of the European Union, 2026), <https://digital-strategy.ec.europa.eu/en/library/ai-office-publishes-frontier-ai-expert-findings-eu-competitiveness-sovereignty-and-security>. The Expert Forum met in April 2026; the report aggregates discussions held under the Chatham House Rule and does not represent the Commission’s official position.

For India, it is imperative to invest in domestic oversight capacity through effective regulations influencing the use and adoption of AI. Source code rules can be important indicators in this regard.

A domestic regulatory framework delivering for India what Article 74(12) of the EU's AI Act does for it, requires statutory power, vested in designated authorities, for ensuring providers of AI systems in regulated sectors to furnish documentation and provide access to training, validation and testing data; defined risk categories; and confidentiality safeguards for disclosed material, which the trade texts presuppose as a condition of access. The sectoral work of the RBI, SEBI and their counterparts supplies the domain expertise on which such a framework would draw, and the India AI Mission's Safety Institute, constituted on a hub-and-spoke model under the Mission's Safe and Trusted pillar, is an early vehicle for the technical capacity to use what disclosure would yield.²⁶

None of this requires renegotiating the EU-India FTA. These were available to India before the FTA was negotiated and remain available now.

.

Dr Amitendu Palit is a Senior Research Fellow and Research Lead (Trade and Economics) at the Institute of South Asian Studies (ISAS), an autonomous research institute at the National University of Singapore (NUS). He can be contacted at isasap@nus.edu.sg. Ms Atyantika Kothuri Mookherjee is a former Research Intern at the same institute. She can be contacted atatmookherjee@davidson.edu. The authors bear full responsibility for the facts cited and opinions expressed in this paper.

²⁶ Ministry of Electronics and Information Technology, Government of India, "India Takes the Lead: Establishing the IndiaAI Safety Institute for Responsible AI Innovation", January 2025, <https://indiaai.gov.in/article/india-takes-the-lead-establishing-the-indiaai-safety-institute-for-responsible-ai-innovation>.