The following laws and regulations in Russia and China require their citizens to render assistance to their respective intelligence and security services, including in espionage against, and theft of technology from other states and those states' private companies. No democratic government imposes any such requirements on their citizens, as such requirements are not consistent with individual freedom and free markets.

Chinese Law	Statement	Year it went into effect	Sources	Russian Law	Statement	Year it went into effect	Sources
Article 77 of China's National Security Law	Citizens and organizations shall perform the following obligation for safeguarding national security: facilitate national security efforts and provide public security and military officials any support deemed necessary.	Effective July 2015	Gov.hk Chinalawtranslate Stanford.edu	Chapter 2: Rights and Freedoms of Man and Citizen; **Article 55** of Constitution of the Russian Federation	"Human and civil rights and freedoms may be limited by federal law only to the extent necessary for the protection of the basis of the constitutional order, morality, health, rights and lawful interests of other people, and for ensuring the defence of the country and the security of the State."	1993	Gov't archives constituteproject
Article 9 of China's Counter-Terrorism Law	All work units are obligated to aid and assist the relevant departments in the carrying out of counterterrorism work.	Effective Jan. 1, 2016 (Passed Dec. 27, 2015)	Chinalawtranslate Thediplomat Ohchr.org	Chapter 2: Rights and Freedoms of Man and Citizen; **Article 56** of Constitution of the Russian Federation	In the conditions of a state of emergency, in order to ensure the safety of citizens and the protection of the constitutional order and in accordance with federal constitutional law, certain restrictions may be imposed on human rights and freedoms with an indication of their limits and the period for which they have Effect.	1993	Gov't archives constituteproject
Article 28 of China's	Network operators shall provide technical support and assistance to public and	June 1, 2017	Newamerica	Chapter 2: Rights and Freedoms of	"Defence of the Fatherland shall be the duty and obligation of a citizen of	1993	Gov't archives

Cybersecurity Law	national security organs deemed necessary to safeguard national security.	(Passed Nov. 6)	Stanford.edu	Man and Citizen; **Article 58** of Constitution of the Russian Federation	the Russian Federation."		
Article 7 of China's Intelligence Law	All organizations shall support, assist, and cooperate with national security efforts. (Under the National Intelligence Law, the PRC has the ability to direct PRC firms to covertly install backdoors or "bug doors" into their equipment or software, allowing for easy access by PRC intelligence services.)	July 2017	Wikipedia Thediplomat Chinalawtranslate Brown.edu	**Federal Law No. 374** (an amendment to Federal Law "On Combating Terrorism")	"Data retention: Under the amendments, telecom operators must store all call and text message content for a period of six months, and the metadata of all calls and text messages for three years; Organizers of information distribution on the Internet must store metadata and user data for one year, and user content – for up to six months, and provide that information to law enforcement authorities at their request; All this data should be physically stored in the Russian Federation. Mandatory backdoors: Organizers of information distribution on the Internet must provide decryption keys at the request of FSB (Federal Security Service)."	Amendment: most in 2016 and the rest in 2018	Stanford.edu Cls.ru Hrw.org Tass
MOFCOM Order No. 1 of 2021 on Rules on Counteracting Unjustified Extra-territorial Application of Foreign Legislation and Other Measures	"Companies, organizations or social groups on the list shoulder the responsibility to roll out detailed measures against foreign espionage, including arranging their working staff to sign letters of commitment before taking up posts, reporting their activities related to national security, giving education to personnel ahead of their	2021	http://legal.people.com.cn/n1/2021/0426/c205462-32088423.html http://english.mofcom.gov.cn/article/policyrelease/a	**Federal Law No. 90-FZ** On Communications (an amendment to Federal Law No. 126-FZ; 2003)	"The telecom operator providing services for providing access to the information and telecommunications network 'Internet' is obliged to ensure the installation in its communication network of technical means to counter threats to the stability, security and integrity of the functioning of the information and telecommunications network "Internet" and the network on the territory of the Russian Federation….	Amendment: May 2019	consultant.ru internetgovernance Morganlewis Resourcehub exology

	departures abroad, and interviewing personnel after their return to China." (NOT A DIRECT TRANSLATION OF THE LAW; Global Times Summary of Law)		nnouncement/20210 1/2021010 3029708.s html https://ww w.globalti mes.cn/pa ge/202104 /1222185. shtml		provide information to the federal executive body exercising the functions of control and supervision in the field of mass media, mass communications, information technologies and communications."		
Article 31 of China's Cryptography Law	"Cryptography administrative departments and relevant departments shall establish the mechanism of both in-process and ex-post supervision on commercial cryptography, which combines routine supervision with random inspection, and shall establish a unified information platform for supervision and administration on commercial cryptography, coordinate the in-process and ex-post supervision mechanism and the social credit system, strengthen the self-discipline of commercial cryptography entities and public supervision." (Meaning: "The State Cryptography Administration" has full access to decryption keys, passwords, and any other information needed to access data on a commercially encrypted	2020 (Drafted April 2017)	https://the diplomat.c om/2019/1 0/decodin g-chinas-c ryptograph y-law/ https://the hill.com/op inion/cyber security/53 2583-for-c hinese-fir ms-theft-of -your-data -is-now-a-l egal-requir ement/ https://ww w.dhs.gov/ sites/defau lt/files/publ ications/20 _1222_dat a-security- business-a dvisory.pdf	**Russian Federal Law N 40-FZ** on the Federal Security Service; **Article 15**	"State authorities and also enterprises, establishments and organisations shall be under obligation to assist federal security service organs in the execution of the duties assigned to them. Physical persons and legal entities in the Russian Federation providing postal communications services and electronic communications services of all types, including scrambled, confidential, satellite communications systems, shall be under obligation, at the request of federal security service organs, to include in the apparatus additional hardware and software and create other conditions required by federal security service organs to implement operational/technical measures."	1995	policehuman rights Wired Internetgover nance

	server. Therefore, American technology companies must turn over intellectual and technological property if they seek to do business in China.")						
China's Data Security Law: **Article 2 →** **Article 21 →**	"Where data processing outside the territory of People's Republic of China harms the national security, public interests, or the lawful rights and interests of individuals or organizations of the People's Republic of China, legal liability shall be investigated in accordance with the law." —- "The state shall establish a categorized and classified system and carry out data protection based on the importance of the data in economic and social development, as well as the extent of harm to national security, public interests, or the lawful rights and interests of individuals or organizations that will be caused once the data are altered, destroyed, leaked, or illegally obtained or used. The coordination mechanism for national data	Sept. 2021 (Passed June 2021)	http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml https://foreignpolicy.com/2022/01/28/china-data-governance-security-law-privacy/?fp_data_gov_completed_form=1 https://thehill.com/opinion/cybersecurity/532583-for-chinese-firms-theft-of-your-data-is-now-a-legal-requirement/	**Decree of the Government of the Russian Federation No. 299** dated 06.03.2022 "On Amendments to Clause 2 of the Methodology for Determining the Amount of Compensation Paid to a Patent Owner When Deciding to Use an Invention, Utility Model or Industrial Design without His Consent, and the Procedure for Its Payment" Which countries are	"In relation to patent holders associated with foreign states who commit unfriendly actions against Russian legal entities and individuals (including if such patent holders have citizenship of these states, their place of registration, the place of their primary business activities or the place of their primary profit from the activities are these states), the amount of compensation is 0 percent of the actual proceeds of the person who has exercised the right to use an invention, utility model or industrial design without the consent of the patent owner, from the production and sale of goods, performance of work and provision of services, for the production, implementation and provision of which the relevant invention, utility model or industrial design has been used." Which countries are unfriendly? ("Albania, Andorra, Australia, Canada, members of the European Union, Iceland, Japan, Liechtenstein, Micronesia, Monaco, Montenegro, New Zealand, North Macedonia, Norway, Singapore, San Marino, South Korea, Switzerland, Taiwan	2022	http://actual.pravo.gov.ru/text.html#pnum=0001202203070005 http://government.ru/en/docs/44745/

Article 22 →	security shall coordinate the relevant departments to formulate a catalog of important data and strengthen protection of important data. Data concerning national security, lifelines of the national economy, important aspects of people's lives, major public interests, ect., are core data of the state, for which a stricter management system shall be implemented. All localities and departments shall, in accordance with the categorized and classified data protection system, prepare specific catalogs of important data for their respective regions, departments, and relevant industries and sectors, and give priority to the data listed in the catalogs in terms of data protection." —- "The state shall establish a centralized, unified, highly effective, and authoritative mechanism for assessing, reporting, information sharing, monitoring, and early alert of data security risks. The coordinating mechanism for national data security shall make an overall plan on and coordinate relevant departments in strengthening the work		https://thediplomat.com/2020/09/chinas-draft-data-security-law-a-practical-review/ https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf	"unfriendly?": (**Government Directive No. 430-r** of 5 March 2022)	(the Republic of China), Ukraine, the United Kingdom, including Jersey, Anguilla, British Virgin Islands and Gibraltar, and the United States of America.")		

	about acquiring, analyzing, researching and evaluating information of data security risks and the work about early alert of such risks." —- "Those conducting data activities as well as research and development of new data technologies shall benefit the advancement of economic and social development, enhance the people's welfare, and conform to social morals and ethics." —- "Processors of important data shall, in accordance with the relevant provisions, conduct risk assessments of their data processing on a regular basis and submit risk assessment reports to relevant competent departments. Risk assessment reports shall include the types and amounts of important data processed, information on data processing, data security risks and the response measures for them." —- "An organization or individual shall collect data by lawful and proper means, and shall not acquire data by theft or in other illegal						
Article 28 → **Article 30 →**							

	manners.						
Article 32 →	Where laws or administrative regulations have provisions on the purposes or scopes of data collection and use, data shall be collected and used for the purposes and within the scopes provided for by those laws and administrative regulations." —-						
Article 33 →	"When providing services, data transaction intermediaries shall require data providers to specify the sources of the data, verify the identities of both parties to the transactions, and retain the verification and transaction records." —- Commentary: "New data classification categories aimed at protecting national security are loosely defined, leaving interpretation up to Chinese authorities. The DSL references two main categories of sensitive data—national core data and important data—with new guidelines for governing each. "National core data" is defined as data concerning national security, economic interests, Chinese citizens'						
(Builds on Cybersecurity Law and expands China's reach)							

	welfare, or the public interest, and is categorized as the most sensitive data type. "Important data" is categorized as the second most sensitive data type but is not clearly defined in the text. Instead, regulatory authorities at the local level are expected to issue additional guidelines as to what constitutes important data for their jurisdiction, but the timeline for issuing the guidelines has not yet been determined."						
Article 13 of China's Personal Information Protection Law	"Personal information handlers may only handle personal information where they conform to one of the following circumstances: 1. Obtaining individuals' consent; 2. Where necessary to conclude or fulfill a contract in which the individual is an interested party, or where necessary to conduct human resources management according to lawfully formulated labor rules and structures and lawfully concluded collective contracts; 3. Where necessary to fulfill statutory duties and responsibilities or statutory	November 2021 (Passed Aug. 2021)	https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ https://foreignpolicy.com/2022/01/28/china-data-governance-security-law-privacy/?fp_data_gov_completed_form=1 https://ww		(There is a 2021 National Security Strategy that is very different from years past. Could not find translated versions; however, there might be something related to this law) See here	2021	

	obligations; 4. Where necessary to respond to sudden public health incidents or protect natural persons' lives and health, or the security of their property, under emergency conditions; 5. Handling personal information within a reasonable scope to implement news reporting, public opinion supervision, and other such activities for the public interest; 6. When handling personal information disclosed by persons themselves or otherwise already lawfully disclosed, within a reasonable scope in accordance with the provisions of this Law. 7. Other circumstances provided in laws and administrative regulations. In accordance with other relevant provisions of this Law, when handling personal information, individual consent shall be obtained. However, obtaining individual consent is not required under conditions in items 2 through 7 above." Commentary: "The law governs data		w.skadden.com/Insights/Publications/2021/11/Chinas-New-Data-Security-and-Personal-Information-Protection-Laws https://thehill.com/opinion/cybersecurity/532583-for-chinese-firms-theft-of-your-data-is-now-a-legal-requirement/				

	collection from both public and private companies and includes provisions mandating that Chinese government agencies notify and obtain consent from individuals. However, the provisions related to Chinese government data collection do not apply in situations where it is necessary for “acting in the public interest.”						