

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES
[ISSN 2581-5369]

Volume 9 | Issue 3
2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of any suggestions or complaints, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the International Journal of Law Management & Humanities, kindly email your Manuscript to submission@ijlmh.com.

Reimagining Trade Secret Protection for Semiconductor Fabrication and Masking Data in an Emerging Digital and Global Regulatory Landscape

KAVYA S*

ABSTRACT

The semiconductor sector plays an integral role in the development of pioneering digital technology and industrial innovation. The sector's competitive advantage is rooted in the secrecy of its fabrication processes and process combinations, which are protected as trade secrets. However, the growing digitalisation of the manufacturing workplace, the use of cloud-based design collaboration and cross-border data transfers have posed critical legal and regulatory challenges to the protection of these trade secrets. The current national and international framework for trade-secret protection is fragmented and inadequate, and existing data-protection laws do not adequately protect non-personal industrial data, deepening the legal lacuna. This paper analyses the existing trade-secret protection regime for semiconductor fabrication, reviewing the legal and enforcement mechanisms across jurisdictions, and examines the regulatory gap under data-protection laws. It discusses the overlap of trade-secret law, digital data regulation and international compliance with reference to semiconductor fabrication and masking data. The paper concludes by suggesting a holistic approach that balances the protection of trade secrets with the principles of digital governance in semiconductor manufacturing, so as to protect innovation and unify global compliance norms. This research adds to the existing debate on securing industrial data in the era of digitalisation.

Keywords: Semiconductor Fabrication, Masking, Trade Secrets, Non-Personal Industrial Data, Digital Data Regulation.

I. INTRODUCTION

Semiconductors are the main industrial input underlying modern computing, digital communications, high-end manufacturing and national-security systems. As the electronics market grows, countries are actively participating in regulation and promoting the manufacture of semiconductor integrated circuits alongside private-sector firms. In the evolving digital

* Author is a Student at The Tamil Nadu Dr. Ambedkar Law University, Chennai, TamilNadu, India.

landscape, a country's ability to produce and manufacture semiconductors has become a determinant of geopolitical power. The Indian Semiconductor Mission is one such initiative to achieve self-reliance and reduce dependency on imports. An integrated circuit is made by repeated photolithographic patterning and deposition, which involves creating ultra-high-resolution features on a silicon substrate by exposure to ultraviolet light, selective etching, selective deposition and continuous metrology. Within this process, the fabrication phase (the sequence of processes that introduce the transistor and interconnect layers onto silicon wafers) and the masking phase (the generation of patterning instructions and physical reticles that imprint circuit geometry onto wafers) are the most information-dense and value-rich parts of the value chain. The topography designs are protected primarily under the Semiconductor Integrated Circuits Layout-Design Act, 2000, and the final finished good by patent, but the underlying process is not explicitly protected under the existing intellectual property framework.

What determines economic advantage in fabrication and masking is not a single discrete invention. It is the entire accumulated body of proprietary production knowledge: the process settings and tolerances, the model and correction parameters, the tuning between design rules and real tool limits, the interpretation of defect signals, the tool-specific optimisation practices, and the learning that comes from successive yield ramps. These elements are not visible in the finished devices, cannot be reverse-engineered at a node-competitive cost, and are not revealed by a patent. They exist as non-public proprietary information, which makes them a core intellectual-property asset. The trade secret, rather than the patent, is therefore the legal right used to safeguard this information. Nevertheless, the doctrinal legacy of trade-secret law was designed for a setting in which knowledge could be geographically localised, employment relations were single-jurisdiction, and confidentiality rules were highly localised. None of these underlying assumptions holds in present-day semiconductor production networks. The relevant trade information is fully digital, resides in cloud infrastructure and automated EDA tool flows, and is regularly exchanged, often by necessity rather than choice, across many legal jurisdictions, supply-chain levels and legal instruments, including subsidy covenants, export controls, data-localisation requirements and national-security screening regimes.

This paper subjects the expertise of semiconductor fabrication and masking to a legal test, examining whether the existing form of trade-secret legislation can operate where the object of protection is a highly granular dataset distributed across borders in digital form. In particular, the paper will:

- (a) identify the elements of fabrication and masking that may be protected under the statutory definitions of the key trade-secret regimes;
- (b) consider how the “reasonable measures” standard must be applied where the secret is not a physical practice but a cloud-native, model-based, continuously-cycled and co-created dataset; and
- (c) compare the regulatory boundaries between the key regimes that govern the industry and assess whether this proprietary information can be protected under the ambit of data-protection laws.

A. Review of literature

Intellectual property in the semiconductor industry is heavily dependent on trade secrets, which safeguard proprietary manufacturing techniques, chemical formulas, circuit blueprints, software algorithms, business strategies and other confidential information essential to competitive advantage. The significance of trade secrets is highlighted by studies suggesting that they may constitute up to 80% of a semiconductor company’s intellectual-property value.¹ While patents must be disclosed and can become outdated with rapid technological advances, trade secrets can offer durable protection so long as confidentiality is maintained;² the short, rapid innovation cycles in semiconductor manufacturing make this feature particularly important.³

International law has established minimum standards for trade-secret protection in the TRIPS Agreement, which requires member States to protect undisclosed information of commercial value against unauthorised use or disclosure.⁴ In 1984, the United States enacted the Semiconductor Chip Protection Act (SCPA) to supplement international requirements and to offer a distinct form of protection for mask works.⁵ Mask-work protection is separate from trade-secret protection, which extends to the underlying know-how, manufacturing techniques and operational intricacies necessary to produce semiconductor products.⁶

Cross-border enforcement of trade-secret rights is particularly problematic in the semiconductor industry, as empirical studies show. Complex geopolitical and enforcement challenges have

¹ SEMICONDUCTOR INDUS. ASS’N, SEMICONDUCTORS & THE WORLD TRADE ORGANIZATION 4 (2020), https://www.semiconductors.org/wp-content/uploads/2020/11/The-WTO-and-the-Semiconductor-Industry-Nov-2020_2.pdf.

² Siemens Cre8 Ventures, *Strategies on IP Protection for Semiconductor Startups* (Nov. 10, 2024), <https://blogs.sw.siemens.com/cre8ventures/2024/11/11/strategies-on-ip-protection-for-semiconductor-startups/>.

³ *Id.*

⁴ Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299 [hereinafter TRIPS].

⁵ Semiconductor Chip Protection Act of 1984, 17 U.S.C. §§ 901–914; see *Intellectual Property: Mask Works*, KI Legal (June 2023), <https://www.ix-legal.com/blog/2022/february/intellectual-property-mask-works/>.

⁶ *Id.*

arisen in disputes involving trade-secret theft in jurisdictions with active semiconductor sectors, such as China, Taiwan and the United States.⁷ These studies emphasise that trade secrets are vulnerable to both conventional corporate espionage and cyber threats: supply-chain vulnerabilities or insider threats can allow actors to compromise semiconductor manufacturing secrets, with examples including former employees attempting to sell proprietary lithography process data, or malware infiltration through third-party suppliers causing production defects and large recalls. A strong trade-secret defence therefore requires a comprehensive strategy combining strict legal remedies, continuous technological protection and organisational discipline.⁸

A “trade-secret culture” is a crucial aspect of corporate practice. Taiwan Semiconductor Manufacturing Company (TSMC) maintains its technological superiority through strict internal controls, employee compliance programmes and advanced security measures.⁹ Trade secrets are not limited to layout designs and fabrication techniques; they also encompass chemical usage, impurity controls and testing protocols that secure competitive advantage and compliance with environmental and health regulations.¹⁰

In India, trade secrets are protected primarily through the equitable doctrine of breach of confidence and through contractual obligations under the common law, which poses enforcement difficulties given the rapidly growing sector and the strategic objective of becoming a major semiconductor manufacturing hub under initiatives such as “Make in India”.¹¹ Indian jurisprudence acknowledges trade secrets as commercially important, but the absence of a dedicated legal framework and rigorous enforcement mechanisms has been identified as limiting the protection of proprietary manufacturing knowledge.¹² To foster innovation and competitiveness in the rapidly expanding Indian semiconductor industry, commentators consider it essential to introduce legislative reforms that harmonise Indian trade-secret law with international standards while remaining tailored to domestic needs.¹³

⁷ Daniel Taylor, *An Empirical Study on Cross-Border Trade Secret Litigation Involving the Semiconductor Industry* 1 (2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4827530.

⁸ SEMICONDUCTOR INDUS. ASS’N, *supra* note 1; *Top 5 Cyber Threats Facing Semiconductor Manufacturing* (Aug. 24, 2025), <https://www.jisasoftech.com/top-5-cyber-threats-facing-semiconductor-manufacturing/>.

⁹ Tangibly, *Taiwan’s TSMC: A Trade Secret Cult(ure)* (Oct. 23, 2025), <https://www.tangibly.com/taiwans-tsmc-a-trade-secret-culture/>.

¹⁰ C. Yoon et al., *Chemical Use and Associated Health Concerns in Semiconductor Manufacturing*, 9 INT’L J. ENV’T RSCH. & PUB. HEALTH 1, 3 (2020), <https://pmc.ncbi.nlm.nih.gov/articles/PMC7728705/>.

¹¹ *Integrated Circuits and Intellectual Property Rights in India*, MANUPATRA NEWSLINE (2023), <https://docs.manupatra.in/newsline/articles/Upload/EADBC6CD-281A-4624-880F-8AB66E262126.pdf>;

MINISTRY OF ELECTRONICS & INFO. TECH., GOVERNMENT OF INDIA, MAKE IN INDIA INITIATIVE.

¹² M.P. Singh, *Legal Protection of Trade Secrets in India: Issues and Prospects*, 2024 J. INDIAN L. & SOC’Y 103.

¹³ *Id.*

B. Research Gap

The existing literature offers limited guidance on how to redesign trade-secret protection for fabrication and mask data in the face of cloud-based manufacturing, digital EDA tools, cyber risks, cross-border supply chains and emerging market trends. Most writing remains general, addressing trade secrets at large without engaging the specific semiconductor data that is actually stolen, such as reticle data, mask data and process recipes.

II. TRADE SECRET PROTECTION IN SEMICONDUCTOR FABRICATION AND MASKING

Trade secrets are a form of intellectual property comprising confidential business knowledge that provides economic value to the holder by being kept secret from competitors and the public. In the semiconductor industry, trade secrets encompass proprietary methods of depositing semiconductor layers, fabrication techniques that increase yield or minimise defects, and chemical formulas tailored to wafer treatments or photolithography. The mask works that represent the intricate layout designs of integrated circuits' transistor topographies, which form the basis of chip production, are also protectable assets of unique commercial value. Owing to the functional and competitive edge they provide, design algorithms and specialised testing and quality-control protocols are often protected as trade secrets as well. While patents offer only temporary exclusive rights upon publication, trade secrets can be preserved indefinitely if their confidentiality is maintained.

A. Legal Frameworks for Trade Secret Protection

A combination of national and international laws governs trade-secret protection in semiconductor manufacturing, shaped by industry demands and policy goals. This section outlines the primary legal systems, with emphasis on the United States, India and global standards, each of which has particular characteristics and significance in safeguarding semiconductor fabrication and masking trade secrets.

B. United States

The United States has a highly developed and robust trade-secret framework that integrates federal and state legislation, with the Defend Trade Secrets Act (DTSA) of 2016 viewed as introducing sweeping modernisation. Before the DTSA, the Uniform Trade Secrets Act (UTSA) and other state laws were the primary means of enforcing trade secrets, and they remain in place. Under the DTSA, owners may bring trade-secret misappropriation claims in federal court, which offers remedies such as injunctions, compensation and the civil seizure of property used

in the theft.¹⁴ The UTSA defines a trade secret as confidential information that derives independent economic value from its secrecy and is the subject of reasonable measures to maintain that secrecy.

The federal framework is crucial given the semiconductor industry's supply-chain and cyber-theft threats. The SCPA of 1984 complements the DTSA by safeguarding the layout designs of integrated circuits, commonly known as mask works, from unauthorised copying and distribution. The SCPA provides an alternative form of intellectual-property protection, similar to copyright but tailored to the specific challenges of semiconductor mask designs. Judicial clarification of the DTSA has also been significant, with U.S. courts applying the statute extraterritorially to trade-secret theft abroad that has a sufficient nexus to the United States, reflecting an assertive posture on the protection of semiconductor trade secrets in a globalised market.

C. India

By contrast, India's protection of trade secrets is not governed by any specific statute but by contract law, the doctrine of breach of confidence and evolving judicial decisions. Indian law recognises trade secrets as confidential business information of economic value whose protection requires reasonable safeguards. Judicial decisions turn on factors including the confidentiality of the information, its economic significance, and whether non-disclosure or confidentiality clauses are present in the relevant contracts. Landmark authority such as *Bombay Dyeing & Manufacturing Co. Ltd. v. Mehar Karan Singh* has emphasised these principles, establishing standards tailored to India's commercial needs.¹⁵

India's industrial policy has seen a surge of interest in the semiconductor industry, prompting discussion of dedicated legal provisions on trade secrets and strengthened cybersecurity measures to safeguard technical expertise. The Indian intellectual-property regime is expected to be affected by such reforms, which the cross-border nature of semiconductor fabrication and masking makes necessary.¹⁶

D. International Frameworks

A significant international benchmark is the World Trade Organization's TRIPS Agreement. The protection of confidential information of commercial value is a fundamental aspect of TRIPS,

¹⁴ *Explaining the Provisions of the Defend Trade Secrets Act*, Mintz (May 4, 2016), <https://www.mintz.com>.

¹⁵ *Bombay Dyeing & Mfg. Co. v. Mehar Karan Singh*, 2010 (112) Bom. L.R. 375 (India); see *Unresolved Issue at the Heart of the Interface Between IPR and Competition Law: A Trade Secrets Perspective*, NUJS (July 21, 2022), <https://nujssitc.wordpress.com>.

¹⁶ *Id.*

which requires member States to provide legal remedies for misappropriation. Trade secrets are explicitly protected in Article 39 of TRIPS,¹⁷ which mandates the prevention of unauthorised disclosure, acquisition or use through dishonest commercial practices. In addition, the Washington Treaty (the Treaty on Intellectual Property in Respect of Integrated Circuits) provides for a distinct form of intellectual-property protection for semiconductor designs and chip topographies. Such intergovernmental instruments facilitate cross-border regulation and promote conformity in the legal rules essential for semiconductor firms operating across multiple jurisdictions.

The interaction of trade-secret law and non-personal data regulation is complex. Data-localisation requirements, cross-border data-transfer protocols and the rise of artificial-intelligence-driven intellectual-property theft have heightened the need for flexible global legal frameworks that integrate trade-secret protection with broader digital-compliance strategies. The United States provides a comprehensive federal statutory scheme, India employs judicially developed principles within its contractual regime, and international law establishes a unifying baseline. Despite the complexity of this layered system, semiconductor companies must navigate and comply effectively with various legal systems to protect their intellectual-property rights.

E. Trade Secrets of Fabrication and Masking: Industry Practice

Semiconductor companies use a range of technical, legal and organisational methods to safeguard fabrication techniques and masking trade secrets. Each stage of the manufacturing lifecycle presents unique challenges that call for specific protection strategies.

The protection of proprietary wafer-fabrication methods involves compartmentalisation within companies, so that only necessary personnel can access essential knowledge. Digital models of processes and recipes are safeguarded by advanced cybersecurity measures, while fabrication plants are equipped with physical safeguards, including surveillance and controlled entry, that prevent the replication or monitoring of processes without authorisation.¹⁸ Legal measures such as strict confidentiality agreements with workers and partners, together with regular training on the handling of trade secrets, reinforce this protective culture.

Because chemical and material compositions directly affect product performance in wafer treatment and photolithography, they too are protected as trade secrets. Companies restrict

¹⁷ TRIPS, *supra* note 4, art. 39; see WIPO, *Guide to Trade Secrets and Innovation, Part III: Basics of Trade Secret Protection* (2024), <https://www.wipo.int>.

¹⁸ Baker McKenzie, *Protecting Trade Secrets in Your Manufacturing Global Supply Chain* (Feb. 17, 2022), <https://connectontech.bakermckenzie.com/protecting-trade-secrets-in-your-manufacturing-global-supply-chain/>.

supplier disclosure, enforce non-disclosure agreements, and maintain controlled digital and physical records. Techniques such as dual sourcing and internal research-and-development obfuscation help to minimise the risks of reverse engineering or external leakage.

Mask works are transmitted digitally, which exposes them to cyber theft. To prevent tampering, industry practices include encrypting mask data, using secure hardware modules for storage, and employing blockchain or distributed-ledger technology to record transactions. File sharing is typically limited by tightly controlled licences that restrict copying and use.

III. DIGITAL DATA PROTECTION AND ITS LIMITATIONS FOR NON-PERSONAL INDUSTRIAL DATA

The primary objective of most current digital data-protection laws is to safeguard individuals' privacy rather than to manage industrial datasets such as mask layouts and process logs. This is clearest in the EU General Data Protection Regulation (GDPR), which covers all identified or identifiable natural persons, leaving most non-personal datasets beyond its general scope. India's Digital Personal Data Protection Act, 2023 likewise focuses on personal information and leaves non-personal industrial data largely unregulated in private hands.¹⁹

A. The Regulatory Gap: Non-Personal Industrial Data

The absence of laws governing access to, sharing of, or appropriation of non-personal industrial datasets has led policymakers to explore dedicated frameworks for non-personal data (NPD). In India, an expert committee recommended an NPD Governance Framework (2020, revised December 2020), incorporating concepts such as high-value datasets (HVDs), data trustees and mandatory sharing for sovereign and public-interest purposes, but it was criticised for definitional ambiguity and inadequate scrutiny standards. Some commentators argued that the forced release of privately created non-personal datasets could undermine trade secrets, conflict with the protection of undisclosed data under Article 39 of TRIPS, and lower investment in data-intensive innovation. India's debate illustrates a global challenge: extracting social value from industrial data while maintaining firms' incentives to create and protect proprietary knowledge.²⁰

¹⁹ Infosys, *GDPR: An Industry and Geography-Agnostic Regulation* 2 (2017), <https://www.infosys.com/gdpr/documents/gdpr-industry-geography.pdf>.

²⁰ CSIPR (NLIU), *Revised Non-Personal Data Governance Framework and India's IPR Regime: An Inefficient Revision* (2021), <https://csipr.nliu.ac.in/copyright/revised-non-personal-data-governance-framework-and-indias-ipr-regime-an-inefficient-revision/>.

B. Semiconductor-Specific Exposure

Because of its competitive sensitivity, semiconductor manufacturing generates large volumes of non-personal data. Such files are used for design-technology co-optimisation (DTCO), optical proximity correction (OPC) and machine-learning-based optimisation across tools and suppliers, yet they fall within a “governance gap”: privacy laws do not protect them directly, while trade-secret law applies only if firms can demonstrate reasonable secrecy measures.²¹

C. Mandatory Sharing Proposals and Secrecy Interests

NPD proposals for sovereign or public-interest use raise difficult questions: how are semiconductor trade secrets to be protected, who determines a dataset’s “high value,” and what anonymisation requirements, scope restrictions and durations apply? Indian studies indicate that vague “public good” gateways with minimal procedural protection may enable overbroad data demands or facilitate competitors’ free-riding through data trustees. Experts have cautioned that the absence of clear exemptions and stringent confidentiality measures could violate the safeguards of Article 39 of TRIPS, reducing incentives for firms to invest in process research and data infrastructure.²²

D. Trade Secret Protection in Digitalised Manufacturing

Because the GDPR and the DPDP Act cover only personal data, companies must implement parallel trade-secret governance for non-personal industrial data. Leading foundries have shifted towards formal trade-secret registers to maintain inventories of confidential know-how and to simplify the presentation of evidence in disputes, a best practice relevant to any ecosystem. Cross-border master service agreements, data-processing addenda and consortium charters should define confidential information in non-personal industrial datasets, limit scope and implement appropriate technical safeguards. Firms should implement “need-to-know” segregation of mask databases (GDSII/OASIS), OPC models and process logs, minimise disclosure of datasets to third parties, and ensure that de-identification does not expose product signatures.

E. Policy Design Choices for Bridging the Gap

Where NPD regimes are contemplated, semiconductor stakeholders may seek balanced mechanisms: clear definitions of HVDs, transparent necessity tests, narrowly regulated

²¹ PRS LEGISLATIVE RSCH., *Non-Personal Data Governance Framework* (Oct. 29, 2025), <https://prsindia.org/policy/report-summaries/non-personal-data-governance-framework>.

²² SpicyIP, *Non-Personal Data Framework and Intellectual Property Implications* (Oct. 28, 2020), <https://spicyip.com/2020/10/non-personal-data-framework-and-intellectual-property-implications.html>.

applications, strict confidentiality requirements for trustees, audit trails, and remedial remedies for leakage or misuse. Creating carve-outs for proprietary algorithms, models and commercially sensitive manufacturing data can maintain incentives, while voluntary data marketplaces subject to competition-law oversight can achieve access goals without direct mandates. Procedural, multi-layered scrutiny and proportional compensation could secure integral protection of undisclosed information.

F. Risk Landscape and Practical Governance

The proliferation of advanced persistent threats (APTs) and insider threats can widen the attack surface unless zero-trust architectures, privileged-access management and continuous monitoring are in place. Manufacturers should use export-control-aware gateways for mask and process datasets, vet non-personal industrial-data disclosures against data-protection-impact-assessment standards, and conclude incident-response agreements with third parties.²³

IV. GLOBAL DIGITAL COMPLIANCE CHALLENGES AND FRAGMENTATION

Cross-border legal and regulatory challenges pose significant hurdles for semiconductor trade-secret data flows, requiring complex compliance strategies for multinational corporations. The digital-governance environment, which includes export controls, data-localisation mandates and varying national-security provisions, complicates efforts to protect sensitive industrial data in semiconductor manufacturing.

The implementation of stricter export controls in major countries is a significant problem. The U.S. Bureau of Industry and Security (BIS) has consistently heightened restrictions on advanced semiconductors and their manufacturing equipment, introducing licensing and notification requirements applicable to artificial-intelligence-capable chips and production equipment. These controls extend beyond direct shipments to transactions in third countries that benefit restricted entities, with a particular focus on China's technology sector and an expanding reach that now includes Macau and other jurisdictions. Such extraterritorial regimes impose substantial burdens on businesses seeking to control data exchanges while complying with the national-security objectives of various States.²⁴

Differing levels of digital compliance contribute to fragmentation. Under the WTO TRIPS Agreement, trade secrets and undisclosed information are protected by international standards, with member countries required to provide remedies for unfair commercial practices; yet

²³ Defend Trade Secrets Act of 2016, 18 U.S.C. § 1839(3) (codifying the *reasonable measures* requirement).

²⁴ Semiconductor Indus. Ass'n & Baker McKenzie, *Industry Reports on Cross-Border Data Sharing, Contractual Confidentiality, Export Control and Data-Sovereignty Clauses*, <https://connectontech.bakermckenzie.com/>.

methods of enforcement and definitions vary widely. The EU's Trade Secrets Directive provides civil remedies across member States and complements rigorous data-protection laws such as the GDPR, making data handling, cross-border transfers and vendor management in semiconductor supply chains increasingly difficult.²⁵

Several Asian countries have data-localisation laws that mandate the storage or processing of specific data types within their borders. China's regime, in particular, features extensive export controls, de minimis rules, reporting requirements for raw materials and intermediate semiconductor components, and jurisdiction over foreign direct products. This sets a high compliance threshold, requiring companies to track and report sensitive information across globalised manufacturing networks. India's policies remain in flux, with ongoing consultations on cross-border data governance and the protection of industrial trade secrets within the framework of emerging non-personal data laws.

These fragmented environments pose practical difficulties for multinational semiconductor companies. Strict cross-border transfer rules limit the prompt sharing of mask data, design files, telemetry and process recipes needed for collaborative development and just-in-time manufacturing. To meet the strictest applicable requirements, compliance teams must balance operational agility with risk management using layered encryption, segmented access controls and audit logs, while lawyers must draft contracts containing distinct confidentiality, data-sovereignty and export-control provisions for different jurisdictions.

Inadequate interpretation and regulatory overreach may unintentionally increase the risk of intellectual-property theft or forced technology transfer. Regulatory reporting that requires the disclosure of provenance or supplier information could be exploited by competitors or hostile actors, and the accumulation of such data raises the possibility of accidental leaks or targeted cyberattacks, underscoring the importance of comprehensive cybersecurity geared to digital-compliance requirements. To address this, industry leaders propose synchronised international standards that account for both national-security concerns and the commercial need for secure data flows. Sector-specific standards, cooperative enforcement frameworks and mutual-recognition agreements could simplify compliance and strengthen trade-secret protection. Investment in advanced data-governance technologies such as blockchain, artificial-

²⁵ Semiconductor Indus. Ass'n & CERRE, *Reports on Harmonized Compliance, Blockchain Applications and AI-Based Leak Detection in Semiconductor Supply Chains* (2025).

intelligence-driven anomaly detection and hardware security modules is becoming increasingly important to corporate strategy in multi-jurisdictional environments.²⁶

The regulatory split over semiconductor trade-secret data flows reflects broader geopolitical tensions and concerns about technological sovereignty. To thrive, multinational firms require flexible compliance architectures that integrate legal-risk management, cyber defence and operational flexibility supported by modern technology. Industry-wide coordination and policy dialogue are necessary to develop global digital-compliance regimes that ensure both innovation and security in the semiconductor supply chain.

V. TOWARDS AN INTEGRATED FRAMEWORK FOR TRADE SECRET AND DIGITAL DATA GOVERNANCE

A unified framework for trade-secret and digital-data governance in the semiconductor industry should integrate legal, technical and policy dimensions to address cross-border challenges and protect sensitive industrial data. Semiconductor companies operate in a highly fragmented regulatory environment defined by varied export controls, data-localisation laws and privacy requirements. An effective model would combine strong legal protections, modern technical controls and a coherent set of policy instruments to enable secure, accountable and compliant data sharing and cross-border enforcement.²⁷ The legal architecture should rest on explicit legislative trade-secret protections that comply with WTO TRIPS obligations, purpose-limited contracts that preserve confidentiality while curbing reverse-engineering effects, and export controls specific to the relevant jurisdictions and asset types. A layered legal framework converts conventional “reasonable measures” into auditable, legally binding compliance programmes that support trade-secret claims in disputes. Emerging U.S. guidance, supported by industry commentary, highlights an evidence-based approach that harmonises statutory law with effective cybersecurity practices.²⁸

The implementation of technical controls is crucial for translating legal obligations into practical safeguards. Embedding zero-trust data architectures with attribute-based access control tied to project and role specificity reduces exposure. Private or on-premises enclaves protect mask and OPC datasets, while hardware security modules safeguard the cryptographic

²⁶ JISA Softech, *Cybersecurity Risks Aggravated by Mandated Provenance Reporting and Data Aggregation* (2025), <https://www.jisasoftech.com/>.

²⁷ Anand & Anand, *Trade Secrets 2025* (Apr. 25, 2025), <https://www.anandandanand.com/news-insights/trade-secrets-2025/>.

²⁸ SEMICONDUCTOR INDUS. ASS'N, *Comments on U.S. Regulatory Estimates Relating to Semiconductors* (Oct. 31, 2025), https://www.semiconductors.org/wp-content/uploads/2025/10/SIA-Comments-National-Trade-Estimate-Report_FINAL.pdf.

keys that protect data in transit. Watermarking and fingerprinting of layout blocks, supported by blockchain technology, create tamper-evident data trails for detecting or prosecuting leaks, and immutable logs and confidential-computing environments enable third-party analytics without exposing raw data. These capabilities transform abstract legal norms into measurable controls and verifiable custody chains across global manufacturing workflows.²⁹

Policy alignment completes the model by enabling safe, lawful data movement. To avoid costly per-transaction re-engineering, firms should plan data flows in accordance with the strictest applicable baseline, particularly the EU's cyber-resilience requirements and U.S. export controls driven by national security. Standardisation reduces compliance overhead while preserving operational flexibility. Mutual-recognition agreements and multilateral frameworks can facilitate international coordination of enforcement and data-governance practices, ensuring that cross-border trade secrets are protected.³⁰ Governance also enables efficient data exchange and enforcement. Trade-secret datasets can be classified in dynamic registries that maintain relationships with relevant authorities to support targeted disclosure policies and export monitoring. Modular contract annexes, such as master agreements, data-sharing addenda, export-control appendices and cybersecurity schedules with jurisdiction-specific confidentiality and compliance terms, allow flexible adaptation. Before any international transmission, secure brokered data gateways regulate access through rate limits, inline data-loss prevention and export-control validation, while privacy-enhancing computation and pre-sharing data sanitisation reduce risk while respecting necessity-based access. Swift evidence-preservation protocols, forum and governing-law provisions, and thorough incident documentation strengthen the resolution of litigation and injunctions in fast-evolving situations.³¹

Multinational semiconductor firms adopting this framework must meet several practical prerequisites: establishing internal controls to the strictest jurisdictional standards; automating compliance checks; conducting regular cross-functional reviews involving legal, security and engineering teams; and maintaining regulatory horizon-scanning for emerging digital-trade regulations.

²⁹ IISD, *Cybersecurity and International Trade* (Aug. 2025), <https://www.iisd.org/system/files/2025-08/cybersecurity-international-trade-policy.pdf>.

³⁰ CERRE, *Global Governance for Digital Ecosystems* (Nov. 2022), https://cerre.eu/wp-content/uploads/2022/11/GGDE_FullReport.pdf.

³¹ NATIONAL FOREIGN TRADE COUNCIL, *Letter on Section 232 National Security Investigation of Imports of Semiconductors and Semiconductor Manufacturing Equipment*, Docket No. 250414-0066, <https://www.nftc.org/wp-content/uploads/2025/05/XRIN-0694-XC0021-NFTC-submission-and-appendix-Sec-232-semiconductors-and-SME-05072025.pdf>.

VI. CONCLUSION AND SUGGESTIONS

Ensuring the protection of trade secrets in semiconductor fabrication and masking in the evolving digital era requires a combination of legal protections, technical measures and responsive policy frameworks. With its extensive global supply chains and frequent data exchanges, the semiconductor industry faces significant hurdles from regulatory fragmentation, export restrictions, data-localisation laws and privacy regulations that prioritise personal information. This environment poses compliance challenges and exposure risks for sensitive industrial datasets such as mask layouts, OPC recipes and process telemetry.

Legal frameworks such as the U.S. Defend Trade Secrets Act, the Semiconductor Chip Protection Act and the international standards under TRIPS offer fundamental safeguards, but they must be implemented through strict corporate-governance measures, including contractual controls and secrecy protocols, to prevent misappropriation in practice. Meanwhile, non-personal data-governance proposals, particularly in India, highlight an inherent tension between societal interests in data access and the legitimate protection of proprietary industrial knowledge. Trade-secret enforcement increasingly relies on technological advances such as zero-trust architectures, encrypted enclaves, watermarking and immutable logs, which are crucial to keeping trade secrets secure.

Harmonisation remains the most important goal, notwithstanding competing national priorities and changing digital policies. In an increasingly digital and interconnected world, a forward-looking, integrated framework combining legal certainty, advanced technical controls and cross-jurisdictional policy coordination is necessary to maintain innovation incentives and to build resilient, compliant semiconductor manufacturing networks.

VII. RECOMMENDATIONS

A. Strengthen legal certainty. Governments should align trade-secret laws with TRIPS and provide explicit guidance on industrial non-personal data, including clear definitions, remedies and cross-border enforcement mechanisms. Sector-specific legislation should be considered, balanced against public-interest concerns such as whistleblower protection and emergency compulsory licensing.

B. Promote robust corporate governance. Semiconductor firms should establish trade-secret management systems standardised across their global operations, including comprehensive registries, routine staff training, contractual frameworks for data sharing and systematic incident-response protocols, in line with best practices such as the Taiwanese trade-secret management standard.

C. Deploy advanced technical protections. Firms should use cutting-edge data-security architectures such as zero-trust models, encryption, hardware security modules, fingerprinting and watermarking of mask and OPC data, secure enclaves for third-party analytics, and continuous monitoring, so as to translate abstract legal obligations into concrete defences and evidentiary assets.

D. Encourage policy coordination and mutual recognition. International organisations, trade groups and governments should work towards harmonised standards and mutual understandings that reconcile export controls, data-localisation laws and privacy regimes with the realities of the semiconductor supply chain, reducing operational friction and compliance burdens.

E. Promote industry cooperation. Open dialogue platforms involving semiconductor manufacturers, intellectual-property experts, regulators and cybersecurity authorities can help identify regulatory risks, share compliance best practices and jointly develop trade-secret and digital-data-governance standards tailored to industry specifics and evolving technology.

F. Balance access and protection in non-personal data governance. Policymakers should create frameworks for non-personal data governance that include precise definitions and necessity tests, strong safeguards and enforceable confidentiality, so as to secure social benefits while preserving the trade-secret protections and innovation incentives of semiconductor companies.
