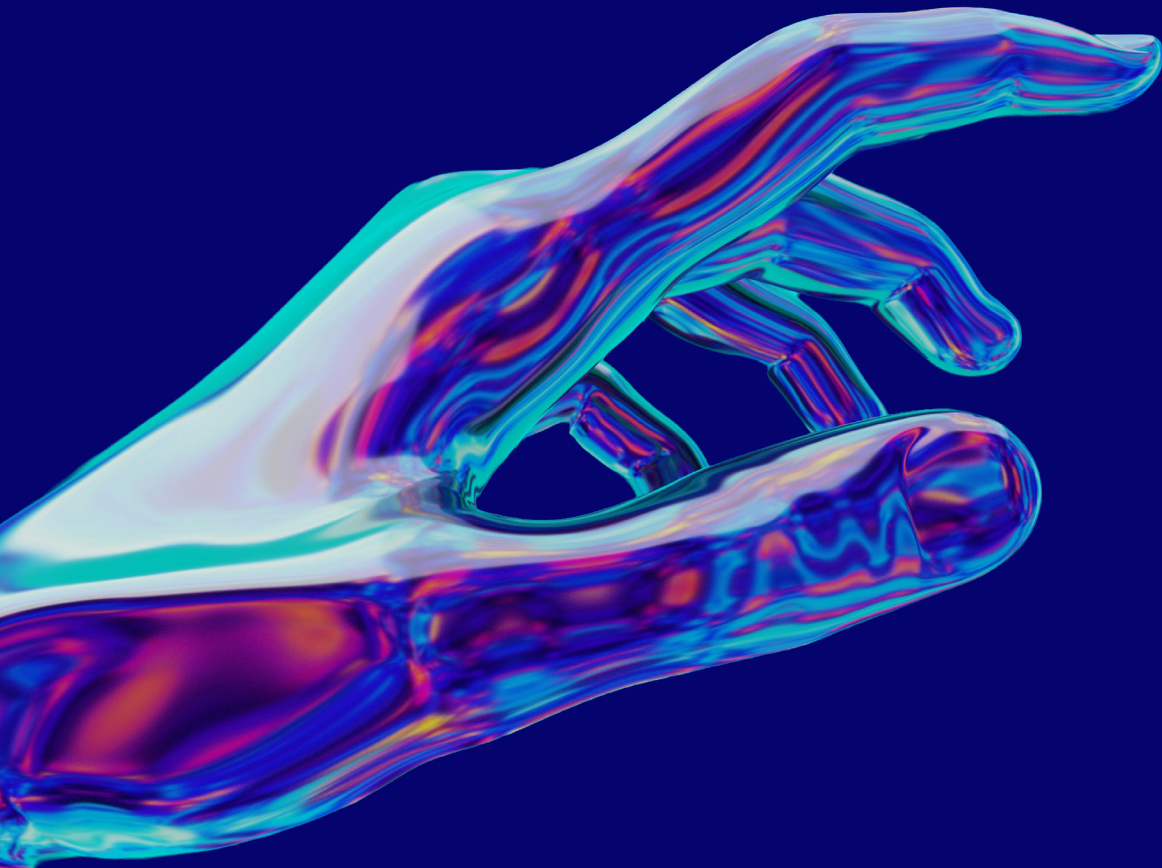


Technology-Based Disputes and Investment Treaty Arbitration



Charlie Lightfoot, Juan Nascimbene
and Yarik Kryvoi

Cooley



British Institute of
International and
Comparative Law

Contents

Introduction	4
Executive summary	5
Scope of the paper	6
Investment treaty arbitration in the technology sector is still in its infancy but is a growing area	8
When will tech investments qualify as protected investments under investment treaties?	10
Technology companies' investments and <i>ratione materiae</i> jurisdiction	10
The <i>Salini</i> test and technology investments	10
Jurisdiction <i>ratione territorialis</i> and technology companies	11
Substantive investment claims that technology companies could bring against states	13
Fair and equitable treatment	13
National treatment and most-favoured nation treatment	13
Full protection and security	14
No direct or indirect expropriation without full compensation	14
No requirement to transfer technology as a condition of investment	14
The impact of states' regulatory powers and defences	16
Case studies of potential areas where technology companies may bring investment-treaty claims against states	18
Data localisation	18
Fair and equitable treatment	19
Performance requirements	19
Indirect expropriation	19
Online censorship	19
Fair and equitable treatment	20
Indirect expropriation	20
Forced compensation schemes	20
Regulation of AI and other disruptive technologies	21
Outlook and future trends	23

Table of recurring terms and abbreviations

FET

Fair and equitable treatment

ICSID

International Centre for Settlement of Investment Disputes

IIA

International investment agreement

Minimum standard of treatment

The customary international law minimum standard of treatment

National treatment

The national treatment standard ensures competitive equality and prohibits any discriminatory treatment between foreign and domestic investors and their investments

Most-favoured nation (MFN)

Clauses intended to ensure equality and nondiscrimination in the treatment of protected investors compared with other foreign investors in the host state

ISDS

Investor-state dispute settlement

BIT

Bilateral investment treaty

1. Introduction

The technology sector has emerged as the dominant force in the global economy, with digital platforms, software companies and technology-enabled services reshaping commerce, communication and social interaction. Technology companies now represent nine of the world's 10 most valuable corporations by market capitalisation, with a collective valuation exceeding \$10 trillion (this is the combined economies of Japan, Germany and the UK). A dramatic shift in regulatory approaches is accompanying this economic transformation, as governments worldwide grapple with challenges ranging from data privacy and cybersecurity to market dominance and content moderation.

The intersection of technology-sector regulation and international investment law represents one of the most significant emerging frontiers in investor-state dispute settlement (ISDS). Whilst investment treaty arbitration has traditionally focused on disputes involving natural resources, infrastructure and manufacturing, today technology companies are increasingly starting to invoke investment treaty protections to challenge regulatory or other measures affecting their operations. This development raises fundamental questions about the applicability of analogue-era legal concepts to the digital economy.

This paper provides a detailed analysis of how investment treaty law applies to technology-sector regulation, examining both doctrinal frameworks and empirical evidence from arbitral practice. The analysis proceeds in the following parts. First, it examines what constitutes a protected 'investment' for technology businesses. Second, it analyses the jurisdictional and territorial challenges posed by digital business models. Third, it evaluates how contested regulatory or other relevant measures relate to core investment treaty standards, including fair and equitable treatment (FET), expropriation and nondiscrimination.

The authors would like to thank professor Tomoko Ishikawa for contributing her expertise as a panellist at the launch event of this paper. Special thanks also go to Victoria Barlow (associate at Cooley LLP) and Nikki Taylor (trainee at Cooley LLP) for their assistance and dedication in helping to prepare this report.

Authors



Charlie Lightfoot
Partner
Cooley (UK) LLP



Juan Nascimbene
Special Counsel
Cooley (UK) LLP



Professor Yarik Kryvoi
Senior Fellow and
Director of the
Investment Treaty Forum
British Institute of
International and
Comparative Law (BIICL)

2. Executive summary

- Data has become one of the most valuable assets in the global economy and is frequently described as the “new oil.” As business models increasingly rely on data analytics, artificial intelligence (AI) and cross-border digital services, disputes involving technology companies are likely to grow. The economic centrality of data makes it inevitable that more regulatory conflicts will reach international arbitration.
- Technology companies now dominate global markets, with nine of the 10 largest companies operating in the tech sector. Their influence extends beyond commerce into communications, finance and even political discourse. This expanding economic and social power has prompted governments to introduce stricter regulation, creating structural tension between innovation and sovereignty.
- Although relatively few investment treaty claims have been brought by technology companies to date, this may soon change. Traditionally, extractive and infrastructure investors have relied more heavily on treaty protections. However, as digital regulation intensifies – particularly in areas like data protection, AI governance and platform moderation – technology companies are increasingly likely to invoke investment agreements.
- A defining characteristic of major technology firms is their centralised operational structure combined with globally distributed services. Strategic decisions regarding data, algorithms and platform governance are typically taken at headquarters, while services are provided across numerous jurisdictions, often without a significant physical presence in each market.
- This delocalised business model raises complex jurisdictional questions. In states where a company has no offices, employees or infrastructure, it may be difficult to establish investor status or territorial nexus. Tribunals may need to determine whether such companies qualify as investors or merely as cross-border service providers.
- To bring a claim under an international investment agreement, a technology company must demonstrate the existence of an “investment” and that it was made in the territory of the host state. Under the Salini test, this generally requires contribution, risk, duration and, in the ICSID context, contribution to the host state’s economy. Digital investments, such as data centres, long term service contracts and local user networks, may satisfy these criteria, but asset-light digital models require careful assessment.
- An unresolved conceptual issue is whether data itself can constitute a protected investment. While data does not typically confer exclusive ownership rights and is subject to regulatory frameworks such as data protection laws, it may fall within broad treaty definitions as intellectual property, goodwill, contractual rights or other intangible property. Although no tribunal has yet ruled definitively on this question, the legal framework allows for such recognition.
- The territorial requirement in investment treaties presents additional challenges in the digital economy. Cloud computing and remote service delivery blur traditional notions of territorial presence. Tribunals may look for substantial economic impact or operational engagement within the host state to establish the necessary nexus, even in the absence of extensive physical infrastructure.
- On the merits, FET is likely to be central in technology-related disputes. However, its scope depends on treaty wording: Some treaties provide broad autonomous protection, while others tie FET to the customary international law minimum standard. Claims may arise from abrupt regulatory changes, discriminatory enforcement or disproportionate restrictions on digital operations.
- National treatment and most-favoured nation (MFN) provisions may also be invoked where foreign technology companies are treated less favourably than domestic competitors. Yet satisfying the “like circumstances” test can be complex in a sector characterised by innovation, disruptive technologies and differing business models.
- Expropriation claims may emerge where state measures substantially deprive technology companies of the value of their investments – for example, through sweeping platform bans or strict data localisation rules. Nevertheless, states retain regulatory powers to act in the public interest, particularly in areas like privacy, national security, public health and competition. Tribunals are likely to focus on proportionality, legitimate expectations and good faith.
- Overall, the convergence of powerful global technology companies and expanding state regulation creates fertile ground for future investment disputes. While doctrinal challenges remain – particularly regarding the nature of digital assets and territorial nexus – international investment law appears adaptable. As regulatory intervention deepens, tech-related arbitration is likely to become a more prominent feature of the investment treaty landscape.

3. Scope of the paper

The World Bank’s Information and Communication Technologies sector strategy paper defines information and communication technologies as “hardware, software, networks, and media for collection, storage, processing, transmission, and presentation of information (voice, data, text, images)”.¹

Applying this definition, these companies may include platform-based businesses enabling commercial transactions (ecommerce); telecommunications; businesses providing services, such as streaming, cloud computing, data analysis, data mining and online gaming; social media; and businesses based on emerging technologies, such as cryptocurrencies and AI.

The past 20 years have seen an exponential rise in the number and scale of technology companies globally. As Table 1 (below) shows, in 2005, technology companies only comprised three out of the 10 largest companies (in terms of market capitalisation). In 2026, nine out of the 10 largest companies in the world are technology companies. Additionally, the top five most valuable companies globally are now all technology-based, in comparison to only one in 2005. For instance, NVIDIA, the most valuable company, has a market capitalisation of more than US\$5 trillion.

Of course, even companies that do not meet the above definition are increasingly adopting new forms of technology to improve their business models, and technology has become integral to virtually all major companies’ operations, with digitalisation and interconnection now permeating every aspect of commercial activity and daily life.

Table 1 – Largest companies worldwide by market capitalisation

10 LARGEST COMPANIES IN THE WORLD, 2005 (BY MARKET CAPITALISATION) ²	10 LARGEST COMPANIES IN THE WORLD, 2026 (BY MARKET CAPITALISATION) ³
1. General Electric Company	1. Nvidia
2. Exxon Mobil	2. Apple
3. Citigroup	3. Alphabet (GOOGL)
4. Microsoft	4. Microsoft
5. Procter & Gamble	5. Amazon
6. Bank of America	6. Meta Platforms
7. Johnson & Johnson	7. Tesla
8. American International Group	8. Taiwan Semiconductor Manufacturing
9. Pfizer	9. Broadcom
10. Philip Morris International	10. Berkshire Hathaway

As the number of technology-based companies and the adoption of AI has surged, so has the number of governmental regulations and states’ appetite to regulate these companies.⁴ For example, since 2016, the total number of times AI has been mentioned in legislative proceedings globally has increased more than ninefold.⁵ The willingness and ability of states to regulate emerging technologies has become a subject of significant political, economic and public debate.

This clash between the rise of technology companies (and their omnipresence in the global economy) and the rise in governmental regulations has led to disputes between technology companies and states across the world. Most of these disputes have been resolved by negotiation, but that will not always be possible and will often take place in the context of actual or threatened legal proceedings. This report aims to examine how technology companies already resort – and may resort in the future – to international arbitration to resolve such disputes.

What makes tech disputes different from other types of disputes?

Investment-treaty disputes in the technology sector differ from other disputes for at least five reasons.

First, most large technology companies today operate through delocalised business models. While core technical functions – data processing, AI model training and the governance of digital platforms – are often conducted from a central headquarters or limited server infrastructure, technology companies offer services and digital assets which span across different jurisdictions where the company may have little to no actual physical presence.

For instance, as of 2026, Meta’s services have users in virtually every country worldwide, yet Meta has established offices in only 37 countries.⁶ Similarly, while PayPal operates across 200 countries and regions,⁷ it has established a physical footprint in only 29 countries.⁸

This delocalised operational model common in the technology industry raises complex cross-jurisdictional legal issues. For example, there may be no physical or legal entity within a country over which a court can exercise jurisdiction or no jurisdictional nexus by which an aggrieved party may bring a claim against a technology company.

Second, technology disputes often arise in relation to digital assets, including data, algorithms and distributed systems, engaging different governing laws that make enforcement complex or problematic. Some states have responded by requiring technology companies to establish local legal entities, data centres or other physical infrastructure within their jurisdictions – a practice known as ‘localisation’ to ensure regulatory oversight. The emergence of decentralised AI, “which combines the power of AI with blockchain technology”,⁹ further increases the regulatory and jurisdictional complexity of such disputes.

Third, data protection issues more commonly feature in tech disputes than in many other disputes. Data from users is one of the core assets of social media companies and is often the primary means by which they generate revenue, through targeted advertising and sponsored content.

Fourth, intellectual property concerns also arise frequently in technology-related disputes. Technology companies occupy eight of the top 10 positions in Brand Finance’s Global 500 2025 brand rankings,¹⁰ highlighting their crucial importance in this sector. New technologies also raise novel questions for intellectual property law – whether, for example, AI is just a tool for use by humans akin to software or whether its ability to behave autonomously means that it should be dealt with differently under IP law remains unclear.¹¹

Finally, with growing economic power and the ability to decide on and moderate content, Big Tech companies have found themselves with increased political and social influence. In response, governments are looking to introduce new regulatory frameworks and restrictions to moderate this growth. This generates friction and conflict between Big Tech companies and states, giving rise to disputes which could end up in international arbitration.

Against this background, this report discusses disputes between technology companies and states. Rather than attempting to present a comprehensive picture of all potential issues in technology-related disputes, we present and examine several key legal issues which commonly arise and how arbitration tribunals have addressed them in practice or might address them in the future.

4. Investment treaty arbitration in the technology sector is still in its infancy but is a growing area

Technology companies rapidly disrupt existing industries through innovative products, services and business models, often operating in sectors that are unregulated or challenge existing regulatory frameworks. State responses may create tensions with those companies. Sometimes, state-enacted regulation can appear heavy-handed, arbitrary or discriminate in favour of local interests. Some examples of where measures impacting the technology sector may give rise to challenge are:

- AI and autonomous vehicle (AV) rollout
- Forced data localisation requirements¹²
- Intrusive cybersecurity requirements
- Disproportionate digital taxes¹³
- Censorship and blockages of digital platforms and content¹⁴
- Forced transfer of proprietary information, including source code¹⁵
- Outright nationalisation of companies

International investment law can protect against arbitrary, discriminatory and other unfair regulation or treatment by foreign governments and provide a direct right of action against foreign governments for resulting harm. States have entered more than 2,500 international investment treaties (including investment protection chapters in trade agreements) granting foreign investors legal rights under international law directly enforceable against states.¹⁶

Bilateral, or multilateral, investment treaties (BITs) signed between a host state (the country where the investment is made) and home state (the country of the investor's nationality) protect foreign investors and their investments by granting investors the right to bring a claim against host states before independent international arbitration tribunals. This means that investors may have a direct right of action against foreign governments, in a neutral forum, heard by independent arbitrators appointed by the disputing parties.

The resulting awards are generally enforceable as local court judgments, which may be enforced automatically under the ICSID Convention¹⁷ – if the states are party to the convention – and by formal “recognition” under the New York Convention for non-ICSID awards.¹⁸

The legal remedies that protect foreign investors under international investment law may not be available without advanced planning. Access depends on whether the foreign investor is from a home state that benefits from the protection of an investment treaty entered into with the host state of the investment.

An empirical analysis¹⁹ reveals that, to date, relatively few investment treaty claims have been brought by technology companies.²⁰ This may be due to several factors, not least the fact that technology companies generally prefer to settle disputes instead of litigating them.²¹ Yet, companies in extractive industries and infrastructure projects have relied on these rights for many years in disputes with governments.

As evinced in Annex 1, there are relatively few investment arbitrations that have been brought in the technology space and most of them do not so far concern new regulation. However, as technology companies grow in economic importance and governments increase their regulation of the tech sector, we predict that the number of technology-based investment treaty claims will rise in the years to come. There already appears to be some increase. In order to ensure they are protected by investment treaties, technology companies will need to overcome certain jurisdictional and admissibility challenges, as discussed in section 5 below.

Although we have focused primarily on international treaties as the foundation for claims under international investment law, it should be noted that such claims could also arise under domestic host state legislation aimed at promoting foreign investment, which will often provide for disputes thereunder to be resolved by international arbitration.

Despite the relatively few investment arbitrations that have been brought in the technology space, three main observations can be drawn from this empirical picture:

1. The cases that have been brought span a range of technology subsectors (from ride-hailing and domain management to cryptocurrency, 5G infrastructure and aerospace technology) suggesting that investment treaty arbitration is not confined to particular types of technology disputes.
2. The case review reveals a recurring pattern of state conduct – the withdrawal or nonrenewal of concession agreements, the imposition of bans or exclusions on national security grounds, and the initiation of regulatory or criminal proceedings that adversely affect the value of the investment.
3. Third, whilst several of the cases remain pending, those that have concluded have produced mixed results, illustrating that the outcome of these disputes is far from certain and will depend heavily on the specific facts and treaty language in play.

As technology companies grow in economic importance and governments increase their regulation of the tech sector, we predict that the number of technology-based investment treaty claims will rise in the years to come.

5. When will tech investments qualify as protected investments under investment treaties?

To bring a claim under an international investment agreement (IIA), the dispute must pass several jurisdictional hurdles. Two of these hurdles may present particular challenges for technology claims; namely, technology companies must have (i) an “investment” (ii) that is made in the territory of the host state covered by the treaty. This section explores these two jurisdictional points, referred to as *ratione materiae* and *ratione territorialis*, in the context of technology disputes.

Technology companies’ investments and *ratione materiae* jurisdiction

Is data a protected investment?

Perhaps the most significant question concerns whether data itself – particularly, user data collected and processed by digital platforms – constitutes a protected investment. Data has become one of the most valuable assets for many technology companies, driving advertising revenue, enabling algorithmic improvements, and creating network effects

that entrench market position. Yet, data presents unique challenges for investment law classification.

Unlike traditional intellectual property, data is not typically subject to exclusive ownership rights. Personal data, in particular, is increasingly recognised as subject to individual rights under data protection regimes, such as the European Union’s General Data Protection Regulation (GDPR). Moreover, data’s value often derives not from the raw information itself but from the analytical capabilities and network effects that surround it.

To date, no published investment treaty award has directly addressed whether data constitutes a protected investment. However, the conceptual framework exists for such recognition. Data could potentially qualify as:

1. Intellectual property, particularly when compiled into databases protected by sui generis database rights.
2. Business goodwill or know-how.
3. Contractual rights, where users have agreed to data collection and processing.
4. “Any other tangible or intangible property” under broad treaty definitions.

However, many jurisdictions do not recognise data as property. The GDPR treats personal data as subject to individual rights, not corporate property rights. This creates a fundamental challenge for claiming data is a protected investment. This is an important question because regulatory measures requiring data localisation, mandating data deletion or restricting cross-border data transfers could potentially constitute compensable expropriation or violations of FET standards. This possibility has already influenced regulatory debates, with some governments expressing concern that investment treaties may constrain their ability to regulate data flows and privacy.

A threshold question in any investment treaty claim is whether the claimant possesses a protected “investment” under the applicable treaty. Most investment treaties define “investment” through nonexhaustive lists. The challenge for technology investors lies in demonstrating that their characteristic assets – software, algorithms, data, user networks or platform infrastructure – fall within these definitions.

Investment treaties typically define the term “investment” broadly and extend it to both tangible assets as well as intangible rights. This will usually be wide enough to capture the kind of assets that tech companies possess in foreign jurisdictions around the world, including IP rights,²² financial instruments²³ and contractual rights.²⁴ Digital assets held by technology companies – including data, source code, software and computer systems – could therefore constitute covered investments under IIAs, although this remains untested in arbitral practice.²⁵

Where uncertainty exists regarding covered assets, tribunals tend to apply the interpretive framework set out in Article 31 of the Vienna Convention on the Law of Treaties, construing treaty terms according to their ordinary meaning in light of the treaty’s object and purpose.²⁶ The wording of the treaty will therefore be crucial. As noted, many IIAs provide broad nonexhaustive lists of the types of assets covered that are likely to extend to digital assets.²⁷ For example, the German Model BIT (2008) refers to investments as covering “every kind of asset”.²⁸ Another example is the Argentina-United States BIT which defines investments as including “inventions in all fields of human endeavor”.²⁹ In some cases, IIAs provide for a narrower or closed list of assets covered by the investment definition, which may pose greater difficulties for technology investors. For example, the Canada-Chile Free Trade Agreement, the Canada-Peru BIT and Mexico-China BIT all contain various forms of closed-list definitions of investment.³⁰

The *Salini* test and technology investments

In addition to assessing the definition of an investment under a treaty, investment tribunals constituted under the ICSID Convention will also evaluate if a given investment complies with the requirements of the Convention’s Article 25. Under Article 25’s test – referred to as the *Salini* test³¹ – an investment should include:³²

1. The contribution of money/assets.
2. The presence of risk.
3. A long duration.
4. A contribution to the host state’s economy.

Many digital assets will likely satisfy these criteria. For example, a technology company’s establishment of data centres, development of local user networks and multiyear service contracts would demonstrate contribution, risk and duration. However, each case requires individual assessment based on

the specific investment structure.

Further, given tribunals' generally expansive reading of the scope of investments, the ICSID requirements are likely to be fulfilled by investors in businesses which involve cross-border data flows and other digital assets.³³ Tribunals have frequently adopted a holistic approach, where they consider a transaction as a whole to be an investment, even if no individual part of the transaction would qualify as an investment.³⁴

Alternatively, if an investor were to bring a claim before a non-ICSID tribunal, it should not need to meet the requirements of the Salini test. However, even in this setting, tribunals have tended to apply some criteria to establishing an "investment" in addition to the strict wording of the treaty. In particular, non-ICSID tribunals have constructed a three-prong test based on Salini, requiring contribution, duration and risk.³⁵ The exclusion of the requirement for a "contribution to the host state's economy" arguably makes it easier for an asset to qualify as an investment outside of the ICSID framework.

Jurisdiction *ratione territorialis* and technology companies

Additionally, investment treaties typically require that the investment be made in the territory of the host state jurisdiction (see, for example, an extract of the US-Rwanda BIT (2008) below) – a requirement that can pose challenges for digital businesses which operate across borders through cloud infrastructure, distributed networks and remote service delivery.

Treaty Between the Government of the United States of America and the Government of the Republic of Rwanda Concerning the Encouragement and Reciprocal Protection of Investment 2008

Article 1. "Covered investment" means, with respect to a party, an investment in its territory of an investor of the other party in existence as of the date of entry into force of this treaty or established, acquired or expanded thereafter.

"Investment" means every asset that an investor owns or controls, directly or indirectly, that has the characteristics of an investment, including such characteristics as the commitment of capital or other resources, the expectation of gain or profit, or the assumption of risk. Forms that an investment may take include:

- (a) An enterprise
- (b) Shares, stock and other forms of equity participation in an enterprise
- (c) Bonds, debentures other debt instruments and loans
- (d) Futures, options and other derivatives
- (e) Turnkey, construction, management, production, concession, revenue sharing and other similar contracts
- (f) Intellectual property rights
- (g) Licences, authorisations, permits and similar rights conferred pursuant to domestic law
- (h) Other tangible or intangible, movable or immovable property, and related property rights, such as leases, mortgages, liens and pledges

Consider a social media platform operated by a company incorporated in state A, with servers located in state B, users primarily in state C and advertising revenue derived from state D. Where is the "investment" located for treaty purposes? (See image below for a representation of this type of investment.) This question has significant practical implications, as it determines which state's regulatory measures may be challenged and which treaties may be invoked.

Investment tribunals have not been uniform in their treatment of the territorial nexus question:

- In *Bayview Irrigation District v. Mexico (U.S. v. Mex)*, the tribunal held that the North American Free Trade Agreement (NAFTA) was "not intended to provide substantive protections or rights of action to investors whose investments are wholly confined to their own national States, in circumstances where those investments may be affected by measures taken by another NAFTA State Party".³⁶
- In *Apotex Inc v. United States of America*, the tribunal held that preparatory work completed in Canada to comply with US pharmaceutical regulations for the sale of products in the US was not considered an investment in the US.³⁷ The tribunal found that the products were produced in Canada, and that the export to the US was merely cross-border trade.³⁸
- In *SGS Société Générale de Surveillance SA v. Republic of the Philippines*, the existence of a "liaison office" in the host state which employed several people and coordinated much of the claimant's operations was considered sufficient connection with the host state, even though the majority of the services were provided outside of the host state.³⁹
- In *LESI v. Algeria*, the tribunal held that an investment need not be entirely made in the host state, "[n]othing prevents investments from being committed, in part at least, from the contractor's home country, as long as they are allocated to the project to be carried out abroad".⁴⁰ This reasoning suggests that although digital asset investments may have a less evident physical presence in a host state than traditional investments, this is not decisive under IIAs; the key question is whether a sufficient functional nexus to the host state can be established.
- In *European Media Ventures SA v. Czech Republic*, the tribunal held that a contract between a foreign investor and a local Czech television station constituted an investment in the territory of the Czech Republic. The tribunal held that, because the contractual right related to an intended transfer by a Czech individual of a licence to broadcast within the

territory of the state, the contract was “firmly anchored within the territory of the Czech State”.⁴¹ This ruling could be used to support an argument that, although not technically physically located in the territory of the host state, tech companies’ investments fulfil the territorial requirements under investment treaties where they clearly concern matters within the host state.

- In *Société Générale v. Dominican Republic*, the tribunal held that loans extended by a French bank to Dominican borrowers constituted investments “in the territory” of the Dominican Republic, even though the funds were disbursed from France. The tribunal emphasised the economic impact and legal relationships within the host state rather than the physical location of assets.

As shown by these different interpretations, whether a territorial nexus is established is a deeply factual question which will be determined on a case-by-case basis. Indeed, the common thread is that arbitral practice shows that tribunals adopt a flexible, multifactor approach to territorial nexus.

Applied to technology investments, this approach suggests that territorial nexus may be established through:

- Local subsidiaries or branch offices
- Servers or data centres located in the host state
- Local user bases or customers
- Revenue derived from the host state
- Intellectual property registered in the host state
- Contractual relationships with host state entities

The presence of any substantial business operations or economic impact within the host state likely suffices to establish territorial nexus. However, technology companies often operate their businesses over the internet and across multiple jurisdictions. If they do not have any form of physical operations or offices in the states in which they operate, the risk is that a technology company may be viewed as a trader, rather than an investor.

As more IIAs with expansive interpretations of the meaning of “investment” are agreed, and as more tech disputes come before international arbitral tribunals, arbitral tribunals are likely to seek to accommodate the types of investments made by technology companies recognising the changing nature of international commerce in a digital world.

The analysis in this section reveals that whilst technology companies face genuine and novel jurisdictional challenges, these are not insurmountable.

Regarding the *ratione materiae* challenge, investment treaties have historically been drafted in broad and nonexhaustive terms, and arbitral tribunals have consistently demonstrated a willingness to apply those broad terms to new commercial realities. Digital assets are thus capable of falling within the definition of “investment” under most modern IIAs, even if this remains largely untested in arbitral practice. The most significant open question is whether data itself, and in particular, user data, constitutes a protected investment given that many jurisdictions do not recognise data as property.

On the question of *ratione territorialis*, the delocalised nature of technology businesses means that establishing a sufficient territorial nexus with the host state will require careful analysis on a case-by-case basis. Arbitral practice suggests that tribunals adopt a flexible, multifactor approach – the presence of a local subsidiary, servers or data centres, a local user base and revenue derived from the host state, or contractual relationships with host state entities may each, individually or collectively, suffice to establish the requisite nexus. The risk, however, is that a technology company operating purely over the internet, without any form of local presence, may not be characterised as an investor.

6. Substantive investment claims that technology companies could bring against states

IAs require countries to observe enforceable standards of conduct with respect to foreign investors and investments, which might include fair and equitable treatment (FET), national treatment, full protection and security, no direct or indirect expropriation without compensation, and no requirement to transfer technology as a condition of investment.

Fair and equitable treatment

Most IAs include the standard of FET. State measures that commonly give rise to a violation of the FET standard include:

- Arbitrary and discriminatory treatment, which relates to conduct by the host state that results in unequal treatment in like circumstances without any justified motive.⁴²
- Denial of due process, which relates to “legitimate and reasonable expectations” on which the investor relied, including “the stability of the Host State’s legal framework”, and is breached when “the State’s judicial system ... is responsible for a denial of justice which affects the investment”.⁴³
- Unjust enrichment, which requires there to be “an enrichment of one party to the detriment of the other”, with “no justification for the enrichment, and no contractual or other remedy available to the injured party whereby he might seek compensation from the party enriched”.⁴⁴
- Frustration of investors’ legitimate expectations, “a situation where a Contracting Party’s conduct creates reasonable and justifiable expectations on the part of an investor (or investment) to act on reliance on said conduct, such that a failure by the [State] to honour those expectations could cause the investor (or the investment) to suffer damages”.⁴⁵

Various tribunals have held that the concept of legitimate expectations has “generally been considered central in the definition of the FET standard, whatever its scope”. A state may therefore breach FET if it goes against expectations created by representations made to an investor regarding any specific investment stage or matter.

FET may also be applicable to procedural matters, including the manner in which states have passed new laws or how they have taken executive action. FET therefore includes considerations of transparency, due process, nondiscrimination and good faith. Tribunals have, however, recognised that no investor may reasonably expect that the circumstances prevailing at the time of the investment will necessarily remain totally unchanged. There must be a reasonable expectation of regulation. How broadly FET provisions apply to a claim will depend on the wording of the FET provision in the relevant investment agreement.

For technology investors, sudden bans or restrictions on platform operations after initial licensing, opaque or contradictory enforcement of content or competition rules, or retroactive liability under new cybersecurity or data laws could, for example, create FET claims. Some examples of these claims have been brought by Uber against Colombia, where Colombia decided to prohibit ride-hailing activities.

FET – with different wordings and formulations – is included in almost 95% of investment treaties; however, whether technology investors can run FET-style arguments depends on the specific language of the treaty that they are bringing their claim under. For example, in the *Couparang* dispute, US investors have threatened to bring a claim against Korea on grounds of discriminatory treatment under the US-Korea Free Trade Agreement. The agreement does not set out an autonomous FET standard, but it expressly ties FET to the customary international law minimum standard of treatment. Therefore, any challenge brought by investors would need to be framed within that narrower minimum standard rather than a broad FET guarantee. The factual circumstances which could form the basis of FET claims do not always have to be brought under stand-alone FET provisions; sometimes such arguments will be structured to fit the language of the relevant treaty.

National treatment and most-favoured nation treatment

Investment treaties typically include national treatment and most-favoured nation (MFN) treatment obligations, requiring that foreign investors receive treatment no less favourable than that accorded to domestic investors or investors from third countries. These provisions prohibit both de jure discrimination (explicit differential treatment based on nationality) and de facto discrimination (superficially neutral measures that disproportionately burden foreign investors).

The national treatment standard aims to ensure that foreign investors are treated no less favourably than a host state’s national investors in “like circumstances”. Therefore, states should not take any discriminatory measure which benefits local investors to the detriment of the foreign investor. For example, in *SD Myers v. Canada*, the tribunal held that a policy adopted by Canada to favour a local investor for protectionist reasons constituted a breach of national treatment under NAFTA.

If a state were to adopt a policy against a foreign-based technology company to protect a national company or industry, this could potentially give rise to a national treatment claim. This is exemplified by the *United Group and others v. Serbia* case, where the claimant, a Dutch-registered TV and broadband provider, alleged it was subjected to discriminatory treatment from state authorities favouring a local competitor in breach of the Netherlands-Serbia BIT.

Protectionist behaviour of states against overseas technology companies is a real and present concern. However, technology companies would have to pass the “like circumstances” test, which is not always straightforward since the nature of

technology is that it is often disruptive and novel. Domestic and foreign platforms will often offer different services, target different user bases or employ different business models.

Nevertheless, in an international political environment where nationalism and protectionism are on the rise, national treatment protections may prove particularly important.

Full protection and security

The full protection and security (FPS) standard requires the host state not to directly harm investors or investments through acts attributable to the state and to protect investments against actions of private parties or inactions of the host state. This could include protecting investors and their employees and equipment against physical attacks and harassment by the state or state actors, and potentially against radical change to local laws or cybersecurity attacks.

Although the FPS standard could easily apply to the protection of technology companies' physical assets, such as data centres, more novel applications might concern the protection of digital assets, such as websites, computer systems or proprietary information. For example, cyberattacks or theft in the digital domain could constitute actions against which the host state is deemed to have an actionable duty to protect, or at least not to promote or knowingly acquiesce.

The FPS standard has particular resonance for technology companies, whose most valuable assets are often intangible and whose operations are inherently vulnerable to state-sanctioned or state-tolerated interference in novel forms. For example, in the cybersecurity context, where a host state fails to take reasonable measures to prevent or respond to a cyberattack on a foreign technology company's infrastructure – or where state actors are themselves implicated in such an attack – a breach of the FPS standard could arise.

No direct or indirect expropriation without full compensation

Expropriation is the unlawful taking of property by a host state belonging to a foreign investor. Protection against expropriation is included in virtually all IIAs. Expropriation may be direct (which is the mandatory legal transfer of the property's title or, less commonly, its outright seizure by the host state), or it may be indirect (in which case the property may be destroyed or the investor is otherwise deprived of its ability to manage, use or control the property in a meaningful way, without the legal title being affected).

This standard of protection requires that the host state may not forcibly appropriate the tangible or intangible property of foreign investors by means of administrative or legislative action, or may not thereby deprive an investment of its economic use.⁵⁶ Under the standard, a foreign investor can expect the state to pay fair market value for property or compensation where state regulation unfairly destroys the value of an investment.

A straightforward example of direct expropriation is *Mr. Franz Sedelmayer v. Russia*, in which the tribunal held that Russia had expropriated a joint venture's long-term right to use a building by means of a presidential decree that ordered the transfer of the property to a government procurement department.⁵⁷ On the other hand, cases of indirect expropriation tend to be more intricate. For example, the tribunal in *OOO Manolium Processing v. The Republic of Belarus* held that Belarus indirectly expropriated the investor's investment through the adoption of unlawful taxation and enforcement measures that resulted in the confiscation of a partially completed construction project.⁵⁸

In the context of technology companies, expropriation could take place in many ways. One potential scenario is an investor affected by a state restriction on data transfer arguing that the restriction constitutes an indirect expropriation. Commonly, case law has found that a "substantial deprivation" of the investment will amount to an expropriation. This might well apply if the impact of the restriction is fundamental, but the proportionality of the measure and the investor's reasonable expectations may also be relevant considerations. For example, a state measure that is proportional to protect the environment, public health or other core regulatory area of the state may not amount to an indirect expropriation, but rather, it is permitted under the state's regulatory powers. We anticipate that the proportionality of state measures that impact technology companies, purportedly taken in the public interest, is likely to become an important battleground.

No requirement to transfer technology as a condition of investment

So-called performance requirements are measures that require investors to behave in a particular way, including requiring investors to "meet certain specified goals with respect to their operations in the host country".⁵⁹ As each state has the right to determine its own conditions for investment, performance requirements are not specifically prohibited under the majority of BITs. However, in several recent trade agreements, performance requirements have been prohibited or, at least, restricted to protect investors. For example, the draft EU-China Comprehensive Agreement on Investment prohibits certain types of performance requirements.⁶⁰ These include, amongst others, prohibitions on imposing or enforcing any requirement or undertaking to:

- "[P]urchase, use or accord a preference to goods produced or services provided in its territory, or to purchase goods or services from natural persons or enterprises in its territory".
- "[T]ransfer technology, a production process, or other proprietary knowledge to a natural person or an enterprise in its territory".
- "[U]se or favour technology that is owned by or licensed to a natural person or an enterprise of the Party" in connection with the establishment or operation of enterprises in a party's territory.⁶¹

Another example is Article 14.10 of the United States-Mexico-Canada Agreement which requires contracting parties not to impose or enforce any undertaking “to purchase, use or accord a preference to a good produced or a service supplied in its territory”.

The prohibition on performance requirements has particularly acute relevance for technology companies, whose most commercially sensitive assets (like their source code, proprietary algorithms, training datasets and AI architectures) represent the very core of the company’s value. A state that conditions market access on the disclosure or transfer of these assets effectively compels a technology company to surrender the intellectual property upon which its entire business model depends. Just to give two examples of cases where this treaty protection might be engaged:

1. A state requires a foreign AI company seeking to operate to provide local authorities with access to its underlying algorithm or models as a condition of regulatory approval. Even if framed as a cybersecurity or transparency requirement, such a condition might constitute a prohibited performance requirement under a relevant trade agreement, as it would compel the transfer of proprietary knowledge to an enterprise or authority within the territory of the host state.
2. A host state that mandates use of a state-owned or domestically developed AI system may similarly breach performance requirement prohibitions where those obligations are incorporated into the applicable treaty framework.

As the competition between states to develop sovereign technology capabilities intensifies, performance requirements of this kind are likely to become an increasingly common and contested feature of the technology investment landscape.

Table 2 – Summary of key substantive claims that may be brought by technology companies

PROTECTION	KEY FEATURES	RELEVANCE TO TECH
Fair and equitable treatment (FET)	Covers arbitrary/discriminatory treatment, denial of due process, frustration of legitimate expectations	Sudden platform bans after licensing; opaque enforcement of content or competition rules; retroactive liability under new data laws
National and MFN treatment	Foreign investors must receive treatment no less favourable than domestic investors or third-country investors	Policies favouring domestic tech companies over foreign competitors; protectionist digital regulation
Expropriation	May be direct (seizure of property) or indirect (substantial deprivation of use, management or control without transfer of title)	Data transfer restrictions; censorship measures substantially depriving platforms of economic benefit; blocking of market access and consumer reach
Performance requirements	Not specifically prohibited under most BITs, but restricted under several modern trade agreements	Forced disclosure of source code or proprietary algorithms or the handover of technology as a condition of market access

7. The impact of states' regulatory powers and defences

Notwithstanding the protections afforded by investment treaties, sovereign states retain inherent regulatory powers in the public interest, a principle recognised under customary international law.⁶² Where such right is exercised in a nondiscriminatory manner, and the measure is adopted in accordance with the rules of good faith and due process, it constitutes a lawful act which is not in breach of international investment law even if it affects investors' rights.⁶³

States may therefore regulate on the basis of, for example, the protection of the environment, public health, human rights, national security and the protection of citizens' lives. It should be noted, however, that these bases cannot be used merely as a pretext to disguise other illegitimate motives behind regulation.

Another key avenue of defence for states is the existence of exception clauses within IIAs.⁶⁴ These clauses usually make provision for circumstances under which states are not precluded from adopting or enforcing certain measures. This preserves their regulatory powers within certain designated policy areas like national security.⁶⁵ IIA jurisprudence has, however, generally construed express exceptions clauses narrowly.⁶⁶ Although these clauses may turn out to be particularly relevant since they include "national security" as a key carved-out area, their applicability to a particular case will depend on the wording of the treaty.

Finally, even if found to be in breach of an IIA, states can still rely on circumstances precluding wrongfulness to justify the breach of any given treaty provision. One of those defences is "state of necessity", whereby a host state may claim that certain acts or measures, that would have otherwise constituted a breach of IIA provisions, were justified on the grounds that they were the only way of safeguarding an essential interest. This ground is, however, only available in exceptional circumstances where the host state can establish:

- The existence of a grave and imminent peril that threatens an essential interest.
- That the state's act is the only way to safeguard that interest.
- That the state's act does not seriously impair another essential interest.⁶⁷

In investment treaty arbitrations, the threshold of necessity has been a high hurdle for state parties to overcome. However, tribunals have accepted the defence in certain circumstances. For example, one tribunal accepted the necessity defence in a case where economic peril was considered to be an essential interest.⁶⁸

Technology regulation frequently invokes public interest justifications, including protection of privacy, national security, consumer protection and competition preservation. A state may, for example, seek to restrict or censor a social media company from operating on the basis of national security or the protection of the lives of citizens, where it is believed to have been used for the purpose of terrorist activity. This would be considered a legitimate exercise of regulatory power where it is proportionate and adopted in good faith and in accordance with due process.

Similarly, a state may justify a regulation to force the transfer of technology to its territory on grounds of national security, where it is concerned that such technology poses a legitimate threat to its peace and security. Again, this may constitute a legitimate exercise of regulatory power if exercised in the appropriate manner.

Whether the state has legitimately exercised its regulatory powers, will require a case-by-case analysis of the facts and the motivations of the state for adopting a given measure. It tends to focus on a review of the fairness of the process rather than a substantive review of the results. The nature of new technology and the emerging risks it may entail mean there is likely to be considerable scope for argument around whether attempts to tackle or curtail perceived adverse impacts in the public interest are legitimate or represent actionable state overreach.

The recent dispute involving Nexperia, a Chinese-owned semiconductor firm, exemplifies this tension. The company is threatening a US\$8 billion investment treaty claim against the Netherlands after the Dutch ministry of economic affairs issued an emergency order blocking the company's operations on national security grounds. The ministry cited "serious governance shortcomings"⁶⁹ at Nexperia and the need to protect "crucial technological knowledge and capabilities"⁷⁰ in Europe. This case illustrates how efforts to regulate sensitive and strategically significant technologies can quickly give rise to disputes over whether a state is acting legitimately or has crossed the line into actionable overreach.

The defences available to states under international investment law have particular relevance in the context of technology regulation, where the pace of legislative and regulatory action has frequently outstripped the development of clear legal standards. As described above, there are three main defences that might be available to states.

First, the police powers doctrine is likely to be invoked frequently by states seeking to justify regulatory action against technology companies on grounds of national security. The Nexperia example, discussed above, illustrates how swiftly a state may invoke national security concerns to justify intervention in a technology investment, and how contested the line between legitimate regulation and actionable overreach can be.

Second, exception clauses in IIAs (like nonprecluded measures clauses) are likely to be central to technology disputes involving content regulation, data protection and cybersecurity. A state that blocks a foreign social media platform on grounds of public order, or imposes data localisation requirements citing national security, will typically seek to rely on an express exception clause in the applicable treaty. Whether such a clause affords protection will depend critically on its drafting and interpretation by tribunals (i.e. whether it is self-judging – allowing the state itself to determine whether the measure falls within the exception – or subject to review by the tribunal). Technology companies facing such measures should therefore examine the precise terms of the applicable exception clause at the outset, as this will determine the scope of the state’s regulatory space and the viability of any claim.

Finally, the state of necessity defence is unlikely to provide a reliable shelter for states seeking to justify technology regulation, given the high threshold that must be met. The requirement that the state’s act be the only means of safeguarding an essential interest will be difficult to establish in most regulatory contexts, where less restrictive alternatives are typically available.

8. Case studies of potential areas where technology companies may bring investment-treaty claims against states

As the level of regulation by governments in the tech sector expands, an increasing number of technology companies are likely to face issues stemming from state regulatory action. Recent examples include requirements for companies to localise their data infrastructures in particular jurisdictions, censorship of content online, restrictions on social media and certain forced compensation schemes. Such situations could give rise to legitimate investment treaty claims, and we explore some of those cases below.

Data localisation

Data localisation refers to mandatory legal or administrative requirements that data be stored and processed within a specified jurisdiction. Such requirements may be absolute (prohibiting any offshore storage or processing) or conditional (permitting offshore transfers subject to certain safeguards).⁷¹ In countries that have implemented strict data localisation laws, companies will be required to establish local data storage facilities for all data sourced within that jurisdiction.⁷² Data localisation laws can therefore present a number of operational challenges to technology companies, as they can restrict the transfer of data for everyday business purposes, including to support server backups, use of cloud-based services, engagement of nonlocal suppliers or vendors, and sharing data across other corporate offices and entities.⁷³

Recently, more states have enacted data localisation legislation. Countries with stricter data localisation laws include Vietnam, Indonesia, Brunei, Iran, China, Brazil, Australia, South Korea, Russia and Nigeria.⁷⁴ The key common justifications for the enforcement of such laws are the increased level of security and the economic benefits that may be derived from such requirements.

Some of the key developments in different jurisdictions are summarised below:

- In 2021, China introduced a new Data Security Law which requires critical information infrastructure operators to comply with data localisation practices. This means that personal information and important data gathered and produced during operations must be stored within Chinese territory.⁷⁵
- In Russia, since September 2015, all data controllers that collect and process the personal data of Russian citizens are required by law to store this data on servers located in the country. In November 2016, a Russian court upheld the decision of an earlier court to block online access to LinkedIn due to its breach of data localisation laws.⁷⁶ Fines were also introduced in December 2019, whereby the first violation of localisation requirements results in a fine of up to US\$77,000, and any subsequent violations result in fines of up to US\$231,000.⁷⁷ In August 2021, Facebook, Twitter and WhatsApp were fined for failing to localise storage of the personal data of their users in Russia.⁷⁸ Facebook has received previous nominal fines for violating Russian data localisation laws.⁷⁹
- In 2018, the Reserve Bank of India issued a directive requiring all companies to store payments systems-related data in the country.⁸⁰ A new Personal Data Protection Bill is also currently being considered which requires all “sensitive personal data” and “critical personal data” to be stored in India.⁸¹ This is a relaxation of the version of the bill reviewed in 2018, which incorporated blanket provisions on data localisation.
- In 2012, the Australian government enacted the My Health Records Act 2012, which requires personal health records to be stored only in Australia. The Electronic Conveyance National Law, as implemented in each state’s and territory’s domestic law and operating requirements, also contains data localisation requirements – for example, requiring cloud service providers to store land information within a secure computer infrastructure in Australia.
- Canada has enacted a number of data localisation laws at the federal and provincial level. These laws include requirements to localise banking data, credit associations’ data, insurance data, and trust and loan companies’ records in Canada.
- Some countries in Europe have also adopted data localisation laws:
 - In France, the Defence Code requires that any data held by essential service providers is required to be localised in the country. Under the Heritage Code, the transfer of any materials classified as government archives outside of France is prohibited.
 - The German Telecommunication Code requires telecommunications service providers to store communications traffic data in Germany for a specified time. In Germany, there are also data localisation requirements with regard to accounting and tax data, employment data and housing subsidy data.

Data localisation regulations have become particularly relevant in the construction of data centres which provide critical infrastructure for large-scale compute and data storage, which is fundamental to the advancement of AI. This is big business. In 2024, the global data centre market was valued at \$242.72 billion, and it is projected to increase to \$584.86 billion by 2032.⁸³ Data centres are directly impacted by data localisation requirements as they are built to store, process and transfer data across borders. Notably, Big Tech companies build or lease data centres abroad, which would qualify as “investments” under most BITS and are likely protected under applicable investment treaties.

States often frame data localisation laws as a means of responding to the rapid growth of the internet, which has enabled vast volumes of data to move across borders beyond effective territorial control. Data localisation is therefore introduced as a means of reinforcing regulatory oversight. Other considerations include safeguarding national security and law enforcement requirements, consumer data privacy, economic benefits to local businesses and digital sovereignty.

As noted above, each state has the right to regulate proportionately for proper purposes, and the fact of new regulation by itself would not constitute a breach of international investment law – much more so when there are legitimate reasons to adopt data localisation laws in certain domains. The key issue is the extent to which the implementation of data localisation requirements may be considered abusive because, for example, they further no legitimate aim or are discriminatory. Such cases could constitute breaches of protection standards under international investment law, as analysed below.

Fair and equitable treatment

Measures taken against technology companies in connection with data localisation could constitute a breach of FET. For example, in 2016, the Turkish government refused to grant a payments licence for an online payments provider due to its failure to comply with stringent requirements to localise information technology systems in the country. Such stringent requirements were unfeasible for this online payment services provider, which operates a global digital money platform and cannot maintain local payment platforms with technology infrastructure in each single country. Consequently, this online payment services provider might have brought an investment treaty claim against Turkey under the FET standard for a sudden change in the regulatory environment which caused the company to leave the country.

Similarly in Russia, in July 2021, a court in Moscow issued a three-million Russian rubles (approximately US\$41,100) fine against Google for violating Russia’s new data protection law, which came into force on 1 July 2021 and required the storage of personal data of Russian users on servers in Russia. This law, which was adopted speedily and is applicable only to foreign companies, gave the government widespread powers to control the activities of foreign internet providers and could be considered to breach FET provisions. Such laws that are applicable only to foreign companies may arguably also breach national treatment clauses in investment treaties.

Performance requirements

In *Mobil and Murphy v. Canada (I)*,⁹¹ the Canada-Newfoundland and Labrador Offshore Petroleum Board implemented guidelines requiring operators of offshore petroleum projects to contribute a percentage of their revenue to research and development in the province. Those guidelines were held to be inconsistent with the performance requirements provisions of NAFTA, amounting to a breach of Article 1106(1)(c), which prohibits requirements “to purchase, use or accord a preference to goods produced or services provided in its territory, or to purchase goods or services from persons in its territory”. The implementation of the guidelines would, in practice, require local expenditure.⁹²

By analogy, this reasoning could apply to data localisation, where companies are forced to spend money in a host country on local technology infrastructure as a condition of business. Enforcing data localisation in this way might therefore infringe similar performance requirements provisions.

Indirect expropriation

Some state measures concerning data transfers could be sufficient to amount to expropriation since they interfere with investors’ ownership interests and the returns arising out of their investments. However, the availability of an indirect expropriation claim will depend on the level of interference with the investors’ rights, which would need to be substantial.

For example, a technology company with a business model based upon data processing that it conducts overseas (in a central hub) might be very significantly impacted by the implementation of new regulation requiring such processing to be conducted exclusively within the host state. It might be argued that the effect of such regulation is equivalent to expropriation, as the company can no longer operate its business or, at least, realise any meaningful return on its investment.

Online censorship

Online censorship is the control or restriction of what can be accessed, published or viewed on the internet, which may be carried out by governments, regulators or private organisations at the behest of governments or regulators.⁹³

Censorship of online content by governments around the world has increased year on year for the past 15 years.⁹⁴ This has included governments seeking to impose restrictions on large technology companies and regulating online content for political purposes.

In 2020, technology, media and telecommunications companies objected to censorship laws in several countries, including Australia, Burma, China, Colombia, Germany, Hong Kong, India, Mexico, Pakistan, Russia, Singapore, Thailand and Turkey.⁹⁵

Examples of measures to block or censor social media companies and other online platforms

- In 2022, Turkey introduced its “disinformation law”, criminalising “publicly and knowingly spreading false information about Turkey’s internal and external security, public order and state welfare”⁹⁶ which carries one to three years of imprisonment. In September 2025, Turkey enforced temporary blockages preventing access to social media platforms, including X, Facebook and WhatsApp.⁹⁷
- LinkedIn has been banned in Russia since 2016,⁹⁸ and Facebook and Instagram were banned in 2022, after the government designated Meta as an extremist organisation.⁹⁹ On 4 December 2025, Russian authorities blocked access to Snapchat and also recently placed restrictions on use of Apple’s FaceTime.¹⁰⁰
- In April 2019, Sri Lanka blocked access to several social media sites, including Facebook, Instagram and WhatsApp, following terrorist attacks, citing concerns over the spread of misinformation that could lead to further violence.¹⁰¹
- In India, guidelines were issued in February 2021 by the Ministry of Electronics and Information Technology requiring large social media platforms to, among other things, follow additional due diligence rules and remove any content flagged by authorities within 36 hours.¹⁰² WhatsApp filed a lawsuit against the Indian government seeking to block the new regulations, as they require social media companies to identify the first originator of information when demanded by the authorities.¹⁰³

As with data localisation, states are largely free to exercise their regulatory rights and enforce domestic laws. The problem arises when the exercise of state regulatory action is premised upon persecuting dissenting online opinions or arbitrarily affecting technology companies’ rights. This is where technology companies could articulate claims under IIAs.

Fair and equitable treatment

Social media and digital platforms may be able to challenge online censorship under the FET standard if such measures are considered excessively onerous or unreasonable and thereby restrict the legitimate enjoyment of their investments. A stable legal and business framework in a host state has frequently been found to be an essential element of FET.¹⁰⁴ Such claims could therefore arise from the introduction of new laws.

Indirect expropriation

As noted above, most IIAs protect against expropriatory conduct. Expropriatory conduct is conduct that is undertaken not for a public purpose, or in accordance with due process, and that is discriminatory. Expropriatory conduct is also not always limited to the taking of property but has been understood to include interference with the use or benefit of the investment in question.¹⁰⁵ To establish indirect expropriation, tribunals have developed a test requiring “intensity” and “duration”.¹⁰⁶

Social media or digital platforms could satisfy the first criterion where the censorship measures mean that they are substantially deprived of their investment, i.e. the state measure interferes with the “use or reasonably-to-be expected economic benefit” of the investment.¹⁰⁷ Given that social media and digital platforms rely heavily on advertisements and promotions for revenue, if they are blocked in a jurisdiction, it could be argued that this amounts to a substantial interference with the economic benefit derived from the investment because companies will cease to advertise with them.

Moreover, blocking access to consumer markets,¹⁰⁸ including social media users, may constitute expropriation, as it would significantly hinder the foreign investors’ ability to access users and derive any economic benefit from the data that they produce. Blocking digital platforms also deprives them of their rights to their domain names, which could constitute an asset susceptible to expropriation.

The requirement of duration (i.e. that the expropriation has necessary permanence) may be fulfilled by blockage of a social media or digital platform, provided that the measure is more than “merely ephemeral”.¹⁰⁹ A blockage for a defined and limited period, such as the weeklong blockage of several social media sites in Sri Lanka (see above), may not meet the threshold. However, there may be a claim for expropriation where digital platforms are prevented from resuming their activities within a host state or are blocked for a prolonged period without any apparent public purpose.

Forced compensation schemes

Another method of clawing back profits from technology companies is through forced transfers of wealth, which might contravene states’ obligations to foreign investors under IIAs. An example is the recent trend in requiring large technology companies and digital platforms to pay news publishers for their content. Governments across the globe have increasingly looked to compel technology companies and online platforms to bargain and negotiate payment deals with local publishers, aiming to transfer wealth to their jurisdiction.

Today, governments are also exploring the introduction of mandatory compensation schemes concerning the use of news publishers’ content by generative AI tools. The use of generative AI to access news without entering the official site of the publisher has doubled over the past year and looks set to increase with the public’s increasing use of generative AI (which has gone from 18% to 34% over the past year).¹¹⁰

Further, news publishers globally are bringing cases against AI companies over the unauthorised use of their content.¹¹¹ For example, earlier this year, Yomiuri Shimbun, Japan's leading newspaper company, filed a lawsuit against Perplexity AI alleging that the AI startup used its articles and images without permission.¹¹² Similarly, Folha, Brazil's largest newspaper, filed a lawsuit against OpenAI in São Paulo alleging that ChatGPT collected and used its content without permission or compensation.

At the same time, AI companies are making commercial licensing deals with news publishers whereby they will provide compensation for the use and integration of the publisher's content in their AI tools. For example, Meta recently entered into AI data agreements with news publishers including USA Today and Le Monde, giving the company permission to integrate their content into AI chat tools.¹¹³

Against the backdrop of ongoing disputes and negotiated agreements between AI companies and news publishers, states are considering legislating on compensation and licensing mechanisms. Applying the same rationale as applied in the Australia Code example, the introduction of state-enforced compensation schemes for news publishers against AI companies may lead to investment treaty disputes between foreign technology investors and host states.

Regulation of AI and other disruptive technologies

Disruptive technologies are novel products or business models that significantly challenge established industries and markets or establish new ones. Generally, the pace at which AI regulation has been considered and implemented by governments has not kept up with its rapid advancement, which has resulted in regulation gaps globally. Disruptive technologies are often initially deployed in permissive regulatory markets. Where those markets are subsequently restricted by the host state, this can have a sudden devaluing impact, and foreign investors may look to IIAs for redress.

At the heart of the legal debate will be the question of whether the regulations in question were implemented to address legitimate state concerns proportionately or whether regulatory powers are being used to protect local incumbents and treat foreign companies unfairly. The contrasting approaches to regulating disruptive technologies are evident in the field of AI. While the US and China – both global leaders in AI development – have generally adopted more flexible, innovation-driven regulatory strategies, the European Union has prioritised risk mitigation.

Similar trends emerged in the context of national security investment screening with regard to advanced technologies. In 2024, 21 out of 27 EU member states had domestic laws or mechanisms in place to screen and review foreign investments.¹¹⁴ The case *Huawei Technologies Co., Ltd. v. Sweden (2021)* illustrates how differing national approaches to regulating emerging and high-risk technologies, such as 5G telecommunications infrastructure, can lead to investment treaty-based arbitration under BITs between EU member states and China.

Even if new investment cases are launched by technology companies, tribunals may recognise that states retain regulatory discretion to limit or prohibit disruptive technologies on legitimate grounds. For instance, a state could adopt restrictive regulations that apply to AI, robotics or autonomous vehicle companies if these technologies pose a threat to environmental protection, national security or the lives of its citizens. This could be the case where there are untested risks, or where further investigation would be required before wider deployment of such technologies could be permitted.

For example, authorities in Denmark launched an investigation into a potential cybersecurity vulnerability, as it was found that its 262 Chinese Yutong buses, which are equipped with internet access, sensors, cameras and microphones, could be accessed by the manufacturer remotely.¹¹⁵ Similar concerns have been raised in relation to Neo, a disruptive humanoid robot, currently being rolled out in volunteers' homes in the US. The product promises to be a fully autonomous companion, but many activities carried out by Neo require the activation of "expert mode", which uses a human-in-the-loop system.¹¹⁶ In turn, Neo raises significant privacy and data collection concerns. In these contexts, investor-state claims would be unlikely to succeed due to legitimate bases for national regulation of new technologies and a state's right to protect its citizens.

In contrast, where states adopt regulatory measures that restrict a foreign disruptive technology in favour of domestic competitors, there is clear scope for an investment treaty arbitration claim. Sudden arbitrary or retroactive restrictions may also amount to a breach of the FET standard or an indirect expropriation.

The position of large ecommerce platforms, such as Alibaba or Mercado Libre, illustrates the circumstances in which a foreign investor – or broader market disruptor – may challenge such measures. As foreign digital commerce operators, these platforms may encounter restrictions aimed at shielding domestic businesses. Such measures may include limitations on cross-border data flows, discriminatory licensing requirements, exclusion from government digital payment systems, constraints on warehouse or logistics operations, or selectively applied competition or consumer protection enforcement.

Where measures of this nature appear discriminatory, arbitrary or protectionist, a foreign investor could argue that the host state has breached treaty obligations, including national treatment, MFN treatment or – depending on the treaty text – FET. Accordingly, the regulation of digital platform markets provides a compelling example of how state intervention favouring domestic incumbents may expose governments to liability under international investment agreements.

Overall, technology and AI companies are facing an increasing regulatory pressure from states worldwide. New regulatory burdens, particularly those that are swiftly implemented and narrowly targeted, are fertile ground for investment treaty claims.

The case studies examined in this section illustrate that the intersection of technology-sector regulation and investment treaty law is a live and growing area of legal risk for both states and technology investors. Across data localisation, online censorship, forced compensation schemes and AI regulation, a consistent pattern emerges – states are intervening in the operations of foreign technology companies in pursuit of a range of public interest objectives. The manner in which that intervention is carried out (i.e. whether through sudden bans, discriminatory enforcement, mandatory payment schemes or national security exclusions) will frequently determine whether the measure in question constitutes a legitimate exercise of regulatory sovereignty or an actionable breach of international investment law.

Whilst no single case study produces a definitive answer, each shows that the core treaty standards of FET, nondiscrimination and expropriation are capable of being engaged by technology-specific regulatory measures. Regardless, as in most cases of investment treaty arbitration, the viability of a claim will turn on a fact-specific analysis of the measure's purpose, proportionality and the effect on the investment.

9. Outlook and future trends

The inherent flexibility of the international arbitration process, with the parties' ability to tailor the process and select who will resolve their disputes, is well-suited to addressing disputes that explore novel and evolving areas. Disputes involving AI, the cyber economy, the Internet of Things (IoT), blockchain-related transactions, cybersecurity and other new technologies are increasingly resolved through international commercial arbitration. Arbitrator expertise in cybersecurity and data protection has also proven attractive to high-tech companies developing IoT technology in their choice of dispute resolution.¹¹⁷ Thus, the extension of this trend into international investment arbitration seems likely.

As discussed in Section 4 above, the current number of final awards remains small, but the number of reported claims and threats of claims is significant and growing.¹¹⁸ As arbitral institutions and governments come to terms with the advent of new technologies and AI and seek to adapt to the fast-paced notion of time in the virtual world, technology companies are facing a tidal wave of regulation. This will catalyse a wave of regulatory friction across international borders, giving rise to more disputes between technology companies and states. How technology companies choose to manage those disputes will of course be very circumstance-specific, and the prospect of suing a government in a key market will often be unattractive.

Several emerging developments suggest that disputes involving technology companies will become a more prominent feature of investor-state arbitration in the coming years. As digital platforms, data-driven business models and AI expand across borders, they increasingly interact with regulatory frameworks designed for traditional industries. At the same time, governments are adopting new measures relating to data governance, national security, sanctions compliance and digital sovereignty.

These dynamics are likely to give rise to novel legal questions under investment treaties, particularly regarding the definition of investment, jurisdictional nexus and the treatment of digital assets. Against this background, the following five key trends are likely to shape the next generation of investor-state disputes involving technology companies.

1. Defining 'investment' in the digital economy

Technology companies are characterised by investments that are predominantly intangible in nature, encompassing data, algorithms, software, cloud infrastructure, digital platforms and user networks, rather than traditional physical assets. This raises difficult jurisdictional questions in investment arbitration. Many treaties require a contribution, duration, risk and territorial nexus with the host state. Digital business models, however, frequently operate across borders with limited physical presence.

A central challenge will therefore be whether data, digital assets or platform operations qualify as protected investments, and how tribunals interpret treaty language in light of these evolving business models.

2. Data nationalism and data localisation

Governments around the world increasingly seek to exercise sovereignty over data generated within their territory. This includes measures such as data localisation requirements, restrictions on cross-border data transfers, requirements to store data on local servers, and mandatory access to user data for regulatory or law enforcement purposes.

These policies (often described as "data nationalism") can fundamentally alter the economics of digital platforms and cloud services. They may trigger disputes where foreign technology companies argue that such measures violate protections, such as FET, expropriation or national treatment.

3. National security regulation of technology

Technology is increasingly viewed as a strategic sector linked to national security. Governments are imposing restrictions on telecommunications infrastructure, AI technologies and advanced computing, social media and digital platforms, semiconductor supply chains and cloud services.

States are also invoking security exceptions in treaties or relying on public policy justifications to defend regulatory actions. Tribunals will increasingly need to assess how far national security arguments limit investment protections, a question that is politically sensitive and legally complex.

4. Sanctions and geopolitical fragmentation

Technology companies operate at the centre of geopolitical competition.¹¹⁹ Economic sanctions, export controls and technology restrictions, particularly involving digital infrastructure, software, chips and cloud services, are expanding rapidly. This may create grounds for investors to initiate claims against states, including those related to sanctions affecting technology investments in host states, conflicts between sanctions compliance and treaty obligations, disputes arising from asset freezes, technology bans or forced divestment.

Sanctions regimes may also raise public policy and illegality issues within arbitration proceedings.

5. Rapid regulatory change and digital governance

Governments worldwide are introducing extensive regulation governing the digital economy, including AI and online platforms regulation, cybersecurity requirements, digital services taxes and content moderation obligations.

Because technology evolves faster than regulation, states often intervene after substantial investments have already been made. This may lead to disputes over legitimate expectations of investors, regulatory stability versus the state's right to regulate, and whether new digital regulations amount to indirect expropriation or unfair treatment.

The overall trend is that investor-state disputes involving technology companies are likely to grow as the digital economy expands and governments seek greater control over data, digital infrastructure and strategic technologies. The intersection of investment law, digital regulation, national security and geopolitics will become one of the most complex areas of future investment arbitration.

Annex 1: Investment treaty cases in the technology sector

CASE	DESCRIPTION	STATUS
<i>Unisys Corporation v. Argentine Republic</i> (2003) ¹²⁰	Unisys, a US technology company, brought an ICSID case against Argentina claiming that the state breached its investment treaty obligations under the Argentina-US BIT. The claimant alleged that the state breached the contract between its local subsidiary and the state's Consejo de la Magistratura (the government body that selects, disciplines and manages judges) for an information storage and management project.	Case discontinued in August 2022
<i>IBM World Trade Corporation v. Republic of Ecuador</i> (2004) ¹²¹	IBM instituted arbitration proceedings against the Republic of Ecuador under the US-Ecuador BIT. IBM alleged that Ecuador failed to make payments due under a concession agreement for the lease of hardware and software between IBM del Ecuador CA (a company established under the laws of Ecuador and wholly owned by IBM) and Ecuador, which IBM claimed amounted to a violation of the BIT. Ecuador challenged the tribunal's jurisdiction and competence on seven grounds, including that the concession contract was null and void, and that Ecuador had not expressly consented to arbitrate under the ICSID Convention. The tribunal held that it had jurisdiction over the dispute.	Claim settled for US\$3.5 million
<i>Uber Technologies Inc. v. Republic of Colombia</i> (2019) ¹²²	In December 2019, Uber filed a Notice of Dispute under the US-Colombia Trade Promotion Agreement. Uber alleged that numerous measures taken by the government of Colombia had adversely impacted its investments and the viability of its operations in the state. Uber based its claims on breach of certain obligations under the Trade Promotion Agreement, including the requirement not to subject investments to expropriations or nationalisations except for a public purpose in accordance with due process and in a nondiscriminatory manner; the FET provisions; and the MFN provisions. Uber also alleged that Colombia's order against it constituted an act of censorship in violation of international human rights instruments.	A few months after Uber submitted its notice, the Colombian Court of Appeals revoked the order against it, and to date no arbitral claim against the state has been registered ¹²³
<i>Einarsson v. Government of Canada</i> (2019) ¹²⁴	Shareholders of Geophysical Service Inc. (GSI), a geophysical data-services company, claim that Canada unilaterally disclosed proprietary marine seismic data created or acquired by GSI (taking away their IP rights) without compensation or an alternative course of action. ¹²⁵ This case is notable as it considers whether data constitutes a protected investment under an investment treaty.	Case pending
<i>Vercara LLC (formerly Security Services, LLC d/b/a Neustar Security Services) v. Republic of Colombia</i> (2020) ¹²⁶	US data analytics company, Neustar, brought a claim against the Colombian government for refusing to renew its 10-year concession agreement for the operation of the ".co" internet domain. Neustar claimed that the concession agreement was renewable for a further 10-year term if certain requirements were met, which, according to the company were. Neustar alleged that when the Colombian government declined to renew the concession and decided to hold a public bidding process, it violated the US-Colombia Trade Promotion Agreement. ¹²⁷ It also claimed that the state shared proprietary information with Neustar's competitors. ¹²⁸	Claim decided in favour of state
<i>Unisys Corporation v. Argentine Republic</i> (2003) ¹²⁰	Unisys, a US technology company, brought an ICSID case against Argentina claiming that the state breached its investment treaty obligations under the Argentina-US BIT. The claimant alleged that the state breached the contract between its local subsidiary and the state's Consejo de la Magistratura (the government body that selects, disciplines and manages judges) for an information storage and management project.	Case discontinued in August 2022

CASE	DESCRIPTION	STATUS
<i>IBM World Trade Corporation v. Republic of Ecuador</i> (2004) ¹²¹	IBM instituted arbitration proceedings against the Republic of Ecuador under the US-Ecuador BIT. IBM alleged that Ecuador failed to make payments due under a concession agreement for the lease of hardware and software between IBM del Ecuador CA (a company established under the laws of Ecuador and wholly owned by IBM) and Ecuador, which IBM claimed amounted to a violation of the BIT. Ecuador challenged the tribunal's jurisdiction and competence on seven grounds, including that the concession contract was null and void, and that Ecuador had not expressly consented to arbitrate under the ICSID Convention. The tribunal held that it had jurisdiction over the dispute.	Claim settled for US\$3.5 million
<i>Uber Technologies Inc. v. Republic of Colombia</i> (2019) ¹²²	In December 2019, Uber filed a Notice of Dispute under the US-Colombia Trade Promotion Agreement. Uber alleged that numerous measures taken by the government of Colombia had adversely impacted its investments and the viability of its operations in the state. Uber based its claims on breach of certain obligations under the Trade Promotion Agreement, including the requirement not to subject investments to expropriations or nationalisations except for a public purpose in accordance with due process and in a nondiscriminatory manner; the FET provisions; and the MFN provisions. Uber also alleged that Colombia's order against it constituted an act of censorship in violation of international human rights instruments.	A few months after Uber submitted its notice, the Colombian Court of Appeals revoked the order against it, and to date no arbitral claim against the state has been registered ¹²³
<i>Einarsson v. Government of Canada</i> (2019) ¹²⁴	Shareholders of Geophysical Service Inc. (GSI), a geophysical data-services company, claim that Canada unilaterally disclosed proprietary marine seismic data created or acquired by GSI (taking away their IP rights) without compensation or an alternative course of action. ¹²⁵ This case is notable as it considers whether data constitutes a protected investment under an investment treaty.	Case pending
<i>Vercara LLC (formerly Security Services, LLC d/b/a Neustar Security Services) v. Republic of Colombia</i> (2020) ¹²⁶	US data analytics company, Neustar, brought a claim against the Colombian government for refusing to renew its 10-year concession agreement for the operation of the ".co" internet domain. Neustar claimed that the concession agreement was renewable for a further 10-year term if certain requirements were met, which, according to the company were. Neustar alleged that when the Colombian government declined to renew the concession and decided to hold a public bidding process, it violated the US-Colombia Trade Promotion Agreement. ¹²⁷ It also claimed that the state shared proprietary information with Neustar's competitors. ¹²⁸	Claim decided in favour of state
<i>ES Holdings LP and L1bre Holding, LLC v. United Mexican States</i> (2020) ¹²⁹	Canadian company, ES Holdings, with a 50% indirect interest in a Mexican company called Servicios Digitales Lusak, S. de R.L. de C.V., was awarded a 10-year concession agreement by Mexico City Secretary of Mobility (the Semovi), under which it would replace the taxi meters in all taxis operating in Mexico City and develop a mobile application allowing users to remotely request taxis. ES Holdings asserts that the Semovi breached its obligations under the concession agreement and NAFTA. ES Holdings bases its claims on breaches of FET, national treatment, MFN treatment and expropriation.	Case pending
<i>Wang Jing and others v. Ukraine</i> (2020) ¹³⁰	Chinese investment company, Skyrizon, along with a number of other Chinese investors, brought an investment treaty claim against the government of Ukraine at the Permanent Court of Arbitration, alleging breaches of the China-Ukraine BIT. The claim is based on the Ukrainian authorities' alleged actions to freeze the claimants' acquisition of shares in aerospace company Motor Sich that allegedly owns sensitive technology, based on national security concerns. ¹³¹ Skyrizon's claim requests a ruling that Ukraine has violated the BIT – in particular, the encouragement and mutual protection of investment provisions. It is demanding \$4.5 billion in compensation for alleged unfair treatment of Chinese investors. ¹³²	Case pending

<p><i>Huawei Technologies Co., Ltd. v. Kingdom of Sweden</i> (2021)¹³³</p>	<p>Chinese technology company, Huawei, is bringing an ICSID claim against Sweden, challenging Sweden's decision to exclude Huawei from the state's 5G infrastructure rollout on the basis of national security concerns.¹³⁴ Sweden's telecom regulator, PTS, banned Huawei after allegations were made by the US that the Chinese government would use Huawei equipment for spying.¹³⁵ In the Notification of Dispute, Huawei alleges that Sweden violated its international obligations under the Sweden-China BIT, including the principle of FET, the principle of national treatment and the prohibition against expropriation and nationalisation.¹³⁶ The company is reportedly claiming more than \$625 million.</p>	<p>Case pending</p>
<p><i>eDoc v. Republic of Ecuador</i> (2023)¹³⁷</p>	<p>Consorcio eDoc (eDoc), a consortium comprising of Veridos México S.A. de C.V., a Mexican company and Consorcio STC S.A., a company incorporated in Panama, brought a claim against Ecuador concerning a public contract (valued at US\$32 million) to implement a new biometric identification and passport system. Public reports confirm that an UNCITRAL tribunal has been constituted, but the specific grounds of eDoc's claims have not yet been made public.¹³⁸</p>	<p>Case pending</p>
<p><i>Nexo Capital Inc. & Mirastar EOOD v. Republic of Bulgaria</i> (2024)¹³⁹</p>	<p>Nexo AG, a Swiss cryptocurrency lending company, and two of its Bulgarian affiliates (Mirastar/NDS) brought a claim against Bulgaria under the Bulgaria-Switzerland BIT. Nexo AG claimed that the Sofia City Prosecutor's Office initiated pretrial criminal investigations into the claimants' financial operations, which allegedly caused the claimant reputational damage and harmed its business. Nexo AG sought for US\$3 billion in damages/ compensation for lost opportunities. The state's investigations were terminated with no findings of criminal activity.</p>	<p>Case pending</p>
<p><i>Travizory Border Security SA v. Republic of Kenya</i> (2025)¹⁴⁰</p>	<p>Travizory Border Security SA, a Swiss border security technology company, filed an ICSID arbitration against Kenya, alleging that Kenya unlawfully expropriated and breached their agreement by replacing Travizory's proprietary border management technology without following due process or compensation. Travizory is seeking full reparation for its losses under the Kenya-Switzerland BIT (2006) and the ICSID Arbitration Rules.</p>	<p>Case pending</p>
<p><i>Park Avenue Capital v. Moldova</i> (2025)¹⁴⁰</p>	<p>US company Park Avenue Capital (operating through MaxMD, its healthcare technology business) is bringing an ICSID claim against the Republic of Moldova. The .md domain was exclusively managed by Park Avenue Capital in English- and Spanish-speaking regions for 20 years. The claimant argues that Moldova is in breach of contract and investor rights after it refused to renew the claimant's marketing contract for the country's top-level .md domain for a further 20-year term.</p>	<p>Case pending</p>
<p><i>Fibranet, Sociedad Anónima v. Republic of El Salvador</i> (2025)¹⁴²</p>	<p>Fibranet, a Guatemalan telecom company, sought more than US\$130 million for alleged cancellation of the automatic renewal of radiofrequency spectrum concessions in violation of the Dominican Republic-Central America-United States Free Trade Agreement and the Agreement on Investment and Trade in Services between the Republics of Costa Rica, El Salvador, Guatemala, Honduras and Nicaragua. The claimant argued that the state was acting in breach of the treaties' provisions on expropriation, FPS and standard on FET.</p>	<p>Case settled; El Salvador did not admit liability or make any payment to Fibranet or to Cablefrecuencias, its subsidiary¹⁴³</p>
<p><i>Humans Mobile Ltd. v. Republic of Uzbekistan</i> (2025)¹⁴⁴</p>	<p>Humans Mobile, a Singaporean-based subsidiary of the international Humans Group, brought an ICSID claim against Uzbekistan under the Singapore-Uzbekistan BIT. Humans Mobile seeks damages arising from the actions of several state authorities, including the Central Bank of the Republic of Uzbekistan and AK Uzbektelecom. Human Mobile alleges that the Central Bank, in breach of established procedures, effectively halted the operations of AO "Maroqand", a digital payment organisation, which was integral to its ecosystem. Simultaneously, AK "Uzbektelecom" began systematically putting pressure on the company, which allegedly restricted Humans' capabilities and discriminated against its customers.</p>	<p>Case pending</p>

Endnotes

- ¹ World Bank, [Information and Communication Technologies: A World Bank Group Strategy](#), World Bank 2002, accessed 13 February 2026.
- ² Kayla Zhu, 'Ranked: The Largest S&P 500 Companies Over Time (1985–2024)', Visual Capitalist, 10 April 2025, 13 February 2026.
- ³ FinanceCharts.com, 'Biggest Companies in the World by Market Cap for Feb 2026', FinanceCharts.com, accessed 13 February 2026.
- ⁴ Enrique Dans, 'Around the World, Governments Are Ready to Regulate Big Tech', Forbes, 2 May 2021, accessed 13 February 2026.
- ⁵ Stanford University Institute for Human-Centered Artificial Intelligence, [AI Index Report 2025](#) (Stanford HAI 2025), accessed 13 February 2026.
- ⁶ Meta, [Careers by Location](#) (Meta Careers), accessed 12 February 2026.
- ⁷ PayPal, [Country List](#), accessed 13 February 2026.
- ⁸ PayPal, [PayPal Careers](#), accessed 13 February 2026.
- ⁹ Forbes, 'The Era of Decentralized AI: Navigating Blockchain and AI Convergence', 15 March 2025, accessed 13 February 2026.
- ¹⁰ Brand Finance, [Global 500 2025: The annual report on the world's most valuable and strongest brands](#), accessed 13 February 2026.
- ¹¹ Herbert Smith Freehills Kramer, 'Technology Disputes: The Wave of the Future', 2 December 2020, accessed 13 February 2026.
- ¹² See section 8.1 below on the data localisation requirements that recently came into force across the globe.
- ¹³ See, for example, France's Digital Services Tax (FDST), which entered into force on 1 January 2019 and applies a 3% tax rate to companies that provide either digital interfacing services or digital advertising services. In 2018, the European Commission also proposed new rules for taxation of the digital economy; however, these have been postponed until the international tax system and rules have been adapted to capture the digital economy.
- ¹⁴ For example, a Russian court recently banned Facebook and Instagram in the country, as it claimed that the parent company, Meta, was 'extremist'. See Pjotr Sauer, 'Russia bans Facebook and Instagram under "extremism" law', The Guardian, 21 March 2022, accessed 13 February 2026.
- ¹⁵ For example, a US government report raised concerns that companies may be forced to disclose critical technologies, including source code, to China. The US has accused China of using ownership restrictions and administrative processes to compel US firms to transfer technology to Chinese entities. See Office of the United States Trade Representative, [Findings of the Investigation into China's Acts, Policies and Practices Related to Technology Transfer, Intellectual Property and Innovation under Section 301 of the Trade Act of 1974](#), 22 March 2018, accessed 13 February 2026.
- ¹⁶ Organisation for Economic Co-operation and Development (OECD), [Investment Treaties](#), accessed 13 February 2026.
- ¹⁷ Convention on the Settlement of Investment Disputes between States and Nationals of Other States (adopted 18 March 1965, entered into force 14 October 1966) 575 UNTS 159 (ICSID Convention), art. 54.
- ¹⁸ The ICSID Convention (1966) establishes the framework for investor-state conciliation and arbitration, defining ICSID's institutions, jurisdiction and basic procedural rules.
- ¹⁹ Our empirical analysis draws on the UN Conference on Trade and Development (UNCTAD) Investment Policy Hub and International Arbitration Reporter databases, supplemented by manual research to capture cases fitting our definition of the technology sector. In constructing our database, one of the most up-to-date investor-state arbitration databases, UNCTAD's investment policy hub, is not the best database to build our empirical assessments for the following reasons: 1) UNCTAD's database is outdated, as it only covers cases until December 2024; 2) UNCTAD does not have an equivalent category to the World Bank's Information and Communication. The closest category also includes telecommunications cases which are not exactly the kind of cases we want to track as part of "technology companies"; and 3) UNCTAD does not track those cases (for example, *Uber v. Colombia*) where there was no formal Request for Arbitration. Taking this into consideration, our method for tracking cases which fit within our definition of "technology" sector was more "manual" and aligned". We did go through UNCTAD's database and also International Arbitration Reporter's database – which captures more up-to-date disputes and even those disputes that have not crystallised into actual arbitration proceedings.
- ²⁰ See Annex 1 for a full review of those cases. Note that Annex 1 has been developed by reviewing Investment Policy Hub's and AI Reporter's websites in connection with this paper's definition of technology companies, as portrayed in the World Bank's definition of Information and Communication Technologies.
- ²¹ The 2016 Queen Mary University of London (QMUL) study, 'Pre-empting and Resolving Technology, Media and Telecoms (TMT) Disputes', concluded that technology firms systematically eschew litigation in favour of negotiated settlements to preserve the "commercial ecosystem" and mitigate the existential risk of technological obsolescence. Drawing on empirical data from in-house counsel, the study noted that approximately 75% of surveyed organisations maintain formal dispute resolution policies that prioritise mediation. See Queen Mary University of London, 'Pre-empting and Resolving Technology, Media and Telecoms Disputes: International Dispute Resolution Survey', School of International Arbitration, 2016.
- ²² [Bridgestone Licensing Services Inc. and Bridgestone Americas Inc. v. Republic of Panama](#), ICSID Case No. ARB/16/34, accessed 13 February 2026.
- ²³ *Deutsche Bank AG v. Democratic Socialist Republic of Sri Lanka*, ICSID Case No. ARB/09/2, Award, 31 October 2012, paras. 288 – 291.
- ²⁴ *Nova Scotia Power Incorporated v. Bolivarian Republic of Venezuela*, ICSID Case No. ARB(AF)/11/1, Award, 30 April 2014.
- ²⁵ Case law in the English courts, for example, has recently confirmed that cryptocurrencies constitute property at common law. Whether this approach will also be adopted by international arbitral tribunals is yet to be confirmed. See *AA v. Persons Unknown & Others* [2019] EWHC 3556 (Comm).
- ²⁶ Vienna Convention on the Law of Treaties (adopted 23 May 1969, entered into force 27 January 1980) 1155 UNTS 331, art. 31.
- ²⁷ See, for example, art 1(2) of the Colombia-UK BIT (2010), art 1 of the Rwanda-US BIT (2008), art. 1(1) of the China-Korea BIT (2007) and art. 10.29 of the Panama Trade Promotion Agreement.
- ²⁸ German Model BIT (2008), art. 1.
- ²⁹ Argentina-US BIT, art. 1(a)(iv).
- ³⁰ See, for example, art. G 40 of the Canada-Chile Free Trade Agreement; Agreement between Canada and the Republic of Peru for the Promotion and Protection of Investments (signed 14 November 2006, entered into force 20 June 2007) art. 1; Agreement between the Government of the United Mexican States and the Government of the People's Republic of China on the Promotion and Reciprocal Protection of Investments (signed 11 July 2008, entered into force 6 June 2009), art. 1.
- ³¹ Coined after the *Salini v. Morocco* tribunal issued its award on how to interpret Article 25. See *Salini Costruttori SpA and Italstrade SpA v. Kingdom of Morocco*, ICSID Case No. ARB/00/4, Decision on Jurisdiction (23 July 2001), which interprets the requirements set forth in Article 25 of the ICSID Convention in relation to what are the characteristics of an investment.
- ³² *Salini Costruttori SpA and Italstrade SpA v. Kingdom of Morocco*, ICSID Case No. ARB/00/4, Decision on Jurisdiction (23 July 2001).

- ³³ A. Mitchell and J. Hepburn, 'Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer', *Yale Journal of Law & Technology*, 2017.
- ³⁴ See L. Cuatrecasas, '[International Investment Policy and the Coming Wave of Data Flow Disputes](#)', *Michigan Business & Entrepreneurial Law Review*, 2021, citing *Maygar Farming Company Ltd v. Hungary*, ICSID Case No. ARB/17/27, Award (13 November 2019), paras. 274 – 275.
- ³⁵ See, for example, *Romak SA v. Republic of Uzbekistan*, PCA Case No. AA280, Award (26 November 2009), para. 207.
- ³⁶ *Bayview Irrigation District v. Mexico (U.S. v. Mex)*, ICSID Case No. ARB(AF)/05/1, Award (19 June 2007) para. 103. See also *Grand River Enterprises Six Nations Ltd and others v. United States of America*, UNCITRAL, Award (12 January 2011) para. 87.
- ³⁷ *Apotex Inc v. United States of America*, UNCITRAL, Award on Jurisdiction and Admissibility (14 June 2013).
- ³⁸ *Ibid.* See also A. Mitchell and J. Hepburn, 'Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer', *Yale Journal of Law & Technology*, 2017.
- ³⁹ *SGS Société Générale de Surveillance SA v. Republic of the Philippines*, ICSID Case No. ARB/02/6, Decision on Jurisdiction (29 January 2004). See also *British Institute of International and Comparative Law, 'ISDS and Corporate Restructuring'*, accessed 13 February 2026.
- ⁴⁰ *LESI SpA and Astaldi SpA v. People's Democratic Republic of Algeria*, ICSID Case No. ARB/05/3, Decision on Jurisdiction (12 July 2006) para. 73.
- ⁴¹ *European Media Ventures SA v. Czech Republic*, UNCITRAL, Partial Award on Liability (8 July 2009) para. 38.
- ⁴² See generally, *Pawlowski AG and Project Sever s.r.o. v. Czech Republic*, ICSID Case No. ARB/17/11, Award (1 November 2021) 108.
- ⁴³ *Pawlowski AG and Project Sever s.r.o. v. Czech Republic*, ICSID Case No ARB/17/11, Award (1 November 2021) paras 289, 291.
- ⁴⁴ *Sea Land Service Inc v. Government of the Islamic Republic of Iran and Ports and Shipping Organization*, IUSCT Case No. 33, Award No. 135 33 1 (22 June 1984), para. 62.
- ⁴⁵ *International Thunderbird Gaming Corporation v. United Mexican States*, UNCITRAL, Arbitral Award (26 January 2006) 147.
- ⁴⁶ *Oxus Gold plc v. Republic of Uzbekistan*, UNCITRAL, Award (17 December 2015), para. 313.
- ⁴⁷ A. Mitchell and J. Hepburn, 'Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer', *Yale Journal of Law & Technology*, 2017.
- ⁴⁸ *Ibid.*
- ⁴⁹ *Saluka Investments BV v. Czech Republic*, UNCITRAL, Partial Award (17 March 2006), para. 305.
- ⁵⁰ *Philip Morris Brands Sàrl, Philip Morris Products SA and Abal Hermanos SA v. Oriental Republic of Uruguay*, ICSID Case No. ARB/10/7, Award (8 July 2016), para. 269.
- ⁵¹ F. Sarmiento and S. Nikiéma, '[Fair and Equitable Treatment: Why It Matters and What Can Be Done](#)', IISD Best Practices Series, International Institute for Sustainable Development, November 2022, accessed 12 February 2026.
- ⁵² In early January 2026, US investors in Coupang filed a notice of intent under KORUS, alleging that South Korea's regulatory response to a major 2025 data breach was discriminatory and punitive. See *Global Arbitration Review, 'US e-commerce investors threaten Korea over data breach response'*, 17 January 2026, accessed 12 February 2026.
- ⁵³ [United States-Korea Free Trade Agreement](#) (entered into force 15 March 2012), art. 11.5, accessed 12 February 2026.
- ⁵⁴ *S D Myers Inc v. Government of Canada*, UNCITRAL, Partial Award (13 November 2000), paras. 252 – 253.
- ⁵⁵ *Global Arbitration Review, 'Broadband provider settles ICSID claim against Serbia'*, accessed 13 February 2026. Please note that although illustrative of potential claims that can be brought, this case has been settled.
- ⁵⁶ *LG&E Energy Corp, LG&E Capital Corp and LG&E International Inc v. Argentine Republic*, ICSID Case No. ARB/02/1, Decision on Liability (3 October 2006), para. 187.
- ⁵⁷ *Franz Sedelmayer v. Russian Federation*, Arbitration Award (7 July 1998).
- ⁵⁸ *OOO Manolium Processing v. Republic of Belarus*, PCA Case No. 2018 06, Final Award (22 June 2021).
- ⁵⁹ United Nations Conference on Trade and Development, '[Trade and Development Report 2003: Capital Accumulation, Growth and Structural Change](#)', 2003, accessed 13 February 2026.
- ⁶⁰ European Commission, '[EU-China Comprehensive Agreement on Investment \(CAI\): Investment Liberalisation – Section II](#)', 2021, accessed 13 February 2026.
- ⁶¹ '[European Union-China Comprehensive Agreement on Investment \(CAI\)](#)', draft text published 2021, arts. 3.1(f), (j), accessed 13 February 2026.
- ⁶² *Joseph Charles Lemire v. Ukraine*, ICSID Case No. ARB/06/18, Decision on Jurisdiction and Liability (14 January 2010), 505; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* (Merits) [1986] ICJ Rep 14, 233.
- ⁶³ *El Paso Energy International Company v. Argentine Republic*, ICSID Case No. ARB/03/15, Award (31 October 2011), 240 – 241.
- ⁶⁴ There are various debates on the applicability of exception clauses in the national security space. We will not rehash all of those in this paper due to limitations of space, but a good review of those debates can be found here: Caroline Henckels, 'General and Security Exceptions and the Question of Compensation in International Investment Law', 28 *Journal of International Economic Law* 63 (2025); Dang Nguyen Phuong Nhi and Pham Hai Quyen, 'Preserving State Regulatory Autonomy through General Exception Clauses in International Investment Agreements: Insights from Vietnam', 14 *Vietnamese Journal of Legal Sciences* 18 (2025); and Caroline Henckels, 'Whither Security? The Concept of "Essential Security Interests" in Investment Treaties' *Security Exceptions*, 27 *Journal of International Economic Law* 114 (2024).
- ⁶⁵ Y. Levashova, 'International investment agreements and the right to regulate: an introduction', in Yulia Levashova, 'The Right of States to Regulate in International Investment Law: The Search for Balance Between Public Interest and Fair and Equitable Treatment', *International Arbitration Law Library Series*, vol. 50, 2019, 27.
- ⁶⁶ *Canfor Corporation v. United States of America*, Decision on Preliminary Question (6 June 2006), para. 187.
- ⁶⁷ International Law Commission, '[Draft Articles on Responsibility of States for Internationally Wrongful Acts](#)', 2001, art. 25, accessed 13 February 2026.
- ⁶⁸ *LG&E Energy Corp, LG&E Capital Corp and LG&E International Inc v. Argentine Republic*, ICSID Case No. ARB/02/1, Decision on Liability (3 October 2006), para. 257.
- ⁶⁹ Toby Fisher, '[Chinese chipmaker threatens multibillion claim against Netherlands](#)', *Global Arbitration Review*, 30 December 2025, accessed 13 February 2026.

- ⁷⁰ Ibid.
- ⁷¹ D. Svantesson, '[Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines](#)', OECD Digital Economy Papers No. 301, OECD Publishing, 22 December 2020, 4, accessed 13 February 2026.
- ⁷² Clifford Chance, '[Is the Clock "Tik Toking" on Global Data Localisation?](#)', 20 August 2020, accessed 13 February 2026.
- ⁷³ Practical Law Data Privacy & Cybersecurity, '[Global Data Localization Laws: Overview](#)' (Practical Law, law stated as of 16 April 2025), accessed 13 February 2026.
- ⁷⁴ BigBang360, '[Understanding Data Localization Laws](#)', accessed 13 February 2026.
- ⁷⁵ Global Data Review, '[China: Data Localisation](#)', 2021, accessed 13 February 2026. See also Data Security Law of the People's Republic of China (adopted 10 June 2021, in force 1 September 2021), art. 32; Cybersecurity Law of the People's Republic of China (adopted 7 November 2016, in force 1 June 2017), art. 37; Personal Information Protection Law of the People's Republic of China (adopted 20 August 2021, in force 1 November 2021), art. 40.
- ⁷⁶ Covington & Burling LLP, '[LinkedIn Blocked in Russia Following Breach of Data Localization Laws](#)', 17 November 2016, accessed 13 February 2026.
- ⁷⁷ International Association of Privacy Professionals (IAPP), '[Encrypt Your Data to Make GDPR and Russian Data Localization Law Compatible](#)', 17 December 2020, accessed 13 February 2026.
- ⁷⁸ Radio Free Europe / Radio Liberty, '[Moscow Court Fines Social Media Giants for Refusing to Localize User Data in Russia](#)', 26 August 2021, accessed 13 February 2026.
- ⁷⁹ Mondaq, '[Facebook Fined \\$50,000 for Violating Russian Data Localization Law](#)', 10 December 2020, accessed 13 February 2026.
- ⁸⁰ The Diplomat, '[The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam](#)', 10 January 2020, accessed 13 February 2026.
- ⁸¹ GRC World Forums, '[Data Localisation: The Curious Case of India's Step Back from Globalisation](#)', 27 March 2020, accessed 13 February 2026.
- ⁸² World Economic Forum, '[This is the state of play in the global data centre gold rush](#)', 22 April 2025, accessed 13 February 2026.
- ⁸³ Fortune Business Insights, '[Data Center Market Size, Share & Industry Analysis, By Component \(Hardware, DCIM \(Data Center Infrastructure Management\) Software, and Services\), By Data Center Type \(Colocation, Hyperscale, Edge, and Others\), By Tier Level \(Tier 1 and Tier 2, Tier 3, and Tier 4\), By Data Center Size \(Small, Medium, and Large\), By Industry \(BFSI, IT & Telecom, Healthcare, Government, Manufacturing, Retail & E commerce, and Others\), and Regional Forecast, 2026 – 2034](#)', last updated January 2026, accessed 13 February 2026.
- ⁸⁴ FTI Consulting (Delta Partners), '[United Kingdom](#)', accessed 13 February 2026. See also, Clifford Chance, '[Is the Clock "Tik Toking" on Global Data Localisation?](#)' 20 August 2020, accessed 13 February 2026.
- ⁸⁵ TechCrunch, '[PayPal to halt operations in Turkey after losing license, impacts "hundreds of thousands"](#)', 31 May 2016, accessed 13 February 2026.
- ⁸⁶ PYMNTS, '[Turkish Regulator Deals Blow X Border Commerce](#)', 1 June 2016, accessed 13 February 2026.
- ⁸⁷ Federal Law on Activities of Foreign Entities in the Information and Telecommunications Network in the Territory of the Russian Federation (Russia, 2021).
- ⁸⁸ Jurist, '[Russia fines Google, sues WhatsApp for violating data localisation law](#)', 1 August 2021, accessed 13 February 2026.
- ⁸⁹ EY, '[Russia: Law on activities of foreign internet companies in Russia signed by the President](#)', accessed 13 February 2026.
- ⁹⁰ S. Zhang, 'Protection of Cross Border Data Flows Under International Investment Law: Scope and Boundaries' in Julien Chaisse, Leïla Choukroune and Sufian Jusoh (eds.), *Handbook of International Investment Law and Policy* (Springer 2021) 11.
- ⁹¹ *Mobil Investments Canada Inc and Murphy Oil Corporation v. Government of Canada*, ICSID Case No. ARB(AF)/07/4, Decision on Liability and on Principles of Quantum (22 May 2012).
- ⁹² Global Affairs Canada, '[NAFTA – Chapter 11: Investment](#)', accessed 13 February 2026.
- ⁹³ IPLocation.net, '[What is Internet Censorship?](#)', 18 July 2016, accessed 13 February 2026.
- ⁹⁴ Freedom House, '[New report: persistent authoritarian repression and backsliding democracies drive 15th consecutive year of decline in global freedom](#)', accessed 13 February 2026.
- ⁹⁵ Allen & Overy, '[Government measures around the globe will lead to more investment treaty claims](#)', accessed 13 February 2026.
- ⁹⁶ OSW, '[Discipline and punish: how Turkey controls the internet](#)', 24 June 2025, accessed 13 February 2026.
- ⁹⁷ TechRadar, '[X, WhatsApp, YouTube, and other social media platforms go dark in Turkey for 24 hours – and VPN usage spikes](#)', 10 September 2025, accessed 13 February 2026.
- ⁹⁸ BBC News, '[LinkedIn blocked by Russian authorities](#)', 17 November 2016, accessed 13 February 2026.
- ⁹⁹ BBC News, '[Russia confirms Meta's designation as extremist](#)', 11 October 2022.
- ¹⁰⁰ The Guardian, '[Russia blocks Snapchat and restricts Apple's FaceTime, state officials say](#)', 4 December 2025.
- ¹⁰¹ The Guardian, '[Social media shut down in Sri Lanka in bid to stem misinformation](#)', 21 April 2019, accessed 13 February 2026.
- ¹⁰² Business Today, '[Why Facebook, Twitter, Instagram could be banned in India from tomorrow?](#)', 25 May 2021, accessed 13 February 2026.
- ¹⁰³ Reuters, '[WhatsApp sues Indian government over new privacy rules – source](#)', 26 May 2021, accessed 13 February 2026.
- ¹⁰⁴ *LG&E Energy Corp, LG&E Capital Corp and LG&E International Inc v. Argentine Republic*, ICSID Case No. ARB/02/1, Decision on Liability (3 October 2006), para. 125.
- ¹⁰⁵ *Metalclad Corporation v. United Mexican States*, ICSID Case No. ARB(AF)/97/1, Award (30 August 2000).
- ¹⁰⁶ *Telenor Mobile Communications AS v. Republic of Hungary*, ICSID Case No. ARB/04/15, Award (13 September 2006), para. 70.
- ¹⁰⁷ *Telenor Mobile Communications AS v. Republic of Hungary*, ICSID Case No. ARB/04/15, Award (13 September 2006), para. 103; Divyansh Sharma, '[Social Media Business: Can BITs Protect?](#)', accessed 13 February 2026.
- ¹⁰⁸ See *Chemtura Corporation v. Government of Canada*, ICGJ 464, Award (2 August 2010), para. 258, where it was held that market share and customer access are assets susceptible to expropriation.
- ¹⁰⁹ *Tippett, Abbot, McCarthy, Stratton v. TAMS AFFA Consulting Engineers of Iran*, 6 Iran US CI Trib Rep 219, 225 (22 June 1984).

- ¹¹⁰ Reuters Institute for the Study of Journalism, '[Generative AI and the News Report 2025: How People Think About AI's Role in Journalism and Society](#)', accessed 13 February 2026.
- ¹¹¹ Press Gazette, '[News publisher AI deals and lawsuits: Full list](#)', accessed 13 February 2026.
- ¹¹² The Japan News, '[Yomiuri Sues U.S. AI Startup over Use of Articles; Perplexity Allegedly Used Over 100,000 News Stories](#)', 10 August 2025, accessed 13 February 2026.
- ¹¹³ Axios, '[Exclusive: Meta strikes multiple AI deals with news publishers](#)', 5 December 2025, accessed 13 February 2026.
- ¹¹⁴ S Gáspár-Szilágyi, '[When the Dragon comes Home to Roost: Chinese Investments in the EU, National Security, and Investor-State Arbitration](#)', (2024) 15(2) Journal of International Dispute Settlement 195, accessed 13 February 2026.
- ¹¹⁵ '[Denmark examines potential cybersecurity gap in Chinese-built electric buses](#)', Sustainable Bus, 5 November 2025, accessed 13 February 2026
- ¹¹⁶ Aparobot, '[NEO Debut: A Leap for Home Automation or a Privacy Predicament? NEO Humanoid, a \\$20k hype? 1X's humanoid uses human help for data, aiming for full autonomy by 2026. Buying it might be trading privacy for data autonomy](#)', 31 October 2025, accessed 13 February 2026.
- ¹¹⁷ N. Ali Khasawneh, M. Mazzawi and R. Christie, '[Arbitration and the Advent of New Technologies](#)', 29 July 2022, accessed 13 February 2026.
- ¹¹⁸ M. Darowski and R. Holland, '[Civil unrest and investor-state claims in the telecommunications sector](#)', Global Arbitration Review, 23 August 2024, accessed 13 February 2026.
- ¹¹⁹ See, e.g., on geopolitical aspects of cybersecurity, Yarik Kryvoi and Tomoko Ishikawa, 'The Geopolitical Divide, Norm Conflict, and Public-Private Partnership in Cybersecurity Governance', in Tomoko Ishikawa and Yarik Kryvoi, eds., 'Public and Private Governance of Cybersecurity: Challenges and Potential', Cambridge University Press; 2023: 240 – 264.
- ¹²⁰ *Unisys Corporation v. Argentine Republic*, ICSID Case No. ARB/03/27, accessed 13 February 2026.
- ¹²¹ *IBM World Trade Corporation v. República del Ecuador*, ICSID Case No. ARB/02/10, accessed 13 February 2026.
- ¹²² *Uber Technologies, Inc. and Uber Colombia, S.A.S. v Colombia, Notice of Dispute*, ICSID-related proceeding (30 December 2019, accessed 13 February 2026.
- ¹²³ Forbes Staff, '[Court revokes SIC decision ordering Uber to leave Colombia](#)', Forbes, 19 June 2020, accessed 13 February 2026.
- ¹²⁴ UNCTAD, '[Investment Policy Hub](#)', 2019, accessed 13 February 2026.
- ¹²⁵ Ibid.
- ¹²⁶ *Neustar, Inc. v. Republic of Colombia*, ICSID Case No. ARB/20/7, accessed 13 February 2026.
- ¹²⁷ Damien Charlotin and Lisa Bohmer, '[US-Based Technology Company Makes Good on Earlier Threat to Initiate Treaty-Based Arbitration Against Colombia](#)', 10 March 2020, accessed 13 February 2026.
- ¹²⁸ J. Edward Moreno, '[Neustar Takes Colombia to Arbitration for Nix of Domain Deal](#)', Law360, 12 August 2021, accessed 13 February 2026.
- ¹²⁹ *Espíritu Santo Holdings, LP (ES Holdings) v. United Mexican States*, ICSID Case No. ARB/20/13, accessed 13 February 2026.
- ¹³⁰ *Wang Jing, Li Fengju, Ren Jinglin, Xu Changshung, Liu Yanning and others v. Republic of Ukraine*, UNCITRAL Arbitration (PCA), accessed 13 February 2026.
- ¹³¹ Freshfields Bruckhaus Deringer, '[The Future of Arbitration in the Tech Space](#)', accessed 13 February 2026.
- ¹³² Global Times, '[China's Skyrizon seeks court arbitration, demands Ukraine pay \\$4.5b compensation](#)', 29 November 2021, accessed 13 February 2026.
- ¹³³ *Huawei Technologies Co., Ltd. v Kingdom of Sweden*, ICSID Case No. ARB/22/2, accessed 13 February 2026.
- ¹³⁴ Global Arbitration Review, '[Huawei brings ICSID claim against Sweden over 5G ban](#)', 24 January 2022, accessed 13 February 2026.
- ¹³⁵ Ibid.
- ¹³⁶ '[Written Notice of Dispute](#)', accessed 13 February 2026.
- ¹³⁷ *eDoc v. Republic of Ecuador*, accessed 13 February 2026.
- ¹³⁸ Investment Arbitration Reporter, '[Ecuador Round Up: New arbitrations are revealed, the state is brought before the ICJ, and government proposes referendum to remove arbitration ban from constitution](#)', 14 July 2025, accessed 13 February 2026.
- ¹³⁹ *Nexo AG, NDS EOOD and Mirastar EOOD v. Republic of Bulgaria*, ICSID Case No. ARB/24/2, accessed 13 February 2026.
- ¹⁴⁰ *Travizory Border Security SA v. Republic of Kenya*, ICSID Case No. ARB/25/54, [Press Release of Travizory Border Security SA on Initiation of the Arbitration](#), 18 December 2025, accessed 13 February 2026.
- ¹⁴¹ *Park Avenue Capital v. Republic of Moldova*, ICSID Case No. ARB/25/25, accessed 13 February 2026.
- ¹⁴² Fibranet, *Sociedad Anónima v. Republic of El Salvador*, ICSID Case No. ARB/25/6, accessed 13 February 2026.
- ¹⁴³ Arnold & Porter, '[Arnold & Porter Secures Settlement in ICSID Arbitration for Republic of El Salvador](#)', 4 December 2025, accessed 13 February 2026.
- ¹⁴⁴ *Humans Mobile Ltd v. Republic of Uzbekistan*, ICSID Case No. ARB/25/24, accessed 13 February 2026.

Cooley's International Arbitration Practice

Cooley

- Provides unparalleled experience in domestic and international arbitrations involving technology and life sciences
- Represents technology and gig economy companies in mass, consumer and employment arbitrations
- Serves as counsel in commercial arbitrations conducted under:
 - International rules – International Chamber of Commerce (ICC), London Court of International Arbitration (LCIA), International Centre for Dispute Resolution (ICDR), Singapore International Arbitration Centre (SIAC), Hong Kong International Arbitration Centre (HKIAC) and China International Economic and Trade Arbitration Commission (CIETAC)
 - US rules – American Arbitration Association (AAA) and JAMS
 - Ad hoc rules – United Nations Commission on International Trade Law (UNCITRAL)
- Counsels investors in investment treaty disputes against foreign sovereigns under the leading rules – including the International Centre for Settlement of Investment Disputes (ICSID), ICC and UNCITRAL
- Handles enforcement, confirmation or vacatur of arbitral awards in the US and leads teams in foreign jurisdictions
- Boasts significant experience with insurance coverage disputes and all aspects of third-party funding
- Offers a multilingual team that includes lawyers trained and qualified in both civil and common law systems collaborating across offices in the US, Europe and Asia
- Ranks in Chambers, The Legal 500, Benchmark Litigation and Who's Who Legal – International Arbitration

“Cooley provides excellent counsel on extremely complex matters. They're very responsive to clients' needs and even anticipate issues before they arise.”

– CHAMBERS USA, 2025

The British Institute of International and Comparative Law (BIICL)



British Institute of
International and
Comparative Law

The British Institute of International and Comparative Law (BIICL) is one of the leading independent research centres for international and comparative law in the world. Its high-quality research projects, seminars and publications encompass almost all areas of public and private international law, comparative law and European law. The Institute is at the forefront of discussions on the many contemporary issues of international and comparative law. BIICL includes within it the innovative Bingham Centre for the Rule of Law, which has a particular focus on the many rule of law issues worldwide.

BIICL exists to develop and advance the understanding of international and comparative law in the UK and around the world, and to promote the rule of law in national and international affairs. Through its work, it seeks to improve decision-making, which will help to make the world a better place and have a positive impact on people's daily lives. BIICL includes three specialist Forums in Competition Law, Product Liability and Investment Treaty Law, as well as the Human Rights Due Diligence Forum.

The Investment Treaty Forum (ITF) was founded as a part of BIICL in 2004 to serve as a global centre for serious high-level debate in the field of international investment law. The Forum is a membership-based group, bringing together some of the most expert and experienced lawyers, business managers, policy advisers, academics and government officials working in the field. Like BIICL itself, the Forum has a reputation for independence, even-handedness and academic rigour. The Forum membership is by invitation only.

Read more:

- [British Institute of International and Comparative Law](#)
- [Investment Treaty Forum](#)

“Throughout its existence, BIICL has been a unique organisation, making a vital contribution to international security and prosperity by influencing debate, legal reform and policy making.”

– LORD NEUBERGER OF ABBOTSBURY, FORMER PRESIDENT OF THE UK SUPREME COURT

“BIICL’s reputation for combining rigorous research and analysis with the practical application of the law, and the respect in which it is held by important stakeholders, made them an obvious partner for us.”

– MICHAEL MEYER, HEAD OF INTERNATIONAL LAW, BRITISH RED CROSS

Cooley



British Institute of
International and
Comparative Law



9 781918 137033 >