WorldECR

ISSUE 78. APRIL 2019
www.WorldECR.com

India: ITT controls

India and its ITT controls


Having traditionally been concerned with controls of exports of tangible products, the Indian authorities are working towards developing controls for intangible transfers and harmonising those with the rights of individuals, write Ameeta Verma Duggal and Aditi Warrier.

In India, goods, services and technology, whose export is controlled, are specified in the List of Special Chemicals, Organisms, Materials, Equipment and Technologies ('SCOMET List'). The SCOMET List, which comprises India's dual-use control list and Munitions List, is issued and regulated by the Directorate General for Foreign Trade ('DGFT'). While the overall regulation of the SCOMET List is carried out by DGFT, the Munitions List is implemented by the Department of Defence Production and the category pertaining to nuclear and nuclear-related material is implemented by the Department of Atomic Energy. The updated SCOMET List, issued in July 2018, is fully harmonised with the control lists of the various multilateral export control regimes, namely, the Missile Technology Control Regime, the Wassenaar Arrangement and the Australia Group, of which India is a Member State, and the Nuclear Suppliers Group, to which India has been an adherent for over a decade.

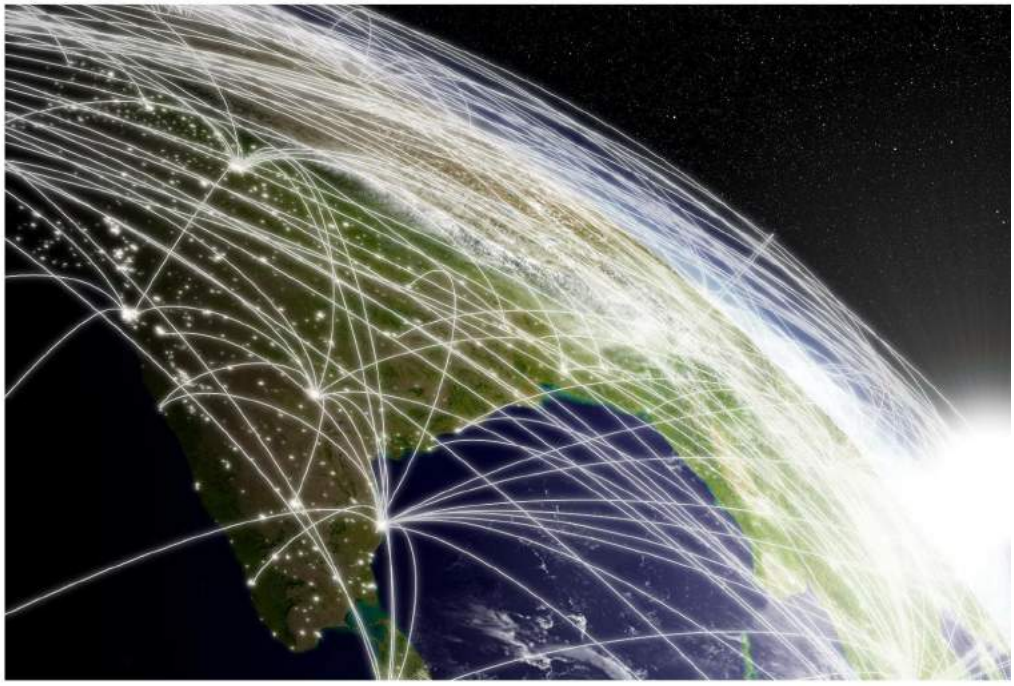
The extant export controls of India regulate the export, transfer, re-transfer, brought-in-transit, transhipment and brokering of goods, services and technology specified in the SCOMET List, which can be used for the development, production, handling, operation, maintenance, storage or dissemination of a nuclear, chemical or biological weapon, or of missiles specially designed for delivering any such weapon. Anything not expressly covered in the SCOMET List can be subjected to catch-all controls where the exporter has knowledge that the goods, services or technology are intended to be used in the design or manufacture of a biological, chemical or nuclear weapon or other nuclear explosive device, or in their delivery systems.

Export of such specified goods, services and technology is either prohibited or regulated. While there is a general prohibition on direct or indirect export to a non-State actor or terrorist, there are also country-, individual-, and/or product-specific prohibitions on exports to sanctioned countries, such as the Democratic People's Republic of Korea ('DPRK'), Iran and Iraq. These are targeted at the protecting national security, public order and fulfilment of obligations under the Charter of the United Nations for the maintenance of international peace and security. All other exports of items specified in the SCOMET List are regulated pursuant to the export control laws of India.

Intangible transfer of controlled technology has largely remained unchecked other than visa controls and telecommunication surveillance.

The SCOMET List regulates the export of controlled technology of both dual-use and munitions, however, the focus of the Indian regulators thus far has essentially been on tangible transfers of such technology, which can be subjected to border controls. Traditionally, India has remained focused on strengthening its enforcement machinery to check, regulate and curb unauthorised physical exports of items specified in the SCOMET List. Intangible transfer of controlled technology has largely remained unchecked other than visa controls and telecommunication surveillance (discussed below).

India's participation in the Wassenaar Arrangement has shifted its focus to the intangible transfer of technology ('ITT'). This is not yet a defined term but it is generally understood to mean the transfer of software and technology through intangible means, including transfer of



India: ITT controls

specific information or technical data necessary for the 'development', 'production' or 'use' of a product, such as blueprints, plans, diagrams, engineering designs, specifications, academic journals, training manuals and so forth, sent through e-mail, telephone, fax or the internet. ITT will also include transfer of technical assistance rendered through transfer of knowledge, training or instruction, consultation, collaborative research in universities and research institutions, seminars, and so on.

Regulatory framework

The export controls of India are governed under the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 ('WMD Act'), which is the umbrella legislation.

The WMD Act was incorporated by reference in the Foreign Trade (Development & Regulation) Act, 1992 ('FT Act') in 2010, as India's foreign trade policy is regulated pursuant to the FT Act. The SCOMET List is also issued by the DGFT pursuant to the FT Act.

Controls on transfer of technology

The WMD Act expressly (i) prohibits direct or indirect transfer of items specified in the SCOMET List to a non-State actor or terrorist; (ii) prohibits export of any material, equipment or technology, knowing that the same is intended to be used in the design or manufacture of WMD or in their delivery systems; and (iii) regulates the export, transfer, re-transfer, brought in transit or transhipment of items specified in the SCOMET List.

The WMD Act specifically prohibits any transfer of technology of an item whose export is prohibited. Transfer of technology controlled under the SCOMET List includes transfers effected

- by a person or from a place within India to a person or place outside India; and/or
- by a person or from a place outside India to a person, or a place, which is also outside India (but only where the transfer is by, or within the control of, any person who is a citizen of India or any person who is a resident in India).

The definition of 'export' in the FT Act also underwent a change in 2010 to mean – in relation to supplying services or technology – supply

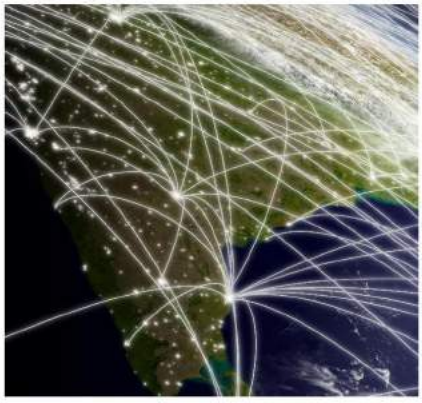
1. from India into the territory of any other country;
2. in India to the service consumer of any other country;
3. by a service supplier of India, through commercial presence in the territory of any other country;
4. by a service supplier of India, through presence of Indian natural persons in the territory of any other country.

Transfer of technology available in the 'public domain' is excluded from the ambit of controlled technology.

Technology defined

There is an express prohibition or regulation, as the case may be, under Indian law against transfer of controlled technology or transfer of technology with the knowledge that the same is intended to be used in the design or manufacture of weapons of mass destruction or their delivery system. The definition of 'technology' in relation to export controls, therefore, assumes significance. The WMD Act and the FT Act define 'technology' in a limited manner. The term has, however, evolved considerably over the years and pursuant to India's membership of the Wassenaar Arrangement, is now wide enough to include ITT. The extant definition of 'technology' in the SCOMET List provides that:

'except as otherwise provided for against any item in the SCOMET List,



information (including information embodied in software) other than information in the public domain, that is capable of being used in:

a. the development, production or use of any goods or software;
b. the development of, or the carrying out of, an industrial or commercial activity or the provision of a service of any kind.

Explanation 1: When technology is described wholly or partly by reference to the uses to which it (or the goods to which it relates) may be put, it shall include services which are provided or used, or which are capable of being used, in the development, production or use of such technology or goods.

Explanation 2: The information takes the form of "technical data" or "technical assistance". Specified technology is defined in the General Technology Note to the SCOMET Category 8. Specified technology for the Munitions List is defined in 6A022.

Technical notes

1. "Technical data" may take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories.
2. "Technical assistance" may take forms such as instruction, skills, training, working knowledge, consulting services. "Technical assistance" may involve transfer of "technical data".'

Exclusions to transfer of technology

Transfer of technology available in the 'public domain' is excluded from the ambit of controlled technology. The term 'public domain' is defined in the WMD Act (also adopted in the FT Act) to mean 'domain that has no restrictions upon dissemination of information within or from it; the existence of any legal rights to intellectual property in that information does not remove such information from being in public domain.' The SCOMET List clarifies this definition by adding that 'Copyright restrictions do not remove technology or software from being in the public domain.'

India: ITT controls

The SCOMET List also does not control software that is generally available to the public as being

1. sold from stock at retail selling points without restriction, by means of (a) over-the-counter transactions; (b) mail order transactions; (c) electronic transactions; or (d) telephone call transactions; and
2. designed for installation by the user without further substantial support by the supplier.

Controls also do not apply to 'technology' required for 'basic scientific research' or to the minimum necessary information for patent applications. Specifically, with respect to information security items, exceptions include those items of which the cryptographic functionality cannot easily be changed by the user; which are designed for installation by the user without further substantial support by the supplier; and, when necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in order to ascertain compliance with the SCOMET conditions.

Penalties for unauthorised export of technology

The express penalties provided for unauthorised export of items specified in the SCOMET List are shown in the table, above right. Apart from those listed, other penalties under the FT Act – such as inclusion in the Denied Entities List and additional penalties under the FT Act – will also be applicable.

Determination of ITT controls

The basic principle applicable to ITT controls is that transfer of technology in the on-line world or electronic media should be regulated equally as in the off-line world. While the broad regulatory provisions governing export controls concerning technology (including ITT) exist in India, the current regulatory mechanism does not actively provide for ITT controls. There is neither a specific definition of ITT in Indian law nor any express provision for what constitutes an export of ITT and when does such export occur. These specifics are integral to ITT controls since ITT controls require specific policies and practices for effective administration and enforcement. The extant regulatory mechanism provides for a single application form for authorisation to export the specified goods, services and/or technology. The same applies to the end-user certificate for export of items in the SCOMET List. The requirement of record keeping is also designed for tangible transfers of goods, services and technology.

Penalties for unauthorised export of technology

1.	Punishment for aiding any non-State actor or terrorist.	Imprisonment – 5 years to life Also fine.
2.	Violation of any provisions of WMD Act, including export of any item knowing that such item is intended to be used in the design of weapons of mass destruction or other nuclear device or in their missile delivery systems.	**First offence** Imprisonment – 6 months to 5 years Also fine **Subsequent offences** Imprisonment –1 year to 7 years Also fine
3.	Penalty for knowingly using false or making forged documents for submission to the competent authority.	Fine – Rs. 5,00,000/ – [five lakh rupees] **Or** 5 times the value of the materials, equipment, technology or services, whichever is more
4.	Punishment for offences with respect to which no specific punishment is provided under the WMD Act	Imprisonment – up to 1 year, **and/or** Fine

The basic principle applicable to ITT controls is that transfer of technology in the on-line world or electronic media should be regulated equally as in the off-line world.

Means of enforcement

Currently, export of controlled ITT is being authorised on the basis of express applications voluntarily made by the industry and such applications are more by way of exceptions rather than the norm. There is no express monitoring of ITT by the licensing authorities. However, there is an existing monitoring system in India, which functions on a general level, to safeguard the national interests of India and the furtherance of its international obligations towards maintaining global peace and security. This can be extended to ITT monitoring. It includes:

- visa screening under the aegis of the ministries of External Affairs and Home Affairs;
- power under the Information Technology Act, 2000 for interception, monitoring or decryption of any information generated, transmitted, received or stored in any computer resource, if necessary or expedient, *inter alia*, in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order;
- the central monitoring system ('CMS'), a centralised telephone interception provisioning system installed by the Centre for Development of Telematics, which is the autonomous telecom R&D centre of the Department of Telecommunications;
- telecom operators in India are also required by law to give access to their networks to law enforcement agencies; and
- the Official Secrets Act, 1923 that governs any wrongful 'communication' of 'information'

India: ITT controls

belonging to the government by 'any person', which is likely to assist, directly or indirectly, an enemy or which relates to a matter, the disclosure of which is likely to affect the sovereignty and integrity of India, the security of the State or friendly relations with foreign States, and so on. Violation of the Official Secrets Act attracts penalties provided thereunder.

The way forward for India and its ITT controls

Recognising this vacuum, the regulators are actively working towards addressing the area of ITT controls and developing a specific policy for their regulation. DGFT, along with the other relevant ministries and departments, including the Ministry of External Affairs, Ministry of Electronics and Information Technology, and the Department of Telecommunications, is working towards identifying and defining ITT and formulating its policy regarding ITT controls. It is understood that the thrust will be to answer the specifics of what and when concerning exports of ITT and the regulation thereof, including specific application forms and end-user certificates.

There is a need to revisit the extant definition of 'public domain', which excludes domain that has no restrictions upon dissemination of information within or from it, and may result in excluding the internet and cloud computing as well. While the regulators deliberate over this policy formulation, they also need to consider that proliferation has at least three aspects to it – export of physical goods, technical data, and technical assistance. It must be considered whether these three aspects are to be regulated individually or only in conjunction with each other.

Knowledge-transfer needs to be specifically addressed and regulated. This can be achieved by engaging with industry, universities, research institutions and academia and with targeted outreach efforts. This also needs to be examined in view of United Nations Security Council resolutions ('UNSCR') concerning DPRK, which require States to implement national controls on the transfer of certain types of technology, including knowledge and technical assistance to the target State. Specifically, UNSCR 1874 of 2009 and 2270 of 2016 call on all States to exercise vigilance and prevent specialised teaching or training of DPRK nationals within their territories or by their nationals of disciplines that could contribute to WMD proliferation. The extant prohibitions pursuant to the UNSCRs concerning DPRK are more economic and financial.

The regulators are actively working towards addressing the area of ITT controls and developing a specific policy for their regulation.

Industry compliance, through high levels of awareness and self-regulation, is especially important for ITT controls. The regulators are expected to provide for adequate internal compliance programmes and/or technical compliance programmes ('ICPs' and 'TCPs') along with periodic audits to ensure that industry is vigilant and compliant with its obligations under the export controls laws. The semantics of such ICPs/TCPs and audits are currently being discussed. The extant laws already provide for pre- and post-shipment verifications and the same will be equally applicable to ITT controls. Travel information regarding employees of sensitive sector industries could be part of the record keeping required.

Conclusion

As the regulators work towards developing a specific policy governing ITT controls in India, they will be required to strike a balance enabling them to regulate transfers without encroaching on personal freedoms, particularly rights to privacy and freedom of speech and expression. The monitoring and surveillance resulting from ITT controls will inevitably result in a debate on the sanctity of personal freedoms *vis-à-vis* such controls.

In 2017, the Supreme Court of India, in its decision in the case of *Justice K.S. Puttaswamy (Retd) vs Union of India*, elevated right to privacy as a fundamental right. The court has observed that privacy is the ultimate expression of the sanctity of the individual. Recognising privacy to be a fundamental right and 'informational privacy' to be a key element of an individual's right to privacy imbibing elements of privacy as secrecy, control and anonymity, the court commended to the government the need to examine and put in place a robust regime for data protection. India is currently finalising the appropriate legislation with a view to creating that robust mechanism to ensure and safeguard data privacy and security.

The National Digital Communications Policy – 2018 also recognises the fact that for purposes of effectively securing India's economic, social and political interests in the emerging data economy, it is imperative that its 'digital sovereignty', encompassing data ownership, privacy, security, autonomy and choice of its citizens, is treated as the prime consideration while participating in the global digital economy. One of the goals set out under the draft policy is to establish a comprehensive data protection regime for digital communications 'that safeguards the privacy, autonomy and choice of individuals'. For the same, the Department of Telecommunications proposes harmonisation of communications law and policy with the evolving legal framework and jurisprudence relating to privacy and data protection in India, including amending various licence terms and conditions to incorporate provisions with respect to privacy and data protection.

With this ongoing debate concerning personal freedoms of citizens of India, the relevant departments of the government need to harmonise their respective objectives and formulate policies that effectively regulate ITT controls while safeguarding these freedoms.

Ameeta Verma Duggal is the founder partner of DGS Associates. Aditi Warrier is an associate with the firm.

www.dgsassociates.in

WorldECR

The journal of export controls and sanctions

Contributors in this issue

Yohan Benizri, Sven de Knop and Alessandra Moroni, Sidley Austin LLP
www.sidley.com

Olivier Dorgans, Paul Charlot and Camille Mayet, Hughes Hubbard & Reed
www.hugheshubbard.com

Oleksiy Gorbatyuk, Ilyashev & Partners Law Firm
attorneys.ua

Mario Mancuso and Anthony Rapa, Kirkland & Ellis
www.kirkland.com

Ameeta Verma Duggal and Aditi Warrier, DGS Associates
www.dgsassociates.in

General enquiries, advertising enquiries, press releases, subscriptions: info@worldecr.com

Contact the editor, Tom Blass: tnb@worldecr.com tel +44 (0)7930405003

Contact the publisher, Mark Cusick: mark.cusick@worldecr.com tel: +44 (0)7702289830

WorldECR is published by D.C. Houghton Ltd.

ISSN 2046-4797. Refer to this issue as: WorldECR [0078]

Correspondence address: D.C. Houghton Ltd, Suite 17271, 20-22 Wenlock Road,
London N1 7GU, England

D.C. Houghton Ltd is registered in England and Wales (registered number 7490482) with its registered office at 20-22 Wenlock Road, London, UK

ISSUE 78. APRIL 2019
www.WorldECR.com