



HERBERT
SMITH
FREEHILLS

**COLLABORATE
AND DIVERSIFY:
CONNECTIVITY
IN THE DIGITAL AGE**

Contents

Overview

The evolving connectivity architecture

04 Infrastructure

08 Digitalisation

15 5G

From builder of networks to provider of new services

20 Internet of Things

26 Cloud

30 Security

35 Verticals

45 Big data

Conclusion

How our team can help

Overview

Transformation in the global telecoms ecosystem is gathering momentum. It is driven, to a large extent, by evolving technologies and growing customer appetite for hyper-connectivity.

Alongside industry stalwarts seeking to retain existing customers and reach out to new ones with more innovative and relevant offerings, a new breed of competitor is emerging.

Skilful at carving out niche opportunities and delivering what customers want, these newcomers are growing quickly and disrupting the market as we know it.

In this report, we examine how traditional telecoms companies can compete with these new competitors by becoming more relevant to the digital age customer and transform themselves into providers of connectivity-enabled services. We assess, in particular, how collaboration and diversification are driving opportunities and growth in the sector, enabling providers to achieve speed and scale and to transition from their core activities into new, profit-enhancing activities.

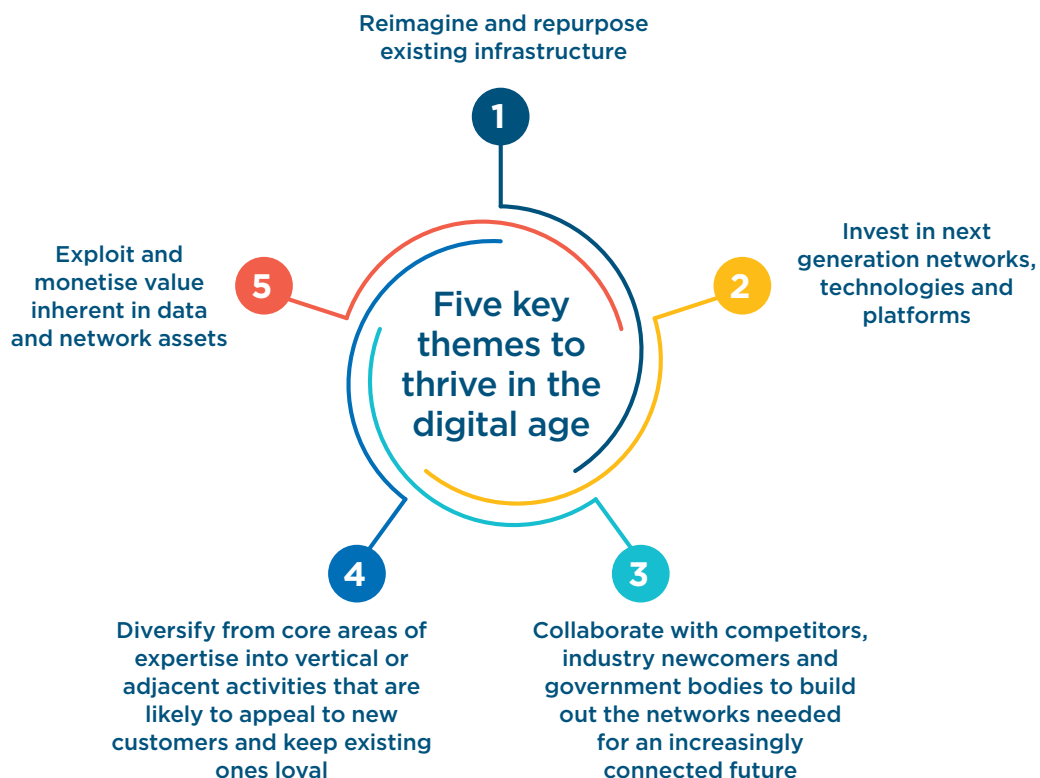
We consider the evolving connectivity architecture; the opportunities inherent in existing infrastructure and those that will be made possible by digitalisation and the advent of 5G. We also examine the scope for traditional players to move from being builders of networks to enablers of new services, such as Internet of Things, cloud, security, verticals and big data.

In their quest for a place within this highly competitive and fast-moving landscape, reinvention is very much on the cards for conventional providers. Though they have recourse to their long-established and trusted reputations, they know that future success will hinge on their adaptability, commerciality and relevance to a new type of customer in a rapidly evolving market.

As such, the term 'telecoms company' no longer seems appropriate, as existing and new players focus on providing connectivity and related services.

Amidst this need for reinvention, Herbert Smith Freehills has identified five key themes in order for connectivity providers to thrive in the digital age.

How well will you cope with the shift from traditional telecoms to enablers of possibilities in the digital revolution?



The evolving connectivity architecture





Infrastructure

For connectivity providers, the costs associated with infrastructure are huge. Investment is needed to maintain and upgrade infrastructure to fit the next technology iteration and to roll out new infrastructure to deliver additional coverage or capacity.

It is not a problem that connectivity providers have to tackle alone. The combination of ever-growing demand for connectivity and the value and long-term returns inherent in assets, such as towers, networks, data centres, subsea cables and satellites, make infrastructure an increasingly attractive asset class.

Infrastructure investors are also attracted to the barriers to competitor entry, low volatility, relatively visible and stable cash

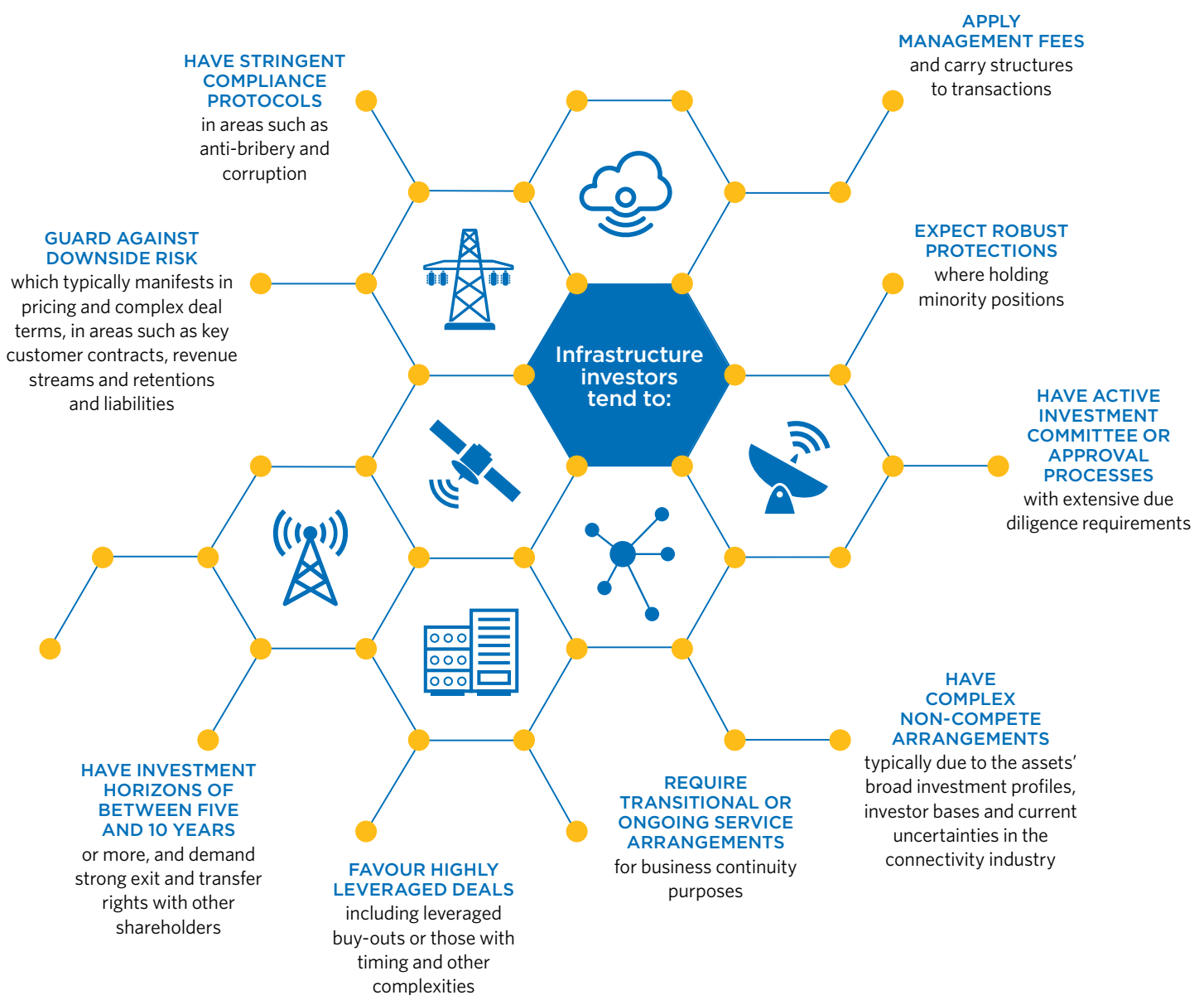
flows and, generally, high cash-conversion potential these assets provide.

By selling off these assets or seeking investment in them, connectivity providers gain access to liquid funds with which to bolster their networks or invest in other areas of their organisations.

Ways to raise capital by full or partial divestment of infrastructure assets

Divestment, whether by full or partial sale of assets or by co-investment, creates opportunity for connectivity providers to raise capital. Typically, infrastructure assets first need to be separated from the rest of the connectivity business in ways that minimise risk and enhance investment attractiveness.

Understanding infrastructure investors



Divestment options, as explored below, include hive off, co-investment and initial public offering (IPO).

Model	Most appropriate for ...	Pros	Cons
<p>Hive off</p> <p>Transfer to or use an independent infrastructure company. This could include sale and leaseback of towers, involving an independent tower company, or the sale of data centres, subsea cable or satellites to specialist providers or infrastructure funds or institutional investors.</p> <p>This is a medium- to high-risk approach.</p>	<ul style="list-style-type: none"> • Connectivity providers looking to refocus the business (eg mobile operators wanting to focus more on offering content services) • Wholesale/lease providers • Companies monetising assets • Infrastructure providers/ investors 	<ul style="list-style-type: none"> • Likely high initial and ongoing financial benefits • Low involvement in management and operations • Ease of ongoing regulatory and competition/antitrust compliance 	<ul style="list-style-type: none"> • Potential loss of control/influence for connectivity provider, including expiry/ on termination of ongoing arrangements • Services/leaseback arrangements may be on arms length terms • Regulatory and competition/antitrust/ foreign investment clearance may be required • May require pre-hive-off restructuring and licences in some jurisdictions
<p>Co-investment</p> <p>Partial sale of infrastructure company or joint venture or other co-investment vehicle for infrastructure.</p> <p>This is a low- to medium-risk approach.</p>	<ul style="list-style-type: none"> • Connectivity providers • Wholesale/lease providers • Companies monetising assets • Infrastructure providers/ investors 	<ul style="list-style-type: none"> • Likely control/influence for connectivity providers • Services/leaseback arrangements may be on preferential terms 	<ul style="list-style-type: none"> • Possible low initial and ongoing financial benefits • Likely ongoing involvement in management and operations • Regulatory and competition/antitrust/ foreign investment clearance may be required and ongoing compliance may prove challenging • May require pre-hive-off restructuring and licences in some jurisdictions • Difficult to unwind • Any asset transfers and shared services may have to be dealt with in separate agreements and services agreements needed for relevant aspects
<p>IPO</p> <p>Listing and initial public offering of infrastructure company, whether full or partial stake.</p> <p>This is a medium- to high-risk approach.</p>	<ul style="list-style-type: none"> • Companies in jurisdictions with shortage of capital/ availability of debt at high interest rates • Large companies with a demonstrable track record and good growth outlook • Companies with substantial capital requirements in aggressive expansion mode • Companies monetising assets 	<ul style="list-style-type: none"> • Exit for investors • Pay off/reduce existing debt, with likely high initial and ongoing financial benefits • Active trading market for shares in the company • Access to much deeper pools of capital at potentially lower costs • Low involvement in management and operations • Ease of some ongoing regulatory and competition/antitrust compliance 	<ul style="list-style-type: none"> • Compliance with listing rules and other regulations (depending on jurisdiction of listing and investors) • Market and investor pressures may compel the company to focus on short-term results, instead of long-term growth or scrutiny by sophisticated investor groups, eg long-term/low-risk pension funds, may sometimes lead to interference or conservatism • Potential loss of control/influence for connectivity provider and inability to unwind • May require pre-IPO restructuring and other activities • Services/leaseback arrangements may be on arms-length terms • Regulatory clearances might be required

How to move forward

To ensure assets are investable and the deal will attract the right calibre of investor, connectivity providers should consider the following aspects:

Financial

- Is there a source of medium to long-term revenue for the business? Infrastructure investors will be attracted by robust contracts with key customers, for instance.
- Is there funding available for planned capital expenditure? Are the infrastructure assets bankable?
- What financial models are in place, between infrastructure providers and users, to guarantee sufficient future revenue protection?
- What are the transaction-related costs, including taxes and write-downs in the context of overall returns?

Commercial

- Given that some connectivity assets come with technology risks, do they best fit an infrastructure or real estate profile?
- Has consideration been given to the lifespan and potential use of infrastructure and the impact of changes in technology or the market on the assets? This might include the impact of new market entrants or consolidation.
- Are there opportunities for expansion, eg into new geographies or products/services?
- What is the relationship between the infrastructure provider and connectivity providers, or other users of the assets? What control or influence, term/termination rights and procurement-driven processes do users of the assets have?
- What consideration should be given to initial and ongoing tax and structuring, including any foreign investment restrictions or required approvals?
- Has consideration been given to the commercial and operational elements of the investment/co-investment strategy? These might include: scope of services and performance framework of the infrastructure co-investment, the level of flexibility afforded to connectivity providers, the required contributions and support from connectivity providers, and exit/unwind issues.

Regulatory

- Is the level of regulation applicable to the infrastructure assets, and any impact of licensing and mandatory access, understood?
- Have the risks of regulatory change or deregulation been explored?
- Are there any issues relating to land, permits and planning processes for upgrading or deploying infrastructure?



Case in point: I Squared Capital and HGC

Herbert Smith Freehills advised I Squared Capital, a private equity infrastructure investor, on the acquisition of the connectivity-related assets of Hutchison Telecommunications' fixed-line business, HGC, for US\$1.86 billion.

HGC is a leading fixed-line service provider to fixed and mobile carriers, OTT service providers, corporates and businesses, residential and data centres, in Hong Kong and around the world. They use HGC's fibre, Wi-Fi, data centre and cable system infrastructure. Much of HGC's revenue is under long-term contracts to a diverse base of customers, including major mobile operators.

Importantly, the transaction included an agreement which gives HGC an exclusive right to provide services to Hutchison Telecommunications in Hong Kong. Hutchison Telecommunications, in turn, will market and promote the fixed-line business services of HGC relating to Hong Kong to certain related entities.

These transactions were awarded Hong Kong Deal of the Year by *FinanceAsia*, 2017, and Global Deal of the Year and Asia Pacific Deal of the Year by *Infrastructure Investor Global Awards*, 2018.



Digitalisation

If connectivity providers are to deliver on customer demands for convenience, speed and personalisation, they will have to digitalise almost every part of their value chains.

Though digitalisation of networks, IT systems and operations will reduce providers' cost to serve, reinvent the customer experience and enable new and more relevant services, it comes at a substantial cost.

It is a cost that connectivity providers cannot afford to dismiss. Failure to act promptly will translate into significant lost earnings and opportunities.

Some of that investment burden could be alleviated by collaborations with vendors and other third parties. Collaboration means that connectivity providers can achieve the benefits of speed, scale, efficiency, flexibility and interoperability, while sharing the risks.

First, however, connectivity providers need to identify those areas of the value chain that most need digitalisation and be alert to the challenges that will come with collaborative endeavour.

What parts of the value chain to digitalise and why



Networks, IT systems and infrastructure

Digitalisation can transform networks. Take software-defined networking and network function virtualisation, for instance. They will enable the shift from capital-intensive and complex physical networks, traditionally managed by large teams of engineers and field staff, to digital networks that are simpler, require fewer people and which can be customised, managed remotely and even self-heal.

As networks become more reliable, secure and powerful, they are also simpler and less costly to deploy, operate and upgrade. In turn,

connectivity providers will be faster to market with their new offerings. Meanwhile, artificial intelligence, analytics and automation tools will transform networks and IT too.

With digitalisation, IT infrastructure will transition from complex, disparate and fragmented systems, to common cloud-based or edge computing solutions. The upshot of consolidated platform layers and proximate processing will be more efficient collection, analysis and use of data, as well as better product conceptualisation, informed by customer behaviour. This will allow connectivity providers to deliver new and enhanced platforms and services to customers more easily and more cost efficiently.

The flipside of this transition to new technology is massive upheaval and challenge for conventional players. This will become more pertinent as they address ever-shortening technology lifecycles and the significant costs of digitalisation.

The World Economic Forum predicts that the value of digitalisation to the connectivity industry could exceed US\$1.2 trillion in cumulative operating profit from 2016 to 2025.

**Digital Transformation Initiative
Telecommunications Industry, January 2017**



DIGITAL STACKS

to accelerate product and service development and near or real-time analytics for greater personalisation of services for customers

A SIGNIFICANT REDUCTION IN OPERATING COSTS

USE OF DIGITALISED SYSTEMS

underpinned by new software and cloud technologies

CUSTOMISED OFFERS FOR CUSTOMERS

with a frictionless online service experience and the speed and convenience of simplified and fully digitalised customer care

A CENTRALISED AND SIMPLIFIED BUSINESS

meaning leaner and more agile operations and a more efficient cost structure

SIMPLER USER INTERFACES

to enhance the customer experience at all levels

SMARTER, SIMPLER AND MORE FUTURE-READY IT SYSTEMS

as new digital services, enabled by an advanced network with future-proof features, are unlocked

AN IMPROVED TECHNOLOGY STRUCTURE

to fast-track digital innovation, for example in entertainment, communication, internet of things and financial services

The case for digitalisation



The customer experience

Customers expect and already receive seamless, omni-channel and hassle-free experiences, service and care from digital companies.

Now they want the same from their connectivity providers too.

They want user-friendly interfaces, exciting in-store experiences and quick and readily available service. Open, interoperable and scalable solutions, that work seamlessly and allow customers to intervene, interact and personalise features, will succeed.

Every element of the customer experience, including fulfilment, assurance and billing, have the potential to be transformed digitally and made leaner and more relevant and productive. Each can be moved from physical to online channels.

Those activities associated with innovation, customer research and product development are most in need of digital investment. This is where connectivity providers lag significantly behind digital businesses and consumer products companies.



Data and analytics

A mix of digital technologies, including smart algorithms, artificial intelligence, predictive analysis and real-time feedback loops, can make connectivity providers more proficient at mining customer data and mapping behaviours.

By adopting digital strategies for data and analytics, connectivity providers will be better equipped to optimise networks, deliver targeted marketing and achieve greater customer retention and return on investment.



The workforce

Those connectivity providers that embrace new digital technologies will not only simplify their operations and cut costs but attract a new generation of talent too.

In-demand individuals are keen to become part of more innovative and agile workplaces, which allow for collaboration and where there is appetite for disruption and experimentation. Connectivity providers need to show that they can offer a more stimulating and dynamic work environment and hire and develop talent free from connectivity backgrounds for new areas of their businesses.

Nonetheless, as changing technological capabilities impact on workforce numbers, roles and responsibilities, evolving organisations must be mindful of managing and retaining talent and dealing with cultural shifts.

The World Economic Forum says telecoms companies only invest between 10 and 15% of their revenues in innovation, customer research and product development. Digital businesses invest a more significant 35%, while consumer product companies invest as much as 70%.

***Digital Transformation Initiative
Telecommunications Industry, January 2017***

The risks and challenges of collaborating on digitalisation

No company is likely to be able to digitalise its networks and operations single-handedly. Connectivity providers will need to collaborate with vendors and third parties if they are to achieve speed, scale and efficiency.

However, collaboration comes with risks. The table below sets out models for collaborating with third parties on digitalisation, the issues that might arise and how risks can be mitigated:

Issue	Summary	Possible risk mitigation
Managing multiple players	<ul style="list-style-type: none"> • More joint venture, partnership or cooperation arrangements • Resources and processes needed to manage different players • Integration risks • Impact on existing arrangements • Antitrust/competition compliance 	<ul style="list-style-type: none"> • More initial trial/pilot arrangements • Pass risks to third parties contractually • Use of integrators • Collaboration charters • Robust notification and communication requirements • Avoiding “spillover” cooperation into areas where competitors should continue to compete
Reliance on external parties	<ul style="list-style-type: none"> • More partner focus than traditional procurement and a need for greater flexibility • Scope and requirements, including development, transformation, warranty, maintenance, upgrades and changes • Technology road map • Performance framework • Governance/management framework, including change management • Financial arrangements and cost uncertainties 	<ul style="list-style-type: none"> • Agile scope and approach, with clear consequences of changes • Possible involvement in vendor technology road map, supplier forums and knowledge sharing • Increased due diligence and contingency plans • Contractual rights, such as renewal, audit/inspection, step-in, termination and handover/access • Liability and indemnity provisions (including credits and liquidated damages) to allocate risk appropriately • Controls over charges, including milestones, holdbacks or earn-outs, and benchmarking
Information sharing and confidentiality	<ul style="list-style-type: none"> • Privacy/data protection compliance, including for analytics • Antitrust/competition compliance 	<ul style="list-style-type: none"> • More flexible terms with customers • Appropriate restrictions on information access and use • Information-sharing and firewall guidelines • Security requirements, including changes and directions
Intellectual property rights, also in respect of information/data	<ul style="list-style-type: none"> • Ownership of intellectual property, including developments and derivative works • Licensing of intellectual property • Possible essential patents • Technology transfers 	<ul style="list-style-type: none"> • A robust intellectual property strategy and framework • Clear intellectual property ownership and use provisions • Access on fair and reasonable terms if required • Escrow of third-party source code

Issue	Summary	Possible risk mitigation
Control over network	<ul style="list-style-type: none"> • Partitioning access, backhaul/line-side and core portions of network • Continue to meet regulatory requirements 	<ul style="list-style-type: none"> • Regulatory and compliance provisions in contracts, including changes and directions • Restrictions on further subcontracting without consent • Advocate for fair and equal regulatory treatment • Advocate for regulatory policy which supports digitalisation, eg in respect of fees/rates/taxes
Cultural shift	<ul style="list-style-type: none"> • Impact on existing workforce • Recruitment of digital natives • Disruption from increased use of technology 	<ul style="list-style-type: none"> • Retraining and redeployment • Framework and sponsorship to support cultural change • Careful management of changes to employment terms

How to move forward

The transition to digitalised service provider is fraught with challenges that come from external influences, such as shortening technology lifecycles and heightened competitor activity. Internally, challenges exist in the shape of cultural and system obstacles.

To move forward with digitalisation, connectivity companies need to consider:

Resourcing

- Human resource rights and employment law issues that are likely to arise from workforce reskilling and realignment.
- Initial and ongoing financial and human capital investment needs.
- Workforce incentives to embed major business transformation/change projects.

External relationships

- Impact of digitalisation on vendor, partner and customer relationships, including existing and future arrangements.

Due diligence

- Impact of transformational change across technical, financial, commercial, legal and regulatory obligations.

Intellectual property

- Strategy to deal with the likely increase in copyright, confidentiality, trade secrets, know how, privacy and similar issues in an 'open innovation' environment.
- Vendor-driven solutions and options to provide input into vendor product roadmaps.

Data management

- Issues relating to reorganisation and use of data and information during and following the digital transformation programme.
- Regulatory matters, including security and access to networks, data and customer information.

Protections

- Business continuity and disaster recovery arrangements.
- Changes to liability and insurance profiles.



Case in point: Software partnership between Veon and Ericsson

Herbert Smith Freehills advised Veon, one of the world's largest communications providers, on a software partnership worth over US\$1 billion to radically transform its global IT infrastructure. It is the largest and most ambitious project of its nature in the industry's history.

The partnership agreement reflects Veon's commitment to bring the best services to customers through innovative solutions and industry collaborations. It marks a fundamental milestone in Veon's transformation into a digital pioneer.



5G

5G is set to arrive in many countries by 2020, with 6G expected by around 2040. 5G auction processes are already moving forward, or have been completed, in some countries, with bidders vying for an allocation of the spectrum bands from national regulators.

5G will offer instantaneous and reliable mobile internet connection, that could be up to one thousand times faster than 4G. It will make possible pioneering innovations, such as remote control surgery, 3D medical imaging, high-risk manufacturing or engineering, as well as improving the safety potential of autonomous vehicles. It will help to power the Internet of Things and enable a raft of innovative new products and services for customers.











These innovations will bring a whole new world of commercial opportunity, alongside evolving social and ethical considerations too.

Collaborative investment models

To lessen the overall 5G investment cost, while enabling participation in its potential revenue growth, connectivity providers might have to consider collaborative ownership or partnering models and alternative risk and reward sharing arrangements.

Already, masts, sites and electronic infrastructure are commonly shared, subject to regulations in force in relevant jurisdictions. Now, collaborative arrangements might extend to partnerships between independent infrastructure and connectivity providers over, say, a shared or neutral host framework, which could even hold 5G spectrum. Equally, collaboration might be possible over national publicly or privately owned shared networks; or single or shared networks in specific cities or regions.

Collaborations can be purely contractual or by joint venture or partnership. They might include creative or complex financing, public concession or managed services agreements. Whichever route connectivity providers take, they need to be mindful of legal, regulatory, tax and accounting structures and obligations, to ensure that they secure the revenues and associated profits from collaboration.

Parameters	 1G	 2G	 3G	 4G	 5G
					
Introduced in	1980s	1993	2001	2009	2020
Location of first commercialisation	USA	Finland	Japan	South Korea	N/A
Speed (data rates)	2.4 Kbps to 14.4 Kbps	14.4 Kbps to 200 Kbps	473 Kbps to 3.1 Mbps	30 Mbps to 100 Mbps plus	1 Gbps plus
Special characteristic	First mainstream consumer wireless communication	Digital version of 1G technology	Digital broadband, speed increments	Very high speeds, all IP	Advanced technologies, Flatter IP
Features	Voice only	Multiple users on single channel	Multimedia features, video call	High speed, real time streaming	High speed and capacity
Band width	Analog 30 KHz	25 MHz	25 to 100 MHz	100 MHz	1000x BW per unit area
Technology	Analog cellular	Digital cellular, CDMA	CMDA 2000 (1xRT, EVDO), UMTS, EDGE	WiMax, LTE Wi-fi	WWWW

Collaborative options might include:

Model	Most appropriate for ...	Pros	Cons
<p>Services agreement</p> <p>Commercial agreement between connectivity providers in respect of 5G network arrangements.</p> <p>This is a low- to medium-risk option.</p>	<ul style="list-style-type: none"> • Mobile operators, either sharing for the first time or with existing services agreement network partners • Spectrum sharing/pooling • Infrastructure provider arrangements • Wholesale/lease arrangements 	<ul style="list-style-type: none"> • Simple and quick to establish or to integrate into existing network-sharing services agreements • Maintains provider's control/independence • Simple to unwind 	<ul style="list-style-type: none"> • Unlikely to allow for various new ownership/partnering models for 5G • May not achieve desired synergies • Regulatory and competition/antitrust compliance might be challenging • Asset transfers might have to be dealt with in a separate agreement
<p>Joint-venture agreement</p> <p>Entity incorporated for purposes of 5G.</p> <p>This is a medium- to high-risk option.</p>	<ul style="list-style-type: none"> • Mobile operators with existing joint-venture entity network partners • New ownership/partnering models for 5G 	<ul style="list-style-type: none"> • Simple and quick to integrate into existing network sharing services arrangements for joint venture company • More likely to allow for new 5G ownership/partnering models • Likely to achieve desired synergies (subject to scope of the joint venture entity) 	<ul style="list-style-type: none"> • Difficult/slow to establish • Loss of control/independence • Difficult to unwind • Regulatory and competition/antitrust clearance and ongoing compliance may be required • Asset transfers and shared services might have to be dealt with in separate agreements • Services agreements might be required
<p>Alternative financing</p> <p>Financing to support new ownership/partnering models for 5G, from:</p> <ul style="list-style-type: none"> • government, including stimulus/cornerstone funding for 5G • development banks or export credit agencies • private investors (including funds) • new forms of hybrid projects, cashflow, asset, vendor financing • mezzanine or high-yield debt <p>This is a medium- to high-risk option.</p>	<ul style="list-style-type: none"> • Mobile operators • Infrastructure providers • Wholesale/lease providers • New ownership/partnering models for 5G 	<ul style="list-style-type: none"> • Access to required/greater investment capital • Ability to compete more effectively • Ability to redeploy capital • Ability to realign other business areas • Diversification of risk • Most issues can be addressed if financial modelling supports alternative financing 	<ul style="list-style-type: none"> • Difficult/slow to set-up • Interest/carries/fees/expenses/distributions • Potential state aid or competition/antitrust issues • Complexity of governance/participation rights/security structure • Liquidity/exit/maturity windows • Complexity of cross-defaults/insolvency/subordination/change of control

Advocacy

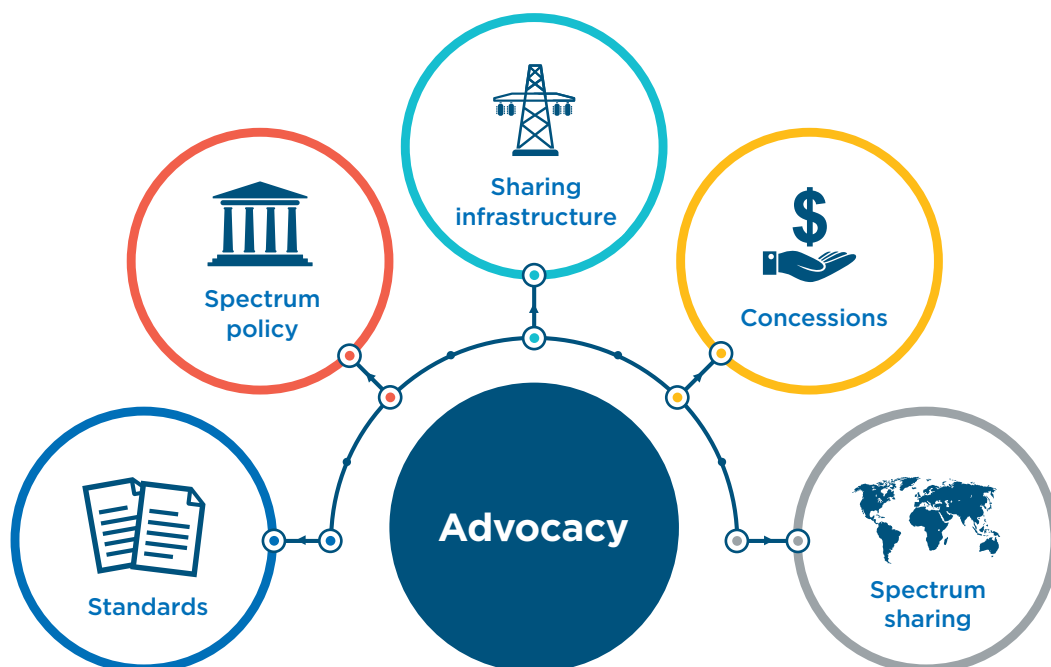
If 5G is to be deployed successfully and effectively, connectivity providers need to participate in shaping the regulatory environment that will govern it. By lobbying regulators and policymakers early in the regulatory process, they can contribute to the creation of a stable, investment-friendly, tax-favourable and conducive operating environment.

Connectivity providers can:

- Counter the risk of fragmented global implementation of 5G and the emergence of different proprietary networks by calling for cross-industry and international standardisation of spectrum policy and technology. The potential risks from unlicensed spectrum, such as Wi-Fi, or dedicated short-range communications (IEEE technology) for autonomous vehicles, can perhaps be reduced.
- Lobby for transparent rules on spectrum allocation and reassignment, trading, pooling and sharing, as well as joint bids.

5G spectrum auction plans are being published by regulators in Europe (the UK has already held its initial auction), as well as in South Korea and Australia. Discussions are underway in the US, Canada, India, China and Japan.

- Advocate for changes to law and regulations on collaborative endeavour and acquiring, sharing and upgrading assets. This will help to counter the shortage of sites for new antennae and lack of fibre for routing traffic from 5G base stations.
- Call for governments and regulators to consider tax concessions and lower fees/rates to reduce both the burden of 5G deployment and encourage investment.
- Petition governments, on grounds of improved efficiency and better services to end users, for sharing, pooling and trading spectrum in jurisdictions in which it is not currently permitted.



How to move forward

At a business level, connectivity providers need to assess their own transitional activities so they can move forward and participate in the 5G world.

Financial

- Assess funding needs and options, both initial and ongoing.
- Consider requirements for bidding at auction for allocation of 5G spectrum.
- Consider assets and resources that might be shared, as well as tax and accounting treatments, valuations and adjustments.

Regulatory

- Assess the regulatory framework needed to deploy 5G efficiently and effectively.
- Assess requirements relating to policy, market structure and regulatory reform, and tax/fee/rates relief.
- Evaluate regulatory and competition issues that might arise, including potential for collusion and information sharing. Merger clearances and ongoing monitoring may also be required.

Governance

- Consider governance frameworks, such as management arrangements, design, deployment and operation, and approach to procurement and key vendor management.

Commercial

- Identify new applications and services that could be served by 5G.
- Consider options to share rights to use spectrum.
- Put in place strategy for 5G sites and fibre to backhaul traffic from 5G base stations, including the extent of collaboration.
- Consider exit and unwinding arrangements for shared assets.



Case in point: One of world's first 5G auctions

A leading digital communications company was awarded 80Mhz of 5G spectrum in one of the world's first 5G auctions. The spectrum, valued at around US\$730 million, is suited to 5G because it can carry large amounts of data.

The spectrum auction follows a multi-billion dollar network sharing arrangement with another leading communications company, through a joint venture company. The arrangements include sharing 5G infrastructure and potential spectrum trading.

The joint venture manages network sites for both companies and consolidates sites to create a single grid. It generates

efficiencies in cell site deployment and operation of network infrastructure. The joint venture also maintains and manages infrastructure assets and sites.

The joint venture, effectively the trusted partner for both companies, brings insight and expertise to all aspects of infrastructure acquisition, design, build, maintenance and property management, to ensure the availability of mobile communications. As a consequence, coverage, capacity and network speeds are strengthened across cities, towns and rural locations.

Herbert Smith Freehills advised on a judicial review of the 5G auction rules and on the joint venture arrangements.

The background features a complex digital environment. A large, semi-transparent wireframe grid structure, resembling a building or a data center, is positioned in the upper left. The scene is filled with numerous glowing lines and streaks of light in shades of blue and red, creating a sense of motion and depth. The overall aesthetic is high-tech and futuristic.

**From builder of
networks to
provider of
new services**

Internet of Things

Human-machine-information interactions are opening up a whole new world of connectivity possibilities and new product and service options. Conventional players, excited by its potential, are expanding their core capabilities to compete for a share of revenue from the Internet of Things (IoT).

Diversification sees them capitalising on greater demand for connectivity as well as venturing into building, acquiring and partnering with or co-investing in IoT platforms so that they can roll out new services to consumers and corporate customers. In this way, they stand to reap the benefits that come with controlling as much of the IoT value chain as possible.

IoT essentially allows increased information flows and collection, computation and exploitation of data between connected devices. Still in its infancy, the potential of IoT will impact almost all industries, at every level in their value chains.

Already, IoT use-cases are making an impact in industrial and commercial scenarios, such as connected homes and vehicles, smart cities and buildings, digital health and agriculture, and in areas of industrial automation, like manufacturing, energy and logistics.

The IoT value chain

Connectivity providers need to first understand the IoT value chain and identify where, within it, they can best play to their strengths and optimise their broader digital strategies.

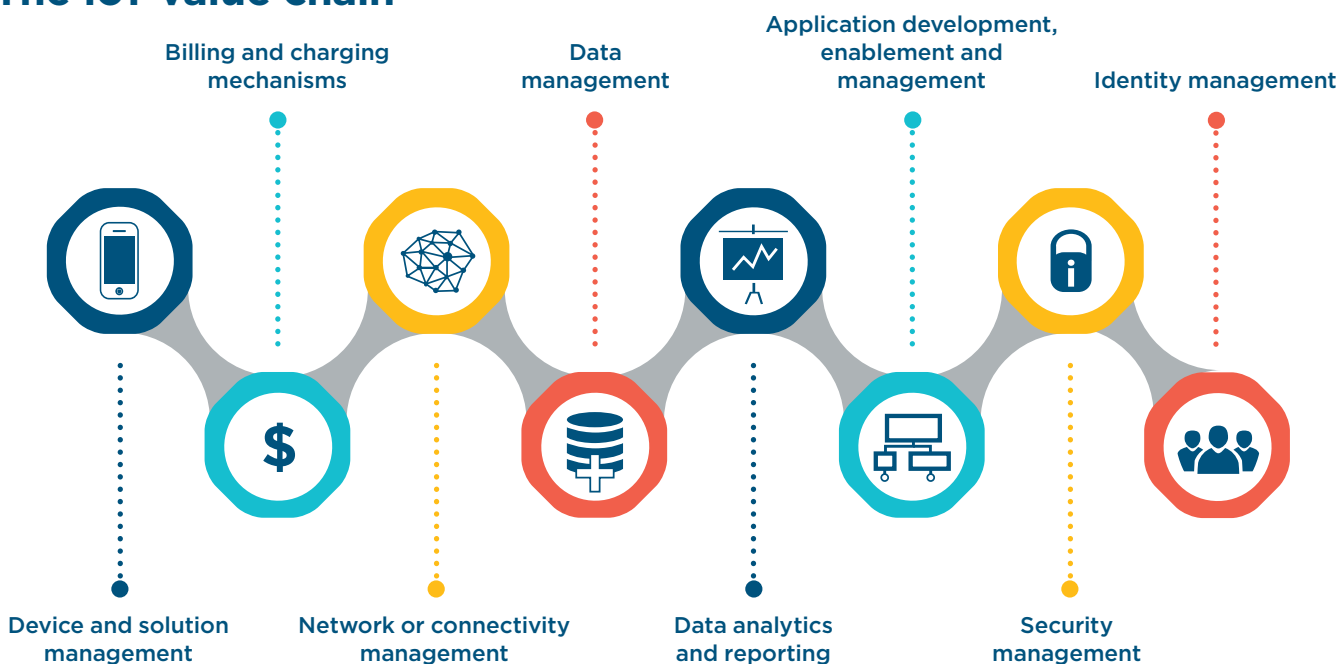
Some providers are focused on gateways, connection efficiency, network optimisation and connectivity and device management.

Meanwhile, other providers are developing standalone operations. They are offering IoT platforms that enable applications and data to be managed and leveraged.

At the network level, though 5G and low-power wireless are expected to be the principal means of connection, threats to IoT and connectivity providers come from solutions that use unlicensed spectrum and from differing technology standards.

Why collaboration is needed for IoT

The IoT value chain



IoT solutions need a mix of participants and technologies to work together.

Collaboration can take on a number of guises that allow players to both compete and cooperate with one another in innovative partnering arrangements or alliances. This creates a vibrant and dynamic market.

To secure funding to build out their IoT networks, connectivity providers might collaborate with competitors, newcomers, government, investors or financiers. We already see connectivity providers working together in an open environment (often via industry associations) to develop and harmonise standards and protocols to support the efficient development of IoT.

In a global market, this collaborative endeavour goes some way to ensuring that international standards can be developed and applied consistently across geographies, industry boundaries and value chains too. Ultimately, this will allow for convergence across worldwide platforms and ecosystems.

On the technology side, connectivity providers might team up with platform and middleware providers, as well as security specialists. IoT platforms can also be used to support large app-development and integration with customers' back end systems.

Collaborations could be by way of acquisition or investment, or strategic alliances with other players in the IoT value chain, in order to strengthen their offerings.

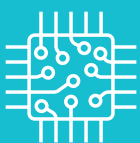
A number of connectivity providers and other IoT players have set up accelerators and ecosystem-collaboration hubs in order to connect and experiment with, and develop ecosystem partners.

Increasingly, the opportunity to act as integrators in the evolution of IoT is being taken up by connectivity providers.

Integration also allows big data, extracted from sensors, machines and databases, to be leveraged and used by other third parties, such as app developers. There are opportunities for connectivity providers to make data sets available through common, interoperable application programme interfaces, harmonised data models/sets, and other access technologies. Data analytics and machine learning also offer prospects for generating value from IoT big data.

The number of connected IoT devices will jump to 125 billion by 2030. Global data transmissions are expected to increase 50% per year, on average, over the next 15 years.

IHS Markit



Participants in the IoT market might include:

- Connectivity providers
- Device makers
- Network vendors
- Original equipment manufacturers
- Chipset makers
- Infrastructure companies
- Developers
- Adopters
- Module suppliers
- Service providers
- System integrators
- Other ecosystem partners



Protections to safeguard providers and customers

Connectivity providers need to be alert to the risks and challenges that come with collaboration and advances in technology. The table below outlines areas that require protection to safeguard the provider's organisation and customers.

Area of protection	Key considerations
Security	<ul style="list-style-type: none"> • The threat of security breaches in the IoT ecosystem increases as more and more devices are connected. Depending on the type of deployment, security breaches may present risks to health and safety • IoT deployments consist of devices, platforms, layers and interfaces, meaning there are many aspects to secure • Companies are embedding security into their products and services at every stage of the IoT value chain, including devices, chipsets, software and services. Industry standard security guidelines, authentication and assessments are being adopted • Connectivity providers have a track record in providing secure, reliable, licensed services and, as such, are established and trusted providers. Some have their own cyber security units. This creates an opportunity for connectivity providers to compete effectively in the IoT market • In the IoT market, connectivity providers often include service and product offerings that go beyond connectivity. These require more specialist security expertise
Privacy	<ul style="list-style-type: none"> • There should be particular focus on how data is used, stored and shared, ensuring that individuals are aware and that requisite consents are obtained • Adequate measures need to be in place to address privacy risks and compliance requirements, particularly for information security purposes and data transmitted across borders • Privacy protocols should be designed into IoT services, specifications and architectures for new systems and processes. They must be implemented in a way that promotes transparency and consumer choice
Data management	<ul style="list-style-type: none"> • IoT business models involve sourcing what is often proprietary data, owned or controlled by another company or individual. Ownership and licensing rules and information-sharing restrictions should be set out in agreements between the parties • Legal and regulatory risk and compliance frameworks need to be adopted, in relation to intellectual property, security, privacy and confidentiality
Regulatory and policy	<ul style="list-style-type: none"> • Connectivity providers need to advocate for regulations that facilitate global connectivity and coverage for remote-managed platforms, as well as harmonised spectrum policies • Availability of numbering resources, both extra-territorial and international, may need to be managed • Remote provisioning and management of connections is required, using over-the-air initial subscription, and allowing subsequent changes from one provider to another • Connectivity providers should advocate for incentives that encourage IoT adoption. Some countries have adopted IoT-specific tax reductions, which have helped to spur activity • The deeper that connectivity providers go in providing IoT applications and data, the greater the likelihood that laws and regulations in other relevant sectors will apply. Regulatory surveys are often needed to identify licensing, compliance or other requirements

Area of protection	Key considerations
Intellectual property rights	<ul style="list-style-type: none"> • A robust strategy and framework for intellectual property is needed, with a clear approach to ownership and use of intellectual property rights • Enhancements and derived data, source code management, open source, confidentiality, collateral-usage rights, and contractual rights and restrictions, including onward-licensing requirements, require consideration • Patents may become 'standard essential patents' and, if so, access on fair-and-reasonable terms may be required
Liability and insurance	<ul style="list-style-type: none"> • Liability for data, software and platform issues needs to be considered, particularly where there are potential consequences for health and safety • Product and tort liability, as well as warranty and contractual recourse, are undergoing a shift. This is because traditional supply-chain models are being disrupted as more direct relationships are formed between service or software providers and end users. More complex issues, around remoteness and causation, arise as a result • Class/collective action-type claims in relation to IoT are likely to increase, which will need to be managed both proactively and reactively • The approach to design or manufacturing defects, warnings/instructions and customer-facing statements needs to be reviewed. Open-ended commitments to cover liability should be avoided • There will be implications for insurance and insured parties. As risk is spread across the value chain, different parties will be responsible. Insurance cover and implications need to be reassessed • Insurance companies may prescribe tools, techniques and guidance relating to IoT, which should be followed by insured parties
Contracts	<ul style="list-style-type: none"> • IoT contracts are often collaborative in nature. Responsibility, including for deployment, maintenance and upgrades, needs to be allocated appropriately across the value chain and integration risk managed carefully. The performance framework should reflect the balance of responsibilities • There should be clear governance arrangements, requirements for cooperation, well-defined interfaces and clear management responsibilities • Terms and conditions should be flexible, eg for pilots and testing, agile methodologies, the development of new standards, changes in technology, innovation and priorities, and law and regulation • Clear pricing models and a robust change-control mechanism should be included • The term, termination, early termination fees and exit, including support for re-tendering and handover, should be included. Employee transfer issues and risks need to be dealt with • The liability regime must be clear, including for defects and damage to property and loss of data or intellectual property, or other damage from cyber attacks or unauthorised access. Liability for inaccuracies in data may also be an issue
Antitrust/competition	<ul style="list-style-type: none"> • Authorities have a clear interest in applying competition law concepts to IoT-related activities, such as big data. These may include merger control, behavioural aspects and technology transfers • In particular, care needs to be exercised in relation to potentially anti-competitive agreements, particularly exclusivity and non-compete clauses

How to move forward

As connectivity providers seek out the commercial opportunities that IoT presents, they need to consider:

Strategy

- What position they will occupy in the IoT value chain and the organisational roadmap for diversification into IoT. Drawing on their network infrastructure and associated expertise, many are positioning themselves as IoT platform providers or rolling out end-to-end IoT solutions.
- Processes to be redefined and new products/services to be created.
- Standardised solutions which mitigate third-party integration risk.
- How the IoT strategy and business case fit with the organisation's cloud, enterprise and data/platform strategies.

Standardisation

- The different technology standards and protocols that are being adopted.
- Flexibility to deal with new standards and changes in technology.

Future proofing

- Adoption of flexible and scalable platforms and engaging a diverse range of ecosystem partners.
- Future-proofing infrastructure, technology and arrangements.

Disaster recovery

- Adequate disaster recovery and cyber security planning and responses.

Risk

- Assessments of products, services and supply chains.
- Coordinated end-to-end management, including integration risks.

Workforce

- How to find, train and retain specialists with IoT skills.



Cloud

Data centres are key to the digital ecosystem. They provide the infrastructure over which cloud services are offered. As operationally intensive businesses, they are dependent on technically proficient management and vast teams of skilled people.

Connectivity providers are reviewing their data centre and cloud propositions. They are weighing up options to own or co-invest in data centres; to provide co-location or proprietary cloud services; or to collaborate and resell cloud services via third parties.

Whatever strategy they pursue, connectivity providers must be mindful of increasingly complex laws and regulations, including:

- data privacy, security and transfers, including onshoring/localisation/sovereignty
- access to data by government/law enforcement/security services or lawful interception
- foreign ownership restrictions or approvals, licensing, authorisation or registration, and
- ongoing compliance.

Moreover, customers are demanding greater transparency. They want to know where their data is stored, not only for reasons of regulatory compliance, but so that they can enjoy improved latency and reliability too.

Collaboration for growth

Connectivity providers, whether seeking to co-invest, own outright or enter into sale and leaseback arrangements, find that collaboration on data centres gives access to:

- an expanded international footprint, greater capacity, and joint-marketing activity
- services, systems or infrastructure and network agility, flexibility and programmability
- sustainable energy systems
- build, integrate and operate services for the data centre, network and systems
- alternative sources of funding, and
- local expertise.

Collaboration also allows parties to optimise their networks and security and disaster recovery arrangements.

For some, however, the active mergers and acquisitions market is an opportunity to divest their data centre and managed hosting assets, in order invest in other strategic priorities.



Connectivity providers, although equipped to manage data centres, are now rethinking their cloud strategies. In the cloud space, they are faced with:

- rising capital and operating costs
- challenges with funding
- competition from technology hyper-scalers with rapid expansion plans
- increased interest from pure-play operators, private equity firms, real estate investment trusts and infrastructure funds, and
- the rise of edge computing, which allows more capabilities to be offered at the edge of the network and away from the data centre itself.



Evaluating the cloud value chain

Data centres are built and operated, and data centre and cloud services offered, utilising a web of relationships.

As collaboration intensifies, the ways in which these arrangements are contracted and interrelate, become critically important. Different approaches to the data centre and cloud value chain come with varying risks and regulatory complexities.

Aspect	Issue to manage	Risk mitigation
Design and construction of data centres	<ul style="list-style-type: none"> • Speculative investment risks and upfront capital expenditure • Permits, licences, approvals, consents and possible foreign ownership restrictions • Management of vendors and integration risks including delays and changes • Construction laws and regulations and environment, health and safety • Price certainty risks 	<ul style="list-style-type: none"> • Site due diligence and assessment of access, power, connectivity and planning requirements • Commitments from customers, access to funding (taking into account that land/buildings may have a different value from mechanical and electrical equipment), development incentives and other tax concessions • Fixed-price, staged payments and robust change control/variation/adjustment mechanisms • Cooperation of vendors, detailed commissioning and sign-off/handover, performance framework, retention/damages regime and performance security/guarantee • Access, oversight, step-in and, ultimately, the right to terminate • Clear liability and insurance regime, including defect notification process and damage to property
Operation and maintenance of data centres	<ul style="list-style-type: none"> • Service scope and responsibilities • Management of vendors and integration risks • Governance, processes and procedures, and access and security • Future proofing, including to address changes in technology and price certainty and price-increase risks • Construction laws and regulations for further works and environment, health and safety • Financing, including vendor finance 	<ul style="list-style-type: none"> • Clear scope for co-location, cloud, management and maintenance • Cooperation of vendors and flexibility around terms and conditions for vendors, eg for changes in technology, innovation and priorities • Fixed price, escalators, cost savings/improvement, robust change control mechanism • Performance framework (including for changes in priority), retention/damages regime, performance security/guarantee, access/inspection/audit, oversight and step in, and agreed acceptable use policies for routine access • Term, termination and early termination fees; exit, including support for retendering and handover; any employee transfer issues and risks • Clear liability and insurance regime, including defect notification process and damage to property

Aspect	Issue to manage	Risk mitigation
Collaboration to resell third party data centre or cloud services	<ul style="list-style-type: none"> • Governance • Management of different players, joint ventures/partnerships/collaboration arrangements • Integration risk • Compliance risks • Antitrust risks (eg information sharing, any exclusivity or non-compete clauses and avoiding resale price maintenance) • Management of intellectual property rights 	<ul style="list-style-type: none"> • Clear governance framework, including planning, committees, procedures, investment requirements, notification and communication • Clear scope of appointment/collaboration, objectives, products/services, rights and duties, ability or otherwise to provide added features or services and make changes, and ownership and licensing of intellectual property rights • Resources, systems and processes needed to manage sales and marketing, delivery and relationships, and performance frameworks • Ensure risks are back-to-back or passed to third parties contractually and that there is a clear liability framework, including for misrepresentations to customers and non-performance • Legal/regulatory and other change management (including directions from regulators, relocation or withdrawal of services) • Term of collaboration, termination rights and consequences of termination (eg for existing arrangements)
Relationship with data centre or cloud end-customers	<ul style="list-style-type: none"> • Roles, responsibilities and critical performance objectives • Security and privacy requirements • Service management, failures and disaster recovery • Governance process including change management • Exit process • Charging model eg utility or banded pricing, potential premiums for additional capacity, and benchmarking 	<ul style="list-style-type: none"> • Clear scope to collocate or cloud service, support, upgrades, flexibility and additional capacity or excess usage • Service levels such as environmental controls, power, network, availability, uptime/downtime, outage, reboot, input/output, restore, processing, response, information persistence and automatic scalability • Clear liability regime including for key areas such as loss of data centre type/status/certifications and damage by other customers • Data segregation, security and protection/privacy, notice of breach and responsibility/liability for loss of data, protections relating to data permitted to be in the cloud • Audit and inspection (if applicable), monitoring, reporting and notification • Clear ownership of data or servers including in respect of insolvency risk, exit strategy eg data egress arrangements including costs and format; and any employee transfer issues and risks

How to move forward

To move forward on their data centre and cloud asset strategies, connectivity companies need to consider:

Broader strategy

- How their cloud strategy and business case fit with the organisation's strategy for the Internet of Things, enterprise and data/platforms.

Standardisation

- Consistent ways to describe services and associated terms, including their price.
- Standardised metrics, security, compliance, control points and risk management, policies and processes.

End-to-end risk

- A coordinated end-to-end process to manage customers and providers, including back-to-back management of integration risks.

Future proofing

- Future-proof facilities, infrastructure, technology and arrangements.

Disaster recovery

- Adequate disaster recovery and cyber security planning and responses.

Exit

- Supported and efficient exit processes



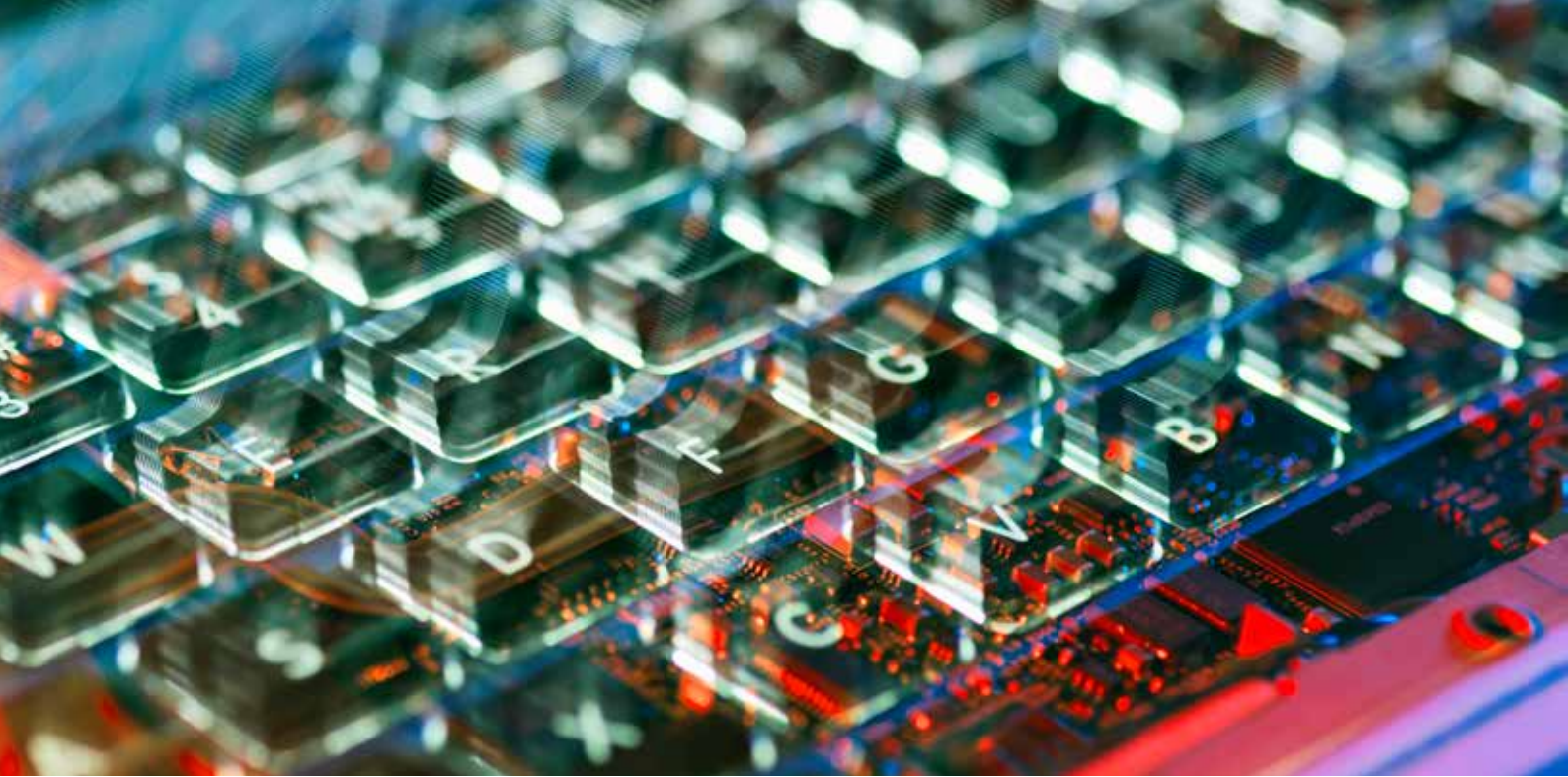
Case in point: Apple's data centres

Herbert Smith Freehills advised Apple on its US\$1 billion investment in Guizhou, a poorer province in southwest China earmarked for high-tech investment, which includes a new one million square feet data centre.

Services for Apple-device users residing in China will be shifted from data centres offshore to those run by GCBD, Apple's Chinese partner, on the ground in China. This will enable compliance with cyber security and telecoms laws in China and

improve customer experiences. Apple is the first major international technology company to set up such a large-scale data centre in China.

The project required negotiation and discussion with the local state-owned data centre company, the provincial government of Guizhou and also the Ministry of Industry and Information Technology (MIIT).



Security

With new digital assets, such as the Internet of Things and cloud, comes greater reliance on remote platforms and systems. Value chains become more interconnected and malevolent activity grows increasingly sophisticated.

The vast volumes of data that flow through connectivity providers' networks make them highly susceptible to cyber attacks. The more data they transmit and use, the more critical security and loss mitigation become a part of their customer value propositions.

In building up their own cyber resilience and investing in sophisticated preemptive defences, connectivity providers have amassed knowledge and expertise in keeping data, infrastructure and networks safe. That security expertise now has value outside the provision of core connectivity services.

IDC forecasts worldwide revenues for security-related hardware, software, and services will grow to US\$101.6 billion in 2020.

International Data Corporation

As a result, connectivity providers are identifying ways to capitalise on their cyber know-how in order to reconnect or build new relationships with both consumer and corporate customers, using data security services.

Some are bundling third-party security services as part of their connectivity packages. Others are developing standalone operations to deliver the latest innovations in cyber security services to third parties. There are also connectivity providers focused on identity and authentication services.

Security as a service is fast becoming a growth driver for connectivity providers and the trusted status reputations of traditional players put them in an advantageous position within the market.

Among other offerings, database scanning, information protection and payment compliance services allow customers to benefit from higher levels of vigilance across their activities.

Collaborate to strengthen the offering

Some connectivity providers, venturing into security as a service, have made acquisitions or investments; others have formed strategic alliances with cyber security providers, in order to strengthen their offerings.

Where complementary solutions are on offer from connectivity providers, security vendors, managed/outsourced security services providers and internet companies, the process of collaborating or pooling expertise can result in best-of-breed security solutions.

Alliances between providers create opportunities to leverage resources and reach billions of customers. They can share and compile information and intelligence on cyber threats; respond collectively and rapidly to threats; and create a more rigorous cyber security environment.

Other connectivity providers are opening engineering centres, security operations centres, research and development facilities, and cyber security institutes, to respond to online cyber assaults.

Other potential opportunities for collaboration include security of perimeters, network, endpoints, applications and data, as well as proactive policy management and reactive monitoring and response.

Protections to safeguard the organisation and customers

Providers that sit at the heart of the connectivity ecosystem have extensive networks and cloud infrastructures. From this central position, they are finding opportunities to improve revenues, reduce customer churn and enhance brands and reputations.

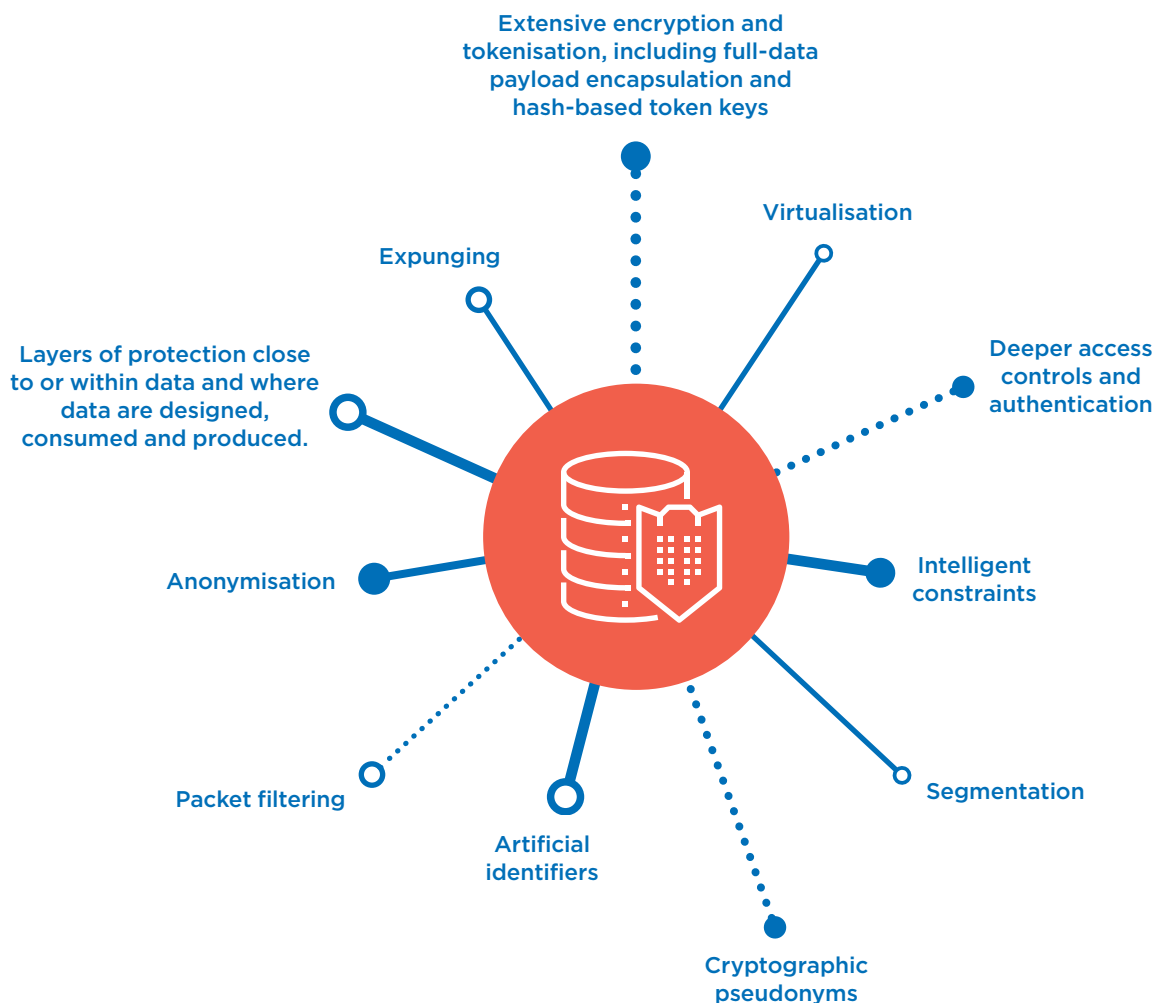
Those providers that operate in the cyber security space must protect critical information without limiting innovation and growth. In doing so, they need to consider investment, risk and user behaviour.

Sophisticated ways to monitor, model and interpret risk data and analyse vulnerabilities are in development. Statistics and machine learning can also be used to correlate customer data with breach data in order to draw meaningful conclusions and insights.

All architecture should be segmented, separated and layered. Advanced intelligence-led simulation testing, code analysis, malware checks and vulnerability assessments, with custom tools to target and exploit specific environments, can be used. Automated machine-learning and artificial intelligence also show promise when it comes to improved security.

Focus on protection of data

Security as a service is not just about protection of systems but is also about protection of data, and includes:



In developing cyber security solutions, providers need to be alert to legal and regulatory obligations including the following:

Area	Legal and regulatory considerations
Product/service development	<ul style="list-style-type: none"> • Processes for developing and maintaining products, including standards and certification requirements • Software vulnerabilities and security controls in the design, development and maintenance of the service package, including ongoing management • Security policy to apply to infrastructure, applications and systems • Software development and change management policies • Cryptographic key management systems and registration, including export controls • Governance of external parties: <ul style="list-style-type: none"> – vendor and partner risks – risk mitigation protocols in the supply chain – third-party risk management programmes
Service provision	<ul style="list-style-type: none"> • Scope of service across network, edge and endpoints, access, applications and cloud • Associated aspects and policies, including: <ul style="list-style-type: none"> – network, infrastructure/system, information access and personnel security – risk and information asset management – information asset management – data security and leakage prevention – access control, including managing internal and external access lists and authentication protocols and multi-level authentication – physical protections and separation – back-up and disaster recovery • Scope of support/maintenance and monitoring (logs, alerts and reports) • Vulnerability assessments and security training • Incident management/response requirements, notification requirements, including support to engage with regulators and law enforcement, customer compliance obligations, and ability to share information with relevant third parties • Staff experienced in safety science and cyber security protocols
Sales and marketing	<ul style="list-style-type: none"> • Avoid over-selling or misrepresenting the potential of cyber security defences or controls, to counter claims of misrepresentation • Third-party assessments and certifications may need to be carried out

Area	Legal and regulatory considerations
Contracts	<ul style="list-style-type: none">• Specify the extent of security within the services and consider whether or not any security-specific performance framework applies, or any security-related exceptions to other performance frameworks• Governance framework, including customer and supplier engagement• Consider responsibility/liability for loss of data or intellectual property, or other damage, from cyber attacks or unauthorised access; ensure liability is appropriately balanced and no further commitments are made to cover liability• Consider customer reporting and notification requirements, including compliance with legal/regulatory requirements• Allocate risk for changes in law/regulation appropriately• Pass risks to third parties, as appropriate
Insurance	<ul style="list-style-type: none">• Consider insurance cover/implications, eg payment of ransom• Prescribed tools, techniques and guidance of insurance companies

How to move forward

Connectivity providers' networks are the conduits via which other organisations' data are transmitted. There are financial, regulatory and reputational consequences for those providers that do not have sufficiently robust cyber defences in place to lessen the consequences of a security breach.

Where connectivity providers market their cyber security expertise to consumers or corporate customers, their defences and protocols for those services must be even more robust.

Strategy

- Assess the approach to proactive policy management and reactive monitoring and response, in relation to connectivity cyber risks.
- Consider how to offer security services to consumers and corporate customers, eg by bundling third-party security services or offering managed/outsourced security services
- Use standardised solutions for third-party aspects, to help mitigate integration risk.

Regulation

- Consider your contribution to the regulatory agenda. Regulation is likely to become more rigorous given the valuable nature of data and growing threat of attacks. More stringent penalties for non-compliance can be expected.
- Develop a plan to ensure you meet requirements, including regulatory or supervisory schemes covering cyber security, privacy and sector specific areas, data onshoring/localisation/sovereignty, impact assessments, confidentiality, breach reporting to regulators and individuals, access and audit, authentication, and protection of essential services.
- Security requirements tend to be risk-based, taking into account state-of-the-art standards, costs of implementation and the nature, scope, context and purposes of processing.
- Foreign investment authorities are particularly sensitive to cyber security-related businesses.

Risk

- Providers need to carry out rigorous assessments of physical and human weaknesses within their own networks and supply chains.

Workforce

- Consider how to find, retain and train scarce security talent.



Verticals

For connectivity providers, growth is under pressure and competition is intensifying, prompting their diversification into vertical or adjacent activities. The intention is to offer a broader range of products and services; to attract and retain customers and to generate new revenues.

Some connectivity providers have set up dedicated business units, innovation centres and venture capital arms in order to develop or access new areas. However, according to the World Economic Forum¹, these tend not to be as well funded as those set up by purely digital companies.

Others are looking at collaborative endeavours, which often involve partnering with third parties or entering into joint ventures. Connectivity providers bring network access, national scale, strong customer relationships, distribution channels and large data sets to the relationship. Third parties contribute technical expertise, resources and know-how in the adjacent activities. Collaboration with players in adjacent areas provides, therefore, opportunities to leverage combined skills and capabilities, innovate compelling products and services and achieve scale.

The search for adjacencies is prompting a rise in mergers and acquisitions and equity investment activity. Typically, transactions involve traditional players and non-connectivity participants.



They range from start-ups to large businesses, on both a local and global scale.

Evaluating adjacent market segments

Connectivity providers, when determining the most relevant market segments for diversification, must assess how they can best leverage their existing capabilities. They might explore:

- opportunities to build on network-resident intelligence, such as video on demand or mobile banking
- integrated applications and content servers, which interact with user devices over transparent communication connections, such as content delivery networks, or
- managed services, such as cloud computing or healthcare or medical technology, where system integration skills can be leveraged.

The table below illustrates the major diversification opportunities for connectivity providers.

Adjacency	Market opportunity	Legal and regulatory considerations
<p>Media and entertainment</p> 	<ul style="list-style-type: none"> • Multi-play offerings and ability to deliver content via multiple network channels, anytime, anywhere • Ability to control network delivery, and ensure quality and priority in delivery of content through intelligent policy controls • Builds on customer relationships and differentiate from other providers • Financing models, such as subscription services • Builds on data asset and exploitation and advertising opportunities 	<ul style="list-style-type: none"> • Media regulation in relevant countries, including licensing/authorisation, where required, and relevant telecoms regulation, eg net-neutrality; connectivity providers are already accustomed to operating in a regulated environment • Intellectual property rights, including rights clearance and royalties; content owners have concerns over piracy • Additional compliance requirements, eg consumer and content laws and regulations and privacy laws in relation to personal data • Intermediary liability • Competition and antitrust laws • Foreign investment restrictions and approvals in many countries
<p>Ecosystems and super-apps</p> 	<ul style="list-style-type: none"> • Online platforms that allow communities of users to connect by voice, messaging, pictures and video • Links users to services, content and providers without having to download multiple apps. Opens up a range of services using chatbots, plugins, artificial intelligence, in-platform search and industrial applications when rolled out to third party businesses and their customers • Attractiveness depends on reach, service, price, user-friendliness, additional features and openness to developers and service providers • Enables self-service or one-stop shop usage models and increases engagement with customers and differentiation and personalisation for customer acquisition and retention • Direct and indirect revenues can be achieved from new offerings and business paradigms. Builds on data asset and exploitation opportunities, including user profiles and access to the customer, and advertising opportunities 	<ul style="list-style-type: none"> • Regulation of internet messaging (often less heavily regulated than communications) • Integration risk and responsibility for third-party elements; fraudulent or similar activity; intermediary liability • Additional compliance requirements, eg consumer and content laws and regulations and privacy laws in relation to personal data, information sharing and rights of publicity • Intellectual property rights, including licensing and tracing • Safety/security/cyber security issues, including lawful intercept, security services and onshoring/localisation/sovereignty • Competition and antitrust laws • Foreign investment restrictions and approvals in some countries

Adjacency	Market opportunity	Legal and regulatory considerations
<p>Financial services</p> 	<ul style="list-style-type: none"> • Opportunity to sell digital financial services utilising network, customer data, and authentication aspects • Trend for financial services providers to move customer interactions onto mobile platforms and the opportunity to reduce costs • Collaborations with issuers, acquirers, merchants and fintech companies • Given the scarcity and compliance requirements of financial services licences, connectivity providers with financial services licences have substantial opportunities • Extends brand and offerings with increased engagement and differentiation opportunities and builds on data asset and exploitation opportunities, including user profiles and access to the customer 	<ul style="list-style-type: none"> • Financial services regulation in relevant countries, including licensing/authorisation, where required; connectivity providers are already accustomed to operating in a regulated environment • Responsibility for third-party aspects, fraud or similar activity • Additional compliance requirements, eg consumer and anti-money laundering laws and regulations and privacy and secrecy laws • Safety/security/cyber security issues • Foreign investment restrictions and approvals in many countries
<p>Healthcare</p> 	<ul style="list-style-type: none"> • Software applications, platforms, data, analytic and security services, relating to diagnostics and treatment. Opportunity in general practitioner, pharmacy, hospital, primary, diagnostic, radiology, aged, residential, disability and community care sectors, as well as with government agencies and insurance companies • Diagnosis information can be reported directly to healthcare practitioners, in real-time, over mobile devices. This saves time and money and enables appropriate interventions without direct physical contact • Future connectivity, such as 5G, will enable innovations, including remote/robotic surgery • Patient and healthcare provider benefits include: increased convenience; lower costs; greater choices; better experiences; increased productivity and efficiency; integrated information; increased access and safety; reduced patient admissions and greater control • Extends brand and offerings with increased engagement and differentiation and builds on data asset and exploitation opportunities, including user profiles and access to the customer 	<ul style="list-style-type: none"> • Health regulation in relevant countries, including licensing/authorisation, where required • Integration risk and responsibility for third-party elements, fraud or similar activity • Additional compliance requirements, eg consumer and safety laws and regulations and privacy laws in relation to personal data and information-sharing, particularly given sensitive nature of healthcare data • Safety/security/cyber security issues • Foreign investment restrictions and approvals in many countries

Adjacency	Market opportunity	Legal and regulatory considerations
<p>Fixed-mobile convergence (FMC)</p> 	<ul style="list-style-type: none"> • The convergence of fixed-line and mobile means the network becomes secondary to the services allowed by collaborative endeavours • FMC enables cost reductions and efficiencies, better broadband coverage, as well as revenue potential. The connectivity provider offers more of the end-to-end delivery, which can be used and managed more efficiently • Allows for a 'multi-play' service, that bundles fixed-line, mobile, broadband and TV and home-life in a single package, delivered over wired and wireless networks • Differentiates against pure-play providers, tending to result in lower churn, and allows for improved product development, strategic marketing and customer-experience management • Longer term, given the rollout of 5G, FMC players will be able to optimise the transmission of all data, voice and video communications between users, irrespective of device or location and enter into new business areas in the Internet of Things and the world of 5G 	<ul style="list-style-type: none"> • Regulation of fixed and mobile, which may be different in some countries; regulation of prices and impact on bundling strategy; media and content issues/regulation • Competition and antitrust issues • Foreign investment restrictions and approvals in many countries • Integration risk and responsibility for third-party aspects • Rights to deliver across all platforms/technologies • Privacy laws in relation to personal data and information sharing

Challenges in diversification

By diversifying from connectivity into content or services, providers will have to adapt to a new world of regulation and compliance requirements, market practices and intellectual property and privacy protections.

Connectivity providers will need to rethink corporate structures and decide whether to hive off vertical or adjacent activities into standalone businesses or take minority positions, so as to ring fence risk and not stifle independent innovation. Indeed, separation might be a condition for collaboration or investment.

In collaborative endeavours each participant must have a clear understanding of roles. They also need to focus on the strategic threats and potential opportunities that come with part-ownership of a larger business. These may prove far more valuable than outright ownership of small, non-collaborative businesses.

Inevitably, there will be workforce challenges. Connectivity providers will need to attract the right calibre of people if they are to make the transition into new competencies and make themselves more attractive to digital-native employees and customers.

Diversification and collaboration likely to give rise to more disputes

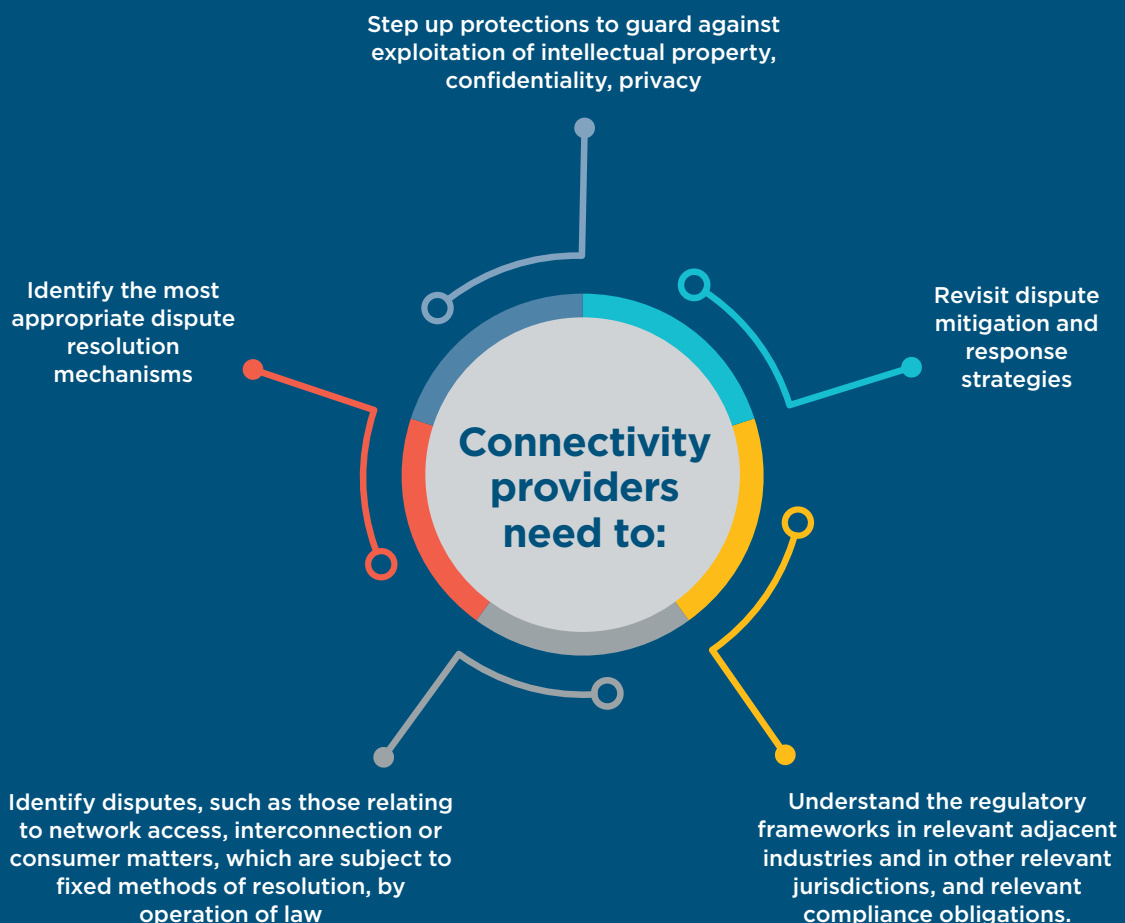
While the number of disputes arising in the telecoms sector has tended to be very high, compared with for instance the IT sector, resolution is typically by way of negotiation or mediation, rather than litigation or arbitration.

Now that the pace of innovation and diversification across the competitive landscape has stepped up, there is likely to be a corresponding hike in disputes. New services and products, competition for content, services and customers, the abundance and value of data seem forecast to change the nature, frequency and scope of disputes very significantly.

Increased collaboration, by way of joint ventures, mergers and acquisitions, investments, partnerships and tie-ups with other connectivity providers and businesses in adjacent or vertical activities, will give rise to clashes between parties. Matters such as breaches of agreements or infringement of various rights are all very likely to contribute to increased tensions and necessitate some form of resolution.

Competitive differentiation within an increasingly crowded market, in which connectivity providers search for new ways to deliver services and products to a more discerning and fluid customer base, is also likely to fuel disputes. Issues relating to intellectual property, copyright and patent infringement, as well as brand and reputational matters and trade secrets, confidentiality and privacy, will become increasingly common battle grounds.

So as the connectivity industry undergoes a very significant shift from its traditional model and experiments with new ventures and new markets, it will expose itself to increased risk. Although mediation and negotiation may continue to be the most appropriate settlement strategies for matters relating to commercial relationships, and adjudication and litigation best suited to intellectual property and data disputes, there is likely to be an increase in cases requiring international arbitration remedies too.



Collaborative investment models

Typically, collaboration or diversification strategies involve equity investment, partnering, joint ventures or acquisitions. Whichever model they pursue, there are a number of considerations that connectivity providers must address in order to minimise risk and maximise opportunities.

Model	Most appropriate for...	Pros	Cons
<p>Equity investment</p> <p>Minority investment in stock/shares, including as part of an equity-funding round or by venture capital, corporate venturing or private equity.</p> <p>This is a medium-risk option.</p>	<ul style="list-style-type: none"> • Gaining knowledge about the investee company's business area • Negotiating strategic commercial arrangement with the investee company, leveraging one or both parties' capabilities • Potential growth and financial returns 	<ul style="list-style-type: none"> • Usually, some information rights can be negotiated including visibility of product roadmap and trials/pilots • Commercial arrangements may be on preferential terms • Possible capital gains, if not dividends • May be an option to acquire at a later date 	<ul style="list-style-type: none"> • Dilution risk; down-round price risk, but can be protected against • Exit may be difficult, eg transfer restrictions or limited market/price • Limited governance rights and certain investors may have significant rights and protections, such as liquidation and dividend preferences, veto/approval rights and rights to drag other investors on a sale • Recourse is against the investee company • Complexities around non-compete clauses; regulatory and competition/antitrust/foreign investment clearance may be required • Commercial agreements needed for relevant aspects; intellectual property and other rights may remain with the investee company
<p>Partnering</p> <p>Strategic 'partner' arrangement.</p> <p>This is a low- to medium-risk option.</p>	<ul style="list-style-type: none"> • Connectivity providers collaborating with one another • Collaboration between connectivity providers and other providers or players 	<ul style="list-style-type: none"> • Vendor independent solutions • Generally simple/quick to establish, integrate and unwind • Allows for research and development, trial and agile arrangements • Regulatory and competition/antitrust compliance generally not required • Clear intellectual property rights and licenses • May be possible to negotiate exclusivity, restriction on use or similar rights 	<ul style="list-style-type: none"> • Less information or knowledge sharing by the partner; difficult to share data, due to privacy laws and affirmative consent requirements • More difficult to shape partner-solution roadmap • Integration risk, particularly when dealing with a number of different players • Change of control risk • Exit risk • May require flexible arrangements eg rights to adapt or develop

Model	Most appropriate for...	Pros	Cons
<p>Incorporated joint venture</p> <p>For the purposes of the collaboration, which may be a special purpose vehicle/greenfield joint venture.</p> <p>This is a medium- to high-risk option.</p>	<ul style="list-style-type: none"> • Connectivity providers collaborating with one another • Collaboration between connectivity providers and other providers or players 	<ul style="list-style-type: none"> • Easier to shape partner solution roadmap • Shared capital gains and any dividends • Information rights • Governance rights • Commercial arrangements may be on preferential terms • Competition/antitrust compliance is likely to be easier • Recourse against other shareholders 	<ul style="list-style-type: none"> • May be difficult/slow to establish and unwind • Shared control and difficulties in acquiring at a later date • Complex intellectual property rights and licences • Complexities around non-compete clauses; may need regulatory and competition/antitrust clearance • Agreements for asset transfers and shared services may be required
<p>Acquisitions</p> <p>Acquiring a vertical/ adjacent company/ business eg content or services.</p> <p>This is a high-risk option.</p>	<ul style="list-style-type: none"> • Connectivity providers looking to refocus the business eg mobile operators moving towards services/content • Potential growth and financial returns 	<ul style="list-style-type: none"> • Control over solution roadmap • Capital gains and any dividends • Information and governance rights • Commercial arrangements on intra-group terms • Recourse against seller for a period 	<ul style="list-style-type: none"> • Greater up-front capital or financing eg control premium • May be difficult/slow and cost more to transact • Regulatory and competition/ antitrust/foreign investment clearance may be required • Business integration risks, eg use of data or intellectual property • Difficult to unwind • May require transitional services



How to move forward

When moving into vertical or adjacent lines of business, connectivity providers need to consider a number of implications:

Financial

- How to increase customer satisfaction and loyalty and reduce churn.
- How the adjacency will perform given both internet/digital players and other competitors.

Risk/compliance

- How to leverage and monetise data while remaining compliant with data protection and privacy laws.
- How laws and regulations might change as a consequence of diversification.
- Changes in risk profile and impact on insurance and compliance.

Structure

- Best structure – eg investment, joint venture, merger or acquisition, partnership or collaboration – to achieve growth in adjacent businesses.
- How to leverage marketing and sales synergies from convergence/verticals/adjacencies.
- How to achieve relevant network and cost efficiencies.
- How to achieve relevant synergies and enhance margins.

Future-proofing

- How to attract and retain expertise to develop products and services.
- How to attract strategic and financial investors or lenders and to gauge risk-versus-reward appetite.



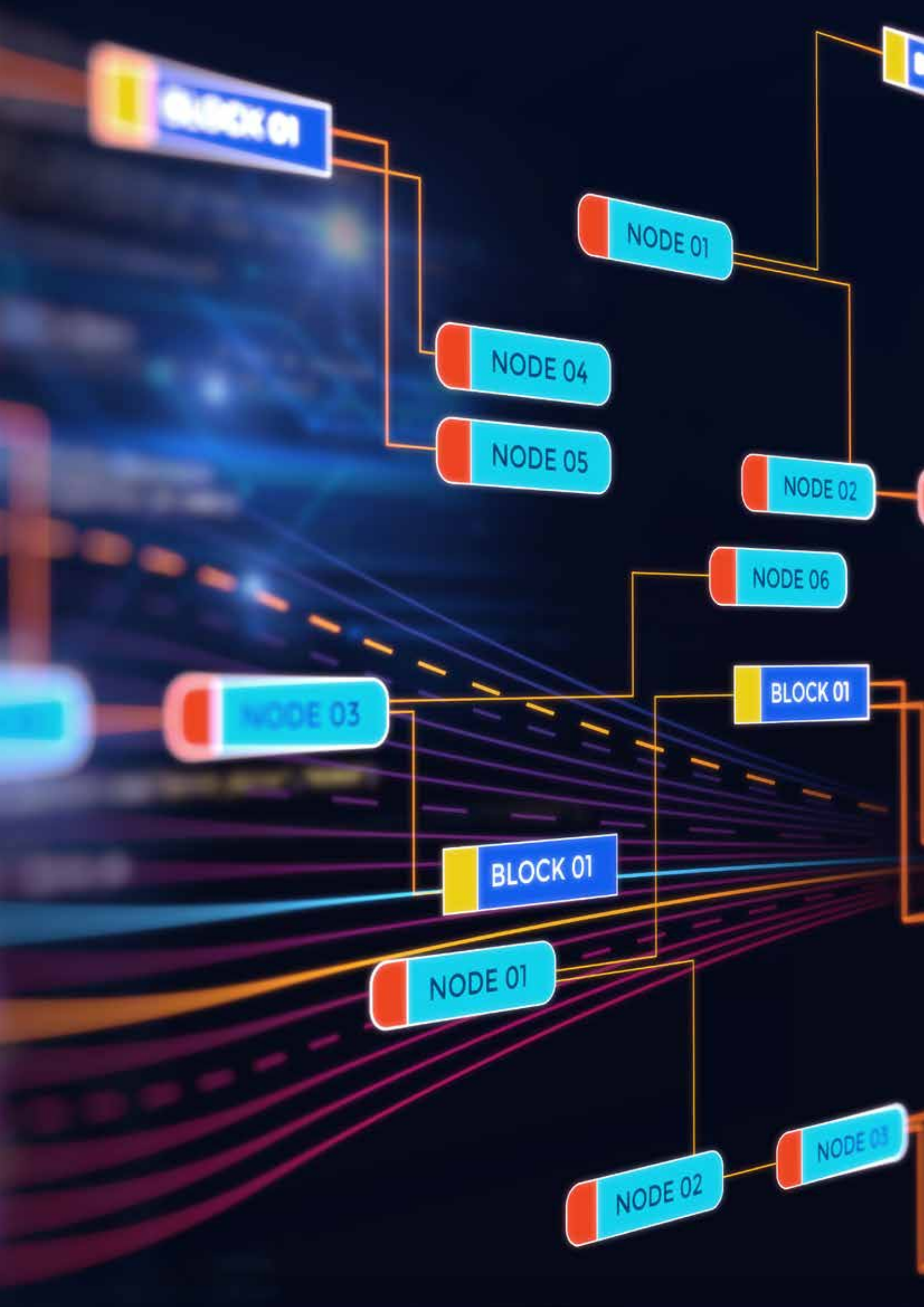
Case in point: AT&T Time Warner

AT&T agreed to acquire Time Warner in a stock and cash transaction valued at US\$108.7billion, including Time Warner's net debt.

The acquisition is expected to lead the next wave of innovation in converging media and communications industries and create

new customer choices – from content creation and distribution to a mobile-first experience that is personal and social.

Herbert Smith Freehills advised Time Warner of non-US aspects of this transaction, including successfully obtaining EU competition/antitrust approvals.



Big data

Now more than ever before connectivity providers need to adapt their mindset and exploit the value inherent in the vast amounts of data to which they have access.

From signing up for a service, through to how they use it on a daily basis, customers leave behind a trail of data, usually for free, that holds valuable clues about their individual habits. So far, connectivity providers have done very little to monetise their data assets.

Internet companies, by contrast, dominate the digital economy with their smart collection, interpretation and use of data.

Connectivity providers have been hesitant to participate in data monetisation for several reasons. They are culturally and traditionally more averse to risk taking than their nimbler and more dynamic internet rivals. They are limited by geographic focus, unlike those that operate over the borderless internet. And the flow of information between connectivity providers and their customers is, for the most part, anonymous or private. It goes very much against the grain to capitalise on personal data and put the trusted provider-user relationship at risk. Connectivity providers are governed by strict rules, regulations and standards on data interception and confidentiality.

To turn the tide on declining revenues, connectivity providers are now entering data exploitation and monetisation territory, albeit cautiously. They are turning to powerful data analytics and artificial intelligence tools to mine valuable insights and to identify ways to improve their offerings and diversify into new business activities. In this way, they aim to preserve or increase revenues, add value and improve customer acquisition and retention.

They are making an impact with:

- more data-enabled, personalised and diversified services to customers
- offerings based on big data analytics, and
- collaborations with other providers to deliver data-driven services.

Collaboration for growth

Collaboration opens up possibilities for exploitation and monetisation of big data and diversification beyond mainstream services and geographies. It offers connectivity providers a way into value add, revenue building activities that could win or retain customer loyalty.

Collaboration can include engagement with other connectivity providers or interactions with advertising players, platforms, service providers and recipients, to deliver more compelling offerings.

Data are now among the most valuable commodities in the world. By 2026, the market is predicted to be worth around US\$92 billion globally.

Wikibon Worldwide Big Data Market Forecast

By collaborating with a player from another region or country, connectivity providers can leverage local understanding of the culture, language, regulation and behaviours. This insight from localised data allows them to command a premium for services that are specifically tailored to the audience.

Given their significant data assets and reputation for proper handling of customer data, connectivity providers are well placed to enter into collaborative arrangements with suitable partners. Across the sector there is a growing trend for transactions, including strategic partnerships, joint ventures and mergers and acquisitions, to capture these opportunities.



Three key strategies for monetising data

Advertising

Advertising is a key monetisation opportunity for connectivity providers. It opens up both new sources of revenue and opportunities to subsidise cheaper connectivity services. Many large connectivity providers have made substantial investments in the advertising space.

Success will depend on connectivity providers' ability to analyse data so they can push relevant adverts to consumers, based on known preferences, interests and locations.

There are opportunities for connectivity providers to:

- provide analytics platforms to support advertisers, agencies, media, platforms or publishers
- actively track consumers' digital footprints, using, where possible, deep-packet inspection to filter metadata and deduce, more accurately, user behaviours and preferences, and deliver targeted advertising, and
- share data with or source it from third parties.

Monetisation opportunities exist for connectivity providers that leverage emerging technologies to enable more targeted advertising than ever before. By drilling down into data to better understand reactions to and interpretations of advertisements, they will improve the chances of reaching the right audience, with the right product, at the right time, in order to elicit a positive response.

Case in point: Diversification into digital advertising

Herbert Smith Freehills advised a telecoms client on the formation of a digital advertising technology company.

The business specialises in using diverse sources of data to place strategic ads and to help brands reach audiences with the right content, at the right moment and in the right place.

The company analyses data to make informed decisions about how to spend marketing budgets wisely. This includes integrated offerings across major social media channels, such as Facebook, Instagram, Twitter and YouTube, as well as over mobile platforms.

Return on investment is achieved by way of advanced data analysis; targeting algorithms; campaign optimisation; monetised data; and preferred relationships with major social media networks.



Authentication

In most countries, connectivity providers, or their agents/dealers, run through know-your-customer and money-laundering protocols when signing customers up to their services. They collate customer data on identity, residence, banking eg there are a number of connectivity providers investing into digital identity and verification.

This store of customer identification data, plus the trust implicit in their regulated status, makes connectivity providers ideal intermediaries, or gateways, between providers of services and customers. By seamlessly authenticating customers who sign up for apps, pay to park, or use mobile shopping or banking, there are fewer abandoned purchases, as well as monetisation opportunities for connectivity providers. Many offer digital certificate management, cryptographic key exchange and mobile identity services.

It is evident that authentication services have a growing relevance in a world where more and more of our interactions take place online and where our cyber identities become an extension of our real selves.

By adding more unique data identifiers, such as biometrics, and by exploiting the potential that blockchain offers, connectivity providers can make it more difficult for malevolent actors to falsify identities or bypass security checks. There may also be opportunities for connectivity providers to manage and act as repositories for users' preferences about how their data can be used.

Authentication represents a particularly valuable monetisation opportunity that connectivity providers can exploit.



Data broking

The internet gives a global audience access to content and applications. As more people participate, as connectivity becomes limitless and as the value chain of traditional industries are restructured, there is greater opportunity to build platforms and data marketplaces. To date connectivity providers have not embraced collecting and selling data in the same manner as many internet and digital companies.

Platforms bring together distinct but interdependent groups and allow automated interactions to take place between them. The exchange of data, or capabilities, across the platform has the potential to become the de facto ecosystem by which parties connect or conduct business. The ecosystem becomes a communication channel in its own right and generates its own enormous volumes of valuable data.



Case in point: Digital authentication services

Working with GSMA, the leading mobile association that comprises around 800 telecoms operators and more than 300 companies in adjacent businesses, Herbert Smith Freehills advised on a digital identity programme.

GSMA developed Mobile Connect, a universal log-in solution that enables secure but convenient online interactions. Mobile Connect provides authentication, authorisation and verification capabilities over a standardised, technical interface. It screens users by matching them to the SIM on their mobile phone. As it eliminates the need for rigorous authentication processes, users do not need to remember passcodes and it reduces abandoned online shopping carts and increases sales.

GSMA is working with leading mobile operators globally, as well as with other ecosystem parties, such as governments, banks and retailers in some countries, to roll out mobile-enabled, digital identity solutions.



Case in point: Cloud-ready platform for mobile operators

Herbert Smith Freehills advised a telecoms company setting up a collaborative cloud-ready platform. It allows mobile network operators to establish an agile collaboration layer that uses web-centric application programming interfaces.

The platform is based on scalable, open-source enterprise solutions. It enables multiple telecoms companies to expose, manage and orchestrate a range of network services at a fraction of the cost of legacy systems.

It facilitates contextual digital services to customers and partnering opportunities. Customers, partners, internal and external systems and services can be quickly integrated into a connected, adaptive and collaborative business ecosystem.

Use cases include billing, advertising, e-money, e-health, e-government, and machine-to-machine interactions.

How to move forward

Connectivity providers, as they seek to reinvent themselves by moving into new ventures, must be mindful of the risks that go hand in hand with exploiting and monetising data assets.

By implementing robust governance strategies, they will be better equipped to guard against regulatory interventions and penalties, private legal actions and, most significantly perhaps, loss of trust and damage to brand and reputation.

Connectivity providers must pay particular attention to:

Regulation

- Regulation, which is unlikely to soften, especially given the mounting value attached to data and high-profile cases of data breaches, loss or misuse.
- More stringent requirements and severe sanctions being introduced in many countries.
- Sector regulations that may apply, such as financial services regulations for payment-related gateway activities.

Privacy

- Customers who have growing concerns about privacy and the potential misuse of their data. Getting the individual's prior consent to use personal information is crucial, especially where the level of intrusion is significant or the data are sensitive.
- Reputations for trust, which are built where privacy is handled well. This needs to be extended to new relationship models, which enable customers to manage their digital experiences and control the data generated by using connectivity providers' products and services in a transparent and secure manner.

Authorities

- The increasing number of transactions that are either investigated or blocked, highlighting the concerns of antitrust and foreign investment authorities about the integrity, treatment, use and security of data.
- Illegal activities involving data access or use, which are on the rise, including in respect of unfair competition and consumer protection violations.
- Data with national security and critical infrastructure relevance being flagged as strategically important and subject to scrutiny.

Rights

- Rights to data as they are not clear cut. Some elements of law relating to intellectual property, confidentiality and trade secrets apply. Much rides, however, on contractual rights, including consents, which can be difficult to trace.
- Difficulties in verifying ownership or use rights that complicate processing, exploiting, pooling, valuing and managing big data.

Other laws

- Consumer, advertising and content laws and regulations which shape big data activity.
- In some countries, data governance being restricted by onshoring/localisation/sovereignty requirements, government scrutiny or law enforcement access.

Intermediary liability

- Responsibility for data and content needing to be managed robustly.
- Connectivity providers, like internet companies, who may claim to be pure intermediaries in order to escape liability. This status needs to be re-examined as connectivity providers exploit data to greater extents.

Other issues

- Demand for talent increasing as expertise in areas such as data science is sought.
- Access to and storage of increased volumes of data which mean data centre arrangements and cyber security protocols must be enhanced.
- Where data are to be exploited to release their full value, more robust management of the information lifecycle being essential.



Conclusion

Legacy systems and processes, investment cycles, fixed-cost structures and competitive threats frustrate growth and profitability for conventional telecoms companies.

In adopting new strategies and business models for the digital age, providers of connectivity are now leveraging their networks, reputations and know-how to attract and retain customers. They are focused on delivering distinctive products, services and experiences and reinventing the very essence of what they do in order to serve tomorrow's switched-on and expectant users.

However, with transformation comes exposure to new sorts of risks that have to be managed if connectivity providers are to navigate and secure a place in our multi-trillion-dollar, ultra-connected future. Those that harness the benefits of reinvention through diversification and collaboration will succeed.

Expand into vertical or adjacent sectors

particularly those that play to their strengths in network services, resident intelligence, application and content servers and managed services.

9

Develop a clear strategy and business plan

that sets out their direction and goals for managed services, platforms, applications, data, and new products and services

8

Leverage their unique strengths,

such as trusted reputations and strong engineering ethos, to secure a foothold in the digital market.

7

Actively advocate for standards, rules, laws and regulations, as well as for tax and other concessions, that will promote investment and efficiency.

Embrace innovative, creative and collaborative models by harnessing their existing infrastructure while investing in new technologies, such as 5G, IoT and cloud/data centres/edge computing.

Invest more of their revenues in the customer experience as digital companies do, to generate greater returns.

Be more open to leveraging and exploiting big data.

Embrace and nurture their next generation workforces, technologies and processes with the backing of committed and determined management, boards and shareholders. Carefully manage existing workforces and re-training or reorganisation, and short-term and contract-workers.

Promote collaboration, innovation, disruption, experimentation and agility which will enhance speed, scale, efficiency, flexibility and profit. It will develop skills and capabilities, while encouraging localisation, standardisation and interoperability..

Expedite the digitalisation of networks and IT
This will enable new product and service innovation and, ultimately, enhance the customer experience and, in turn, profits.

10

1

2

3

4

5

6

Tomorrow's connectivity providers will:

How our team can help

The Technology, Media and Telecommunications (TMT) sectors are experiencing significant change; creating great opportunities and posing equally great challenges.

Few other industry sectors are as fluid, and few have the capacity to change businesses, or indeed society, as quickly or profoundly. Recent years have seen waves of disruptive technologies emerging, and we expect the relentless digitisation of traditional industry sectors and business types to continue to change the way businesses think and operate, and how they are put together.

We are helping our clients on this odyssey. We are helping them to frame their opportunities and navigate the challenges. We are there with our clients when they are engaging in their most complex,

market-defining, 'first of a kind' deals, and when they are managing their most difficult, unexpected, 'first of a kind' challenges.

With unrivaled expertise and extensive resources across the globe in these sectors, we are able to provide practical, informed, sensible solutions. Our sector expertise is backed by strong practice expertise, including our award winning transactional, regulatory and disputes teams.

These sectors are giving rise to great opportunities and great challenges: we are there with you.

For further information, please visit www.herbertsmithfreehills.com

GLOBAL LEADERS



Damien Bailey
Partner
Sydney
T +61 2 9225 5545
damien.bailey@hsf.com



Mark Robinson
Partner
Singapore
T +65 68689808
mark.robinson@hsf.com



Aaron White
Of Counsel
London
T +44 20 7466 2188
aaron.white@hsf.com



Frédéric Bouvet
Partner
Paris
T +33 1 53 57 70 76
frederic.bouvet@hsf.com



Julian Lincoln
Partner
Melbourne
T +61 3 9288 1694
julian.lincoln@hsf.com



Veronica Roberts
Partner
London
T +44 20 7466 2009
veronica.roberts@hsf.com



Liza Carver
Partner
Sydney
T +61 2 9225 5574
liza.carver@hsf.com



Nicolás Martín
Partner
Madrid
T +34 91 423 4009
nicolas.martin@hsf.com



James Robinson
Partner
New York
T +1 917 542 7803
james.robinson@hsf.com



David Coulling
Partner
London
T +44 20 7466 2442
david.coulling@hsf.com



Rebecca Maslen-Stannage
Partner
Sydney
T +61 2 9225 5500
rebecca.maslen-stannage@hsf.com



May Tai
Partner
Hong Kong
T +852 21014031
may.tai@hsf.com



Gavin Davies
Partner
London
T +44 20 7466 2170
gavin.davies@hsf.com



Zubair Mir
Head of Middle East
Dubai
T +971 4 428 6303
zubair.mir@hsf.com



Sönke Becker
Partner
Düsseldorf
T +49 211 975 59071
soenke.becker@hsf.com



Rudolph du Plessis
Partner
Johannesburg
T +27 10 500 2623
rudolph.duplessis@hsf.com



Graeme Preston
Partner
Tokyo
T +81 3 5412 5485
graeme.preston@hsf.com



Edouard Thomas
Partner
Paris
T +33 1 53 57 72 14
edouard.thomas@hsf.com



Pablo García-Nieto
Partner
Madrid
T +34 91 423 4023
pablo.garcia-nieto@hsf.com



Olga Revzina
Partner
Moscow
T +7 495 78 37370
olga.revzina@hsf.com



Juliana Warner
Partner
Sydney
T +61 2 9225 5509
juliana.warner@hsf.com

HERBERTSMITHFREEHILLS.COM

BANGKOK

Herbert Smith Freehills (Thailand) Ltd

BEIJING

Herbert Smith Freehills LLP
Beijing Representative Office (UK)

BELFAST

Herbert Smith Freehills LLP

BERLIN

Herbert Smith Freehills Germany LLP

BRISBANE

Herbert Smith Freehills

BRUSSELS

Herbert Smith Freehills LLP

DUBAI

Herbert Smith Freehills LLP

DÜSSELDORF

Herbert Smith Freehills Germany LLP

FRANKFURT

Herbert Smith Freehills Germany LLP

HONG KONG

Herbert Smith Freehills

JAKARTA

Hiswara Bunjamin and Tandjung
Herbert Smith Freehills LLP associated firm

JOHANNESBURG

Herbert Smith Freehills South Africa LLP

KUALA LUMPUR

Herbert Smith Freehills LLP
LLP0010119-FGN

LONDON

Herbert Smith Freehills LLP

MADRID

Herbert Smith Freehills Spain LLP

MELBOURNE

Herbert Smith Freehills

MILAN

Studio Legale Associato in association with
Herbert Smith Freehills LLP

MOSCOW

Herbert Smith Freehills CIS LLP

NEW YORK

Herbert Smith Freehills New York LLP

PARIS

Herbert Smith Freehills Paris LLP

PERTH

Herbert Smith Freehills

RIYADH

The Law Office of Nasser Al-Hamdan
Herbert Smith Freehills LLP associated firm

SEOUL

Herbert Smith Freehills LLP
Foreign Legal Consultant Office

SHANGHAI

Herbert Smith Freehills LLP
Shanghai Representative Office (UK)

SINGAPORE

Herbert Smith Freehills LLP

SYDNEY

Herbert Smith Freehills

TOKYO

Herbert Smith Freehills