ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

A Total Impact View of Trade, IP, and Data Privacy Law

Intellectual Property

Law Department Management

Technology, Privacy, and eCommerce

Cheat Sheet

- **Global trade restrictions.** Restrictive laws can be highly impactful on companies conducting international business.
- **Crossing specialism boundaries.** These are broader than direct sanctions and have become a wide and disparate group of multi-jurisdictional trade, export, data, and cybersecurity laws.
- **Commercial and strategy.** Business decisions should factor-in evolving and growing risks in these areas.
- **Silo dangers.** An overly siloed legal team may inhibit risk assessment, re-prioritization, and proactive business engagement for these risks.

Companies conducting foreign business today face a world with increasing international trade tensions. For governments of major economies, distinctions between “economic edge” and national security are growing narrower.

The United States, European Union, China, United Kingdom, and other jurisdictions use direct trade sanctions — which limit or prohibit trade — as geopolitical policy tools. Newly arising is the extent to which various jurisdictions are implementing other policies and laws with potentially similar (but indirect) economic effects, such as:

- Origin/export restrictions for new advanced technology;
- Personal data residency and export restrictions;
- Critical information infrastructure (CII) protectionism;
- National cybersecurity rules; and/or
- Local sourcing mandates.

These can work to reduce the size of addressable commercial foreign markets for many companies. We can term these “global trade restrictive” laws when such laws have an overall negative business impact for international trade.

This article touches upon various disparate global trade restrictive laws, before commenting on the structural implications of these developments for in-house legal departments supporting international business.

Globalization outlook

For several years, commentators have considered whether “peak globalization” — the theoretical point at which the trend toward more integrated world economies reverses or halts — has been passed.

It is reasonable to consider that the outlook for the coming decade is significantly more challenging than the past decade with regard to global trade restrictive laws, particularly for companies dealing in technology.

Relevant legal fields

In this context, in-house legal departments that treat the three distinct legal fields of **trade law, intellectual property (IP), and data privacy** as separate “silos” are at a disadvantage. Trade law expertise for sanctions (and increasingly, counter-sanctions) laws will typically require specialists. But the new and increasing prominence and scope of global trade restrictive laws means that a wider lens should be applied by in-house teams.

A holistic approach that enables “total impact” assessment of these laws and risks, coupled with the legal team’s proactive engagement with the business around these issues, can prove to be beneficial.

HQ location matters

Clearly, the headquarters location of your company will have a major impact to the applicability of global trade restrictive laws — that and your chosen foreign business locations will be the decisive factors. (My personal experience is based on working for non-US-HQ companies throughout my in-house legal career.)

Gaining in prominence: Restrictive global trade laws

Matters likely to require enhanced attention for international businesses in coming years include the following.

Export restrictions

Well-publicized are the risks of restrictions for semiconductors, biotechnology, and artificial intelligence (AI), but future restrictions could also apply to a wide scope of advanced technology and software. US restrictions on the export of advanced US technology considered “emerging and foundational” and “essential to the national security” of the United States are likely in the coming years.

The US export restriction review (an advance notice of proposed rulemaking) announced in November 2018 by the Bureau of Industry and Security included categories for: AI; advanced computer vision; speech recognition and machine translation; robotics and micro-drone systems; surveillance technologies; and navigation technology.

The first such restriction in this category was imposed in early 2020 by the Department of Commerce, Bureau of Industry and Security (BIS), on the export of US origin advanced machine learning technology to automate the analysis of geospatial imagery. For new technology with potential military application — which in coming years will include, for example, a potentially wide scope of advanced AI — the future risk of US restrictions to export should be considered.

The impact of such restriction would be to mandate a US BIS export license for any sale, except within the United States or Canada; this is an onerous process and difficult during competitive customer tender/bid processes.

As this is a rule-of-origin consideration, this category of restrictions can apply extra-territorially (i.e., globally), even if the vendor is not a US-headquartered company. Therefore, your resellers and distributors may also be restricted in their dealings with restricted US technology.

The risk of other major economies responding with equivalent restrictions is increased if the US proceeds with additional export restrictions for advanced technology.

Accordingly, for advanced technology, this requires a business awareness of:

- The full supply chain – meaning, suppliers of suppliers;
- The sales chain – monitoring and controlling activities of resellers/distributors; and
- The structure of the product under development – whether the item at risk of restriction is core, or a removable/optional module.

Personal data residency, security, and protection

China's cybersecurity watchdog, the Cyberspace Administration of China (CAC), is moving to impose personal data export protections on its large internet companies operating internationally. Following its US IPO, CAC commenced an investigation and imposed restrictions on Chinese ride-hailing giant Didi Chuxing in July 2021, citing a necessary review of the company’s data collection policies concerning national security. Law.com commented that “few, if any, saw it coming.”

In India in 2021 Mastercard and American Express were ordered by India's central bank to cease adding new customers due to alleged non-compliance with 2018 rules for payment systems providers regarding localization of user data.

Russia is expanding its export restrictions and personal data residency requirements for citizens' personal data. This mandates that for in-scope data the "primary" database, and potentially only database, must be in Russia.

Other countries are revising cybersecurity legislation concerning outsourcing and personal data transfers.

Data hosting location and data portability are therefore important considerations, not just from the Data Privacy angle, but also as regards global trade restrictions risk assessment.

Local sourcing mandates, designations, and foreign restrictions

US restrictions on technology transfer to Huawei and several other Chinese companies (via the BIS Entity List), are another factor making it vital for companies to fully understand their supply chains. Additionally against Huawei, the 2019 US National Defense Authorization Act (NDAA) placed a broad ban on US federal agencies and their contractors from using Huawei equipment on national security grounds. The possibility of these types of broad restrictions being applied to additional technology companies remains.

Under s.301 of the US Trade Act, wide powers are given to the president to impose duties or import restrictions on any country that "engages in discriminatory or other acts or policies which are unjustifiable or unreasonable" restricting US commerce. The 2021 US Trade Representative Report on Foreign Trade Barriers analysed 61 countries' trade barriers for US exports, commenting on several "unjustified" trade rules adopted by other major jurisdictions.

Upcoming requirements placed on Russian government-owned entities to source only Russian technology where possible will impact foreign companies. This mirrors to some extent the US "Buy American" policy rules for government procurement.

Critical information infrastructure designations by governments can impose additional burdens on foreign companies.

IP asset location and origin

IP asset location decisions may often be a tax-driven question. This decision should assess the impact of origin of software code in order that trade law compliance is not impeded for future sales. Software code ownership for IP purposes does not affect original "legal origin" if the development occurred outside a country that moves to restrict sales of its own "legal origin" advanced technology. This issue should be considered for IP sourcing, transfers, and restructurings.

For a non-US-HQ company, a development team outside the United States can maintain their product's exclusion from US jurisdiction only with careful planning. US rules-of-origin and jurisdiction may apply if: Ten percent or more of US-origin code or US-design work (calculated by value) is incorporated into the product (US citizens designing or developing the code outside the US count for this calculation); or IP is legally situated in the US for tax or financial purposes.

Standards strategy

Finally, while not strictly a “restrictive” issue, for rapidly evolving technologies, questions of promoting “universal standards” for adoption by an industry sector is a factor to consider for IP enforcement and therefore IP strategy.

Standards setting bodies can require open-sourcing of relevant patents and software code as a condition of contributing. This is a key strategic decision for companies engaging with standards setting bodies, possibly reducing IP enforceability but potentially leading to a larger addressable market globally.

If a company seeks to open-source its technology, that decision process should understand points of origin and export restrictions applying now and potentially in the future.

Decisions impacted by global trade restriction risks

In summary, the impact and risk of global trade restrictive laws should be factored into a wide range of key business decisions, including:

- Data hosting and support locations;
- Software development locations;
- IP asset locations (for tax purposes);
- Modular vs. core product/systems technology development;
- Sourcing strategy;
- Reseller/distribution strategy; and
- IP commercialization and enforcement strategy.

Structural points for in-house legal departments

For these reasons, in-house leaders should seek to address risks and opportunities of global trade restrictive laws holistically, in coordination with commercial strategy, IP, trade law, and data privacy strategy. This can be difficult when competing priorities exist. Separation of organizational expertise can be a further challenge.

For instance, as structural examples:

- **Trade law** expertise may sit in the compliance department, as primarily a “compliance” risk matter.
- **Data privacy** legal expertise may report to a chief privacy/data protection officer, outside the in-house legal team and focussing on data laws.
- **IP strategy** may largely prioritize commercial/tax considerations.

While these arrangements can be logical for many reasons, as a side-effect for complex international trade this structure may lead to risks of lack of proactive engagement in real-time as international business strategy is set, or global trade restrictive legal impact being insufficiently re-prioritized.

Even with high collaboration, given the overarching nature of global trade restrictive laws, gaps in understanding may still materialize if responsibilities and priorities are not adequately defined.

There is no “magic bullet,” and each organization will naturally approach these issues in the way it sees fit. But the new challenges discussed above may compel less “silo-ing” of legal expertise, to ensure the team is:

- Engaging all relevant legal specialists to **proactively identify** current and potential future global trade restrictive laws;
- Applying mechanisms for **assessment and re-prioritization** of these risks;
- Thereby enabling the company to **accept, avoid, or mitigate** those risks where necessary.

Accordingly, appointing a clear lead within the in-house legal team to own this scope overall, or to manage risk prioritization, may be beneficial (for example, the Deputy General Counsel or a Legal Chief of Staff).

In cases requiring the balancing of business risks arising due to conflicting priorities, facilitating the buy-in of the business’s senior management (e.g., via an appropriate “trade committee”) may also be beneficial.

With the appropriate focus and structure for these issues, engagement by the in-house legal team with the business to address these risks is more likely to bear fruit.

Stephen H. Baird

Associate General Counsel

SITA

Stephen H. Baird is an associate general counsel at SITA, the world's leading specialist in air transport communications and information technology. SITA serves over 200 countries and territories and is headquartered in Belgium and Switzerland. Baird graduated from the University of Western Australia's Law School and was a Federal Court of Australia Judge's Associate (clerk) before working in private practice for several years. He has worked as counsel for SITA for 19 years, leading on product technology, data and trade law matters, and is currently based in Geneva, Switzerland. Follow him on LinkedIn.