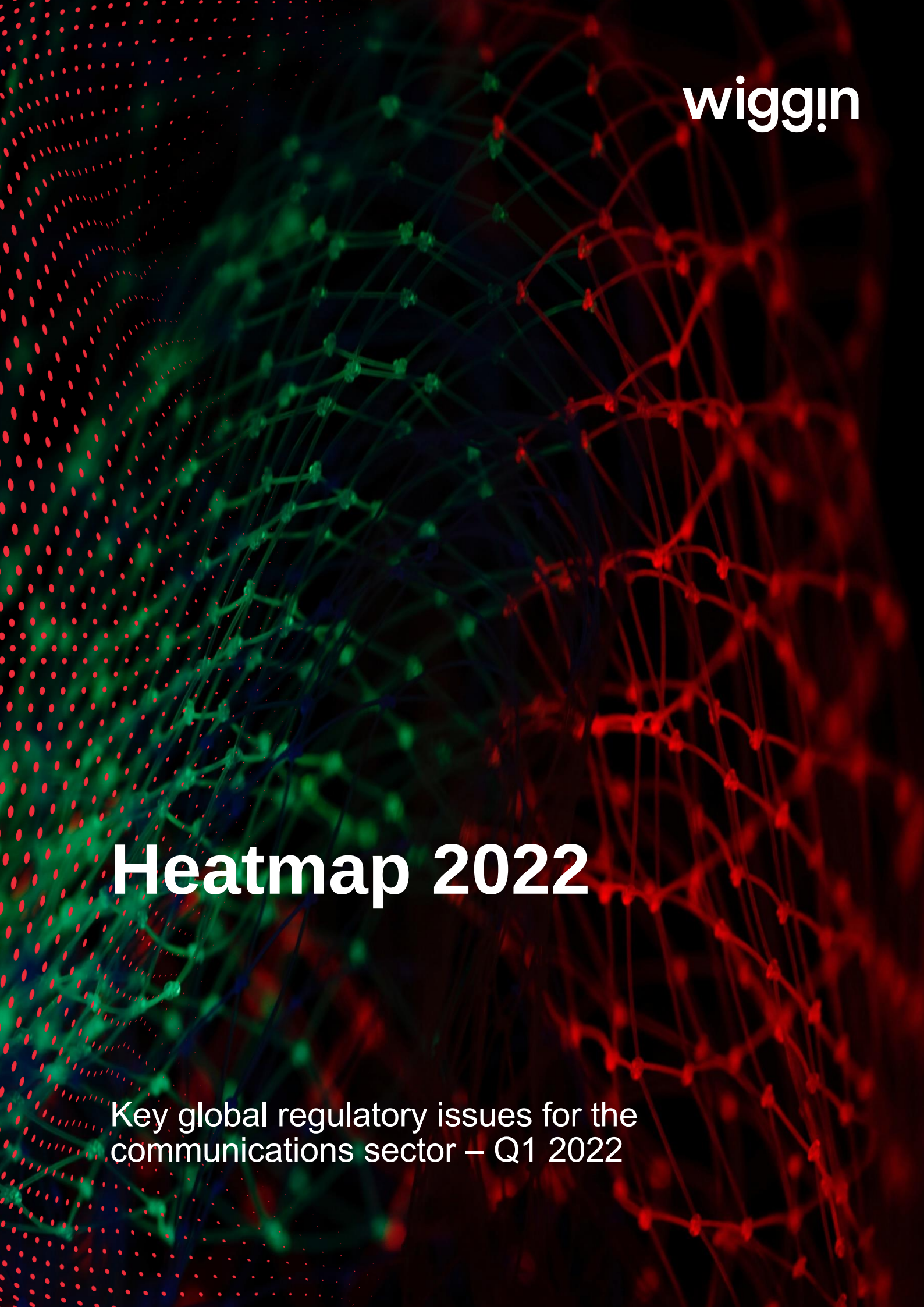

wiggin
Heatmap 2022
Key global regulatory issues for the communications sector – Q1 2022

wiggin

Topics

The digital world is forever evolving - our team of experts have developed this guide to help highlight the key global regulatory issues we see facing the communications sector in 2022.

wiggin

National Security Network and Supply Chain measures - increasing legislation and 'localisation' requirements: implications for TMT providers

In 2021, a number of important security requirements developments were introduced for telecoms networks and services. Ensuring the security of supply chains has been a top priority, with various measures introduced to tackle high-risk vendor concerns and ensure certain key activities are provided locally.

Global overview

The increased risk of cyber threats to national security has recently resulted in legislation imposing stricter security requirements for telecoms service and network providers, with several tough sanctions for non-compliance. Measures have included steps such as banning or controlling the access of certain high-risk vendors from markets due to security risk concerns (particularly in relation to the roll out of 5G – e.g., in Poland and the UK). Obligations requiring the 'localisation' of certain core telecoms activities deemed necessary for conducting an electronic communications business have also increased, representing important restrictions to cross-border provisioning of services (for example, in Belgium or Switzerland). Such trends have been evident around the world and could be extended further in 2022. We examine a few of them in more detail below.

UK

In the UK, telecoms security has been a major recent focus for government. In November 2021, the UK introduced a new security regime for telecoms networks and services under the Telecommunications (Security) Act 2021[1,2]. These rules represent one of the biggest changes to the operating environment for communications providers in the UK in recent times – and aims to introduce one of the toughest network security regimes in the world. Specific measures have also been introduced to address high risk vendor concerns, including a government ban on Huawei supplying new equipment for UK 5G networks (since 31 December 2020) and a requirement that all existing Huawei equipment be removed from the UK's 5G networks by the end of 2027. Another policy objective of the new regime has been to ensure that appropriate protections are in place to ensure that sufficient knowledge, capability, and data should reside locally in the UK to ensure the security and resilience of the network.

The extent and gravity of the new security obligations and the potential sanctions combined with recent changes to the merger regime for communications providers means that multinational communications providers need to

[1]Telecommunications (Security) Act 2021 of 17th November 2021 including the corresponding secondary legislation See full package of security measures at https://www.gov.uk/government/collections/telecommunications-security-bill.

[2]https://www.legislation.gov.uk/ukpga/2021/31/contents/enacted; https://www.ofcom.org.uk/news-centre/2021/ofcom-oversee-telecoms-networks-security.

carefully assess the impact on their existing operations and any potential market entry.

The new UK Act covers the following main categories of new obligations and powers for the Government and Ofcom:

1. Strengthened legal security duties for telecoms network and service providers the UK: providers will face severe penalties for non-compliance with their security duties (including a fine of up to 10% of their relevant turnover, or (in the case of a continuing contravention) a fine of up to £100,000 a day.

2. Stricter information gathering requirements: If, following an Ofcom request, a telecoms provider fails to provide information or refuses to explain a failure to follow a new telecoms security code of practice for industry[3] Ofcom can impose a fine of up to a maximum of £10 million, or in the case of a continuing failure to do this, £50,000 per day.

3. New Ofcom responsibilities to monitor, report to government and enforce compliance with the new UK telecoms security regime.

4. New powers for the Government (Secretary of State) to control the extent to which high risk vendors can provide equipment to be used in telecoms networks (to protect national security). This can include requiring telecoms networks to remove existing network equipment that has been sourced from the high-risk vendors concerned.

EU

While the European Electronics Communications Code (the EECC) has, since 21 December 2020, required security measures to as a minimum, consider all the relevant aspects of certain elements in areas such as security of networks and facilities, handling of security incidents, business continuity management, monitoring, auditing and testing as well as compliance with international standards, some aspects are out of scope. In particular, the EECC lacks provisions directly applicable to network equipment manufacturers and other service providers in the electronic communications supply chain. EU national regulators have therefore responded by introducing national security supply chain measures of their own. Recent EU member state network security developments include:

- **Austria**

  The Austrian Telecommunications Act entered into force on 1 November 2021, with a focus on technological telecoms advances such as 5G. The Act includes network security measures such as supply chain requirements for high-risk suppliers of telecoms hardware.

- **Belgium**

  In November 2021, BIPT (the Belgian National Regulator for electronic communications) consulted on new localisation and security requirements for 5G networks, including a proposal for a draft Royal Decree on localisation requirements for private 5G networks.[4] Under the draft security rules, MNOs and Mobile Virtual Network Operators (MVNOs) providing 5G services would be obliged to obtain a ministerial authorisation (which would take into account any potential national security risks) to purchase network elements and use service providers using certain network elements.

- **Ireland**

  The Irish Government recently announced plans to introduce primary legislation which allows government to assess and, if required, designate network equipment vendors as being high risk. Under the proposals, Ireland would have powers to exclude such high-risk vendors from critical parts of a telecoms provider's network. Ireland has also agreed several measures to enhance the security of electronic communications, including 5G networks – endorsing the *'EU 5G Security Toolbox'* as the framework by which Ireland will secure its next generation Electronic Communications Network.

[3] This will be based on UK National Cyber Security Centre best practice security guidance and government is consulting on a draft..

[4] See https://www.bipt.be/operators/publication/consultation-on-the-draft-royal-decree-introducing-location-requirements-for-5g-networks; https://www.bipt.be/file/cc73d96153bbd5448a56f19d925d05b1379c7f21/4b87fa20ea13e2eed4930df3f03687398eb13555/Consultation_Reseau_priv%C3%A9.pdf; and https://www.bipt.be/file/cc73d96153bbd5448a56f19d925d05b1379c7f21/749da1403bf3c49d9bc440550438bd92c2548f9c/Raadpleging_prive_netwerken.pdf

wiggin

- **Netherlands**

  The publication of additional security requirements for mobile network operators (MNOs) relating to critical components of mobile networks will enter into force from October 2022. These rules relate to the secure configuration of technical equipment and network infrastructure, monitoring of technical infrastructure, security assurance on software and management services and human resource security.

- **Poland**

  The updated Draft Regulation of cyber security systems in Poland published in October 2021[5] contains provisions excluding certain high-risk vendor suppliers from the development of 5G networks in Poland.

- **Switzerland**

  In December 2021, the Federal Council launched a consultation on amending the Ordinance on Telecommunications Services (OTS) to improve the security of telecommunication networks.[6]

  The amended OTS mandates internet access providers to strengthen their security measures against the unauthorised manipulation of telecoms installations and to combat any attacks on the availability of a server, service or infrastructure. They will be also required to report any major disruption in the operation of their telecoms installations and services to the National Emergency Operations Centre (NEOC).

  The draft OTS proposal also contains provisions on the security of 5G mobile radio networks and services operated or provided by 5G licensees. In particular, these licensees must ensure that safety-critical telecommunications installations comply with recognised safety standards and operate their network and security operation centres in Switzerland, the EEA or the UK.

Russia

Russia recently adopted a series of measures aimed at localisation of data necessary for the operation of telecoms networks and service offerings, including far-reaching requirements on pre-installation of software of Russian origin.

The Russian government has long exerted control over the internet in Russia but has pushed in recent years to technically isolate the internet within Russia from the rest of the world (via the introduction of 'RuNet' or the 'internet within Russia'). In May 2019 Russia adopted a specific law on RuNet which entered into effect on 1 November 2019. This consolidates the control of internet architecture within Russia to ensure the internet can be isolated in the event of a security incident. Roskomnadzor, Russia's internet and media regulator, has been deploying deep packet inspection (DPI) in an effort to block access to prohibited apps such as encrypted messaging services and has recently gained further legal powers to regulate the internet.

In December 2021, the Russian Parliament, the Duma, reviewed a government bill on the Data storage rules[7] which provides that communication providers will be required to: (i) store on Russian Federation territory information on reception, transmission, delivery and processing of voice calls, text messages, images, sounds, video or other messages of users for three years from when such actions took place; and (ii) provide authorised state bodies with such stored information as well as information on the services provided to users.

Russia has also introduced draft laws (such as new rules on operator administrator responsibilities)[8] which aim at (i) securing compliance of telecom operators with obligations to connect to or exchange information with a compliance monitoring system operated by the Roskomnadzor, or (ii) terminating the provision of communication services or services for the transmission of traffic to communication networks in cases stipulated by Russian Federation law.

In Summer 2021, Russia adopted legislation on the Pre-installation of Russian Software[9], which

[5] See https://www.gov.pl/web/cyfryzacja/kluczowa-faza-prac-nad-ustawa-o-ksc; and https://www.telepolis.pl/wiadomosci/prawo-finanse-statystyki/huawei-krytykuje-nowy-projekt-ustawy-o-cyberbezpieczenstwie.

[6] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-86234.html

[7] https://sozd.duma.gov.ru/bill/1154099-7.

[8] https://sozd.duma.gov.ru/bill/430721-7.

[9] http://publication.pravo.gov.ru/Document/View/0001202109270018. See also http://publication.pravo.gov.ru/Document/View/0001202108100022 under which the government approved a list of Russian

entered into force on 1 January 2022. Under this new law, Yandex Search will be a default search engine on electronic devices in Russia and Yandex Browser and Kaspersky Internet Security apps have been added to the list of Russian software which must be pre-installed on PCs and laptops. These applications must be pre-installed not only on Windows devices but also MacOS devices.

Since 1 July 2021, a newly adopted federal law[10] has also taken effect, imposing administrative fines on those selling technically complex goods without pre-installed Russian software or software originating from the Eurasian Economic Union (EEU).

Finally in August 2021, Russia published further draft measures on Traffic flow rules for providers.[11] These introduce regulation of internet traffic flows and set out requirements for traffic flows through devices. These have been provided to telecom companies by the Roscomnadzor to counter threats to the stability, security and integrity of the functioning of the internet and public communication networks in Russia. This order is applicable to all internet service providers (ISPs) in Russia.

Turkey

In 2015, Turkey introduced a regime requiring registration and payment of a registration fee for any mobile device used in Turkey for any period that exceeds 120 days. If not registered, local operators are required to discontinue roaming on their networks.[12]

In September 2021 new regulation on the Registration of Devices with Electronic Identity Information[13] was adopted requiring the registration of devices with electronic identity information where operators (i) provide services on their IMSI and networks, (ii) receive international data traffic service for voice communications and (iii) provide any 112 in-vehicle emergency systems (i.e., e-call).

India

In India, the Department of Telecommunications (DoT) is reportedly considering the implementation of a licensing regime to regulate applications and platforms such as WhatsApp, Facebook and Skype from a national security perspective. The aim would be to ensure the storage of call data within India and facilitate responses to law enforcement agencies.[14]

In May 2021, the DoT also issued a notification to all internet service licensees, asking them to comply with the following conditions under current laws:

1. Maintain all commercial records/ Call Detail Records (CDR)/ Exchange Detail Records (EDR)/ IP Detail Record (IPDR) with regard to communications exchanged on the network and archive such records for a least 1 year for scrutiny by the DoT (see further below regarding subsequent extension to two years), after which time they may be destroyed unless directed otherwise.

2. Domestic traffic of entities as identified/ specified by the DoT must not be routed/ hauled to any place outside India.

3. Accounting information relating to any subscriber (except for international roaming/billing) and user information (except pertaining to foreign subscribers using an Indian operator's network while roaming and international private leased circuit subscribers) must not be transferred to any person or place outside India; and

4. Ensure that all subscribers other than individual subscribers record and maintain Network Address Translation (NAT) SYS Log parameters in India as per the prescribed format, which must not be taken outside the country.

Providers were also reminded of the need to comply with past DoT notifications in relation to *'Instructions under the Internet service license*

software, which must be pre-installed on technical complex devices, such as cell phones and tablets. (https://tv.ok.ru).

[10] http://publication.pravo.gov.ru/Document/View/0001202103240040.

[11] https://regulation.gov.ru/projects#npa=119334

[12] https://ikamet.com/blog/how-to-register-your-mobile-phone-in-turkey#:~:text=Go%20to%20your%20nearest%20PTT,password%20to%20register%20your%20phone.

[13] https://www.resmigazete.gov.tr/eskiler/2021/09/20210915-5.htm; or https://www.btk.gov.tr/duyurular/elektronik-kimlik-bilgisini-haiz-cihazlarin-kayit-altina-alinmasina-dair-tebligde-degisiklik-yapilmasina-dair-teblig-taslagi-kamuoyu-gorusune-acilmistir.

[14] Possible new unified communications rules: press Release - https://telecom.economictimes.indiatimes.com/news/dot-mulls-regulating-calling-apps/83025641

wiggin

regarding provision of Wi-Fi services' dated 23 February 2009 and '*Parameter of IPDR and SYS LOG of Network Address Translation*' dated 1 October 2013.

In December 2021, the DoT also issued a further notification - increasing the time period for maintaining and storing Call Detail Records (CDR), Exchange Detail Records (EDR) and IP Detail Records (IPDR) for communications exchanged on the network to 2 years (rather than 1 year). Similarly, an amend to the Unified Licence (UL) was made requiring entities authorised to provide internet services to maintain IPDR for internet and internet telephony for 2 years (rather than 1 year). Licensees are also required to maintain log-in / log-out details of all subscribers for internet access, e-mail, internet telephony, IPTV etc. for 2 years.

USA

In November 2021, the US Secure Equipment Act of 2021 became law, prohibiting the Federal Communications Commission (FCC) from reviewing or issuing new equipment licenses to companies on the FCC's "Covered Equipment or Services List" that pose a national security threat. This list currently includes certain telecoms equipment supplied by Huawei, ZTE and others). Although the Act relates to a US government entity it is worth monitoring as further changes impacting companies may follow. Indeed, some argue this Act does not go far enough, as the FCC not approving equipment authorisations is not sufficient on its own. Some go further and are calling for the US government to prevent the flow of potentially compromised components into devices and to ensure that users have methods of detecting and addressing the serious dangers posed by certain components.

Global developments in 2022

It will be interesting to see how this area develops in 2022. While the importance of ensuring security of telecoms networks is clear, policies such as banning high risk vendors clearly have the potential to conflict with competing policy objectives such as ensuring diversification of supply where vendors are limited. Indeed, in some cases only a single supplier option might be possible. The practical challenge of the related risks of high costs of implementation and service failures are also a very real risk for providers if certain equipment is removed from networks or particularly stringent measures are imposed, so the impact of any new security requirements will need detailed planning and monitoring.

The diversification of telecoms offers international partnership opportunities to achieve economies of scale for a growing global telecom market. Balancing this with security goals will be a path that needs careful navigation. Many operators are focused on investing in new 5G Mobile infrastructure, so the added costs of ensuring security measures are in place for ageing infrastructure will be challenging. The highly politicised nature of action taken by the US, UK and others to date shows that this is a primary area of government focus for many countries, so more requirements may be on the horizon for TMT providers. It will be important for industry to engage with government and regulators to educate them on any potentially damaging business impacts that security measures might have, to enable any security requirements imposed to be both effective and implemented in an informed way as to the likely risks for business and trade.

wiggin

Increasing scrutiny of transactions for national security risks: more investment and acquisition screening

The UK's Security and Investment (NSI) Act has now entered into force, introducing a new foreign directive investment (FDI) regime in the UK. The Act introduces new powers for government to investigate and, if necessary, intervene in investments and other acquisitions of entities and assets in, or linked to the UK where they could harm the UK's national security. The government has called this 'the biggest shake up of the UK's national security investment screening for 20 years.' The Act represents an important new risk factor for acquisitions and corporate restructures with a similar review and notification risk process to merger control rules.

UK

The NSI Act will apply to a wide variety of qualifying transactions that involve the acquisition of 'material influence' in a company – this can be deemed to exist in relation to a very low shareholding (including below 15%) - or involve the acquisition of control over assets which potentially give risk to national security concerns. Assets for this purpose include land, tangible property and intellectual property including trade secrets, databases, code, algorithms, formulae, designs, plans or software.

The UK government has the power to "call in" any qualifying transactions that give rise to UK national security concerns for review. The Act gives significant discretion to government in its review of qualifying transactions and the term 'national security' is undefined in the Act. This means that the range of concerns that can be considered by government in its review are unspecified, providing a lot of discretion to government and potential uncertainty to investors. If the government identifies national security concerns as part of an in-depth review, they have wide powers to impose remedies and can even block and potentially unwind transactions.

In addition, the Act requires certain acquisitions of entities in 17 sectors which have been identified as being the most sensitive sectors for the UK economy to be notified and approved before they are completed. A wide range of industries are caught by this mandatory notification obligation, including energy, transport, communications, defence, artificial intelligence, data infrastructure, and satellite and space technologies, and other hi-tech sectors. If a mandatory notification obligation applies, parties to a transaction will be prohibited from completing prior to obtaining clearance. Breaching this notification obligation will also result in a transaction being automatically void.

In terms of scope, the NSI Act applies to all investors – both UK and non-UK – as the regime applies equally to UK investors. Acquirers who are hostile or a threat to UK national security rather than foreign nationality will be a focus of review. It's also worth noting that the UK government has power to call-in a transaction for review for qualifying transactions involving non-UK companies or assets - for example, where the target entity supplies goods or services to persons in the UK, or the target assets are used in connection with activities carried on in the UK or the supply of goods or services to persons in the UK.

wiggin

Sanctions for non-compliance with the NSI Act are severe and can result in fines of up to 5% of worldwide turnover or £10 million and/or imprisonment as well as director disqualification.

The new UK NSI regime is untested, and its operation will evolve in time. Although the government predicts 1,000-1,800 notifications annually, it expects only around 10 deals per year to require remedies. The government has promised to publish guidance 6 months after the Act entered into force – to allow them to consider how the Act is working practice. For now, parties to transactions, particularly in the 17 sectors subject to mandatory notification, will need to factor the NSI review into any timeline for a transaction and the long stop date. This will have a significant impact on acquisitions and investments in the communications sector and other tech-related sectors that are subject to mandatory notification.

Current situation across the globe

Netherlands

On 19 May 2020, the Dutch Parliament adopted an Act on undesired control in the telecommunications sector (the Act). The Act introduces a notification requirement for any party envisaging acquiring 'a controlling interest' in a 'telecom operator' if such interest results in 'relevant influence' in the Dutch telecom sector. If the controlling interest could result in a 'threat to the public interest' in the case of foreign direct investments, the Dutch Minister of Economic Affairs and Climate has the power to prohibit transactions or impose a ban subject to suspensive conditions.

The Act is of relevance to anyone wishing to acquire control in a Dutch telecom provider, hosting service, internet node, trust service or data centre.

As of October 2021, no transactions have been prohibited. Six transactions have been notified, and seven ex officio investigations have been completed[15].

Denmark

On 5 April 2021, the Danish Parliament passed an Act on Screening of Foreign Direct Investments (FDI), which came into force on 1 July 2021.[16]

The new Danish regime is based on two filing schemes: (i) mandatory notification and (ii) voluntary notification.

(i) Mandatory notification

The mandatory scheme applies to foreign investors intending to acquire a "qualifying holding" in a Danish undertaking which operates in a particularly sensitive sector. A qualifying holding means direct or indirect possession or control of 10% or more of the shares or voting rights or similar control by other means. The obligation to seek prior clearance applies to investments within sensitive sectors, which have been defined as business activities within the national defence industry, IT security services or processing of classified information, manufacturing of dual-use items, other types of critical technologies and critical infrastructure. Details on the application of this scheme will be clarified in executive orders by the Danish Business Authority.

(ii) Voluntary notification

A foreign investor may voluntarily notify the Dutch Business Authority about a foreign direct investment if the contemplated investment potentially implies a risk to the national security or the public order. This scheme applies to acquisitions of holdings of no less than 25% of the shares or voting rights or similar control by other means. Investors from the EU/EFTA are exempt from this scheme, meaning that they should not apply under this voluntary scheme.

It may be difficult for an investor to assess the extent to which an acquisition might imply a risk, and the Danish Business Authority will hopefully provide guidance on this in future.

Once an application for clearance is filed with the Danish Business Authority the Authority will usually have 60 business days to clear the investment.

India

In September 2021, India's Union Cabinet approved several structural and procedural

[15] https://zoek.officielebekendmakingen.nl/kst-1001567

[16] https://www.ft.dk/ripdf/samling/20201/lovforslag/l191/20201_l191_som_vedtaget.pdf

wiggin

reforms in the telecoms sector, including permitting a 100% foreign direct investment into telecom companies without prior government approval. Previously this was only possible for investments of up to 49%[17].

Later in 2021, the Indian DoT also amended guidelines on licence conditions[18] and issued new guidelines on the registration of infrastructure providers[19] to reflect the new FDI rules and clarify that the new automatic (i.e. without government approval) FDI rules for investments into telecoms company of up to 100% would be subject to compliance with security and licensing conditions.

These amendments provide for certain exceptions where:

- The FDI is from an entity of a country which shares a land border with India, or where a beneficial owner of an investment into India is situated in or a citizen of any such country; or
- Transfer of ownership of an existing or future FDI is in an entity in India which directly or indirectly results in beneficial ownership falling within certain conditions.

In such instances, any FDI will fall under the approval route and require prior government approval.

Indonesia

In June 2021, the Investment Coordination Board (BKPM) introduced important changes with Regulation No. 4 of 2021 on Guidelines and Procedures for Risk-Based Licensing and Investment Facilities (Regulation 4/2021)[20], including that:

1. Any subsidiary of a foreign investment company with a domestic investment company status must convert its status to a foreign investment company within one year. If such a change in status is made, if the relevant subsidiary is conducting any activity that is closed or restricted for foreign investments, it must cease such activity immediately.
2. Foreign investment companies are bound to divest if required under investment issued prior to this regulation. Certain exemptions from the divestment requirement exist if:
    a. The company's existing local shareholders do not require a divestment; or
    b. In the case of a 100% foreign-owned company, a foreign direct investment involves all shareholders having no commitment or agreement with any domestic party to divest their shares.

Vietnam

In March 2021, the Government issued a Decree No. 31/2021/NĐ-CP (Decree 31) providing detailed guidance on certain articles of the Laws on Investment 2020. The guidance provides:

1. a Prohibition List, which includes a list of business areas that certain foreign-invested companies are not allowed to invest in;
2. a Market Entry Condition List, which includes a list of business areas for which certain foreign investors must satisfy a set of market entry conditions to invest; and
3. a new negative list approach, which requires that certain foreign investors must be treated as domestic investors for the purpose of market entry conditions when investing in business areas which do not fall within the Prohibition and Market Entry Lists.

[17] https://pib.gov.in/PressReleasePage.aspx?PRID=1755086, https://dot.gov.in/sites/default/files/Telecom%20Reforms%202021-booklet%20as%20on%2001102021.pdf.
[18] https://dot.gov.in/sites/default/files/Amendment in License Agreement of Commercial VSAT service for change in FDI norms.pdf, https://dot.gov.in/sites/default/files/211103-FDI-UL(VNO)-Guidelines.pdf?download=1, https://dot.gov.in/sites/default/files/Amendment in the INSAT-MSS Reporting Services License Agreement (INSAT-MSSR) for change in FDI norms.pdf?download=1, https://dot.gov.in/sites/default/files/211103-FDI-UL_Guidelines.pdf?download=1.
[19] https://dot.gov.in/sites/default/files/RevisedIP-1Guidlines22122021.pdf?download=1.
[20] https://peraturan.bpk.go.id/Home/Details/168903/peraturan-bkpm-no-4-tahun-2021.

wiggin

Enhanced consumer protection and upcoming consumer IoT regulations

The increased use of communication goods and services poses a challenge for legislators looking to protect consumers against poor-quality products and unfair contracts and business practices.

Law makers have recently introduced a number of measures to protect consumers such as the EECC.

Consumer IoT has also raised concerns given the risk of leading companies being able to independently determine interoperability requirements through governed terms and conditions and by limiting data access and use for third parties while keeping extensive data access for themselves. This clearly risks having a negative impact on the investment and expansion of new technologies and ultimately the consumer, who will be restricted to using only devices provided by leading service providers.

EECC and National Transposition

In 2021, most EU/EEA Members States and the UK revised their rules for electronic communications networks and services as a result of the European Electronic Communications Code[21] (the EECC) being transposed into national laws

The EECC amends and replaces the four main directives that made up the 2002 telecoms regulatory framework, incorporating them into a single document. It includes measures to encourage competition and stimulate investment in very high-capacity networks and to enhance consumer protection. This EU Directive had to be implemented by EU Member States by 21 December 2020. However, the transposition into national laws has met with significant delays. Despite several warnings and reminders from the EU Commission, only a handful of Member States met the initial deadline. At the end of 2021, a considerable number of Member States had still failed to notify full transposition. For the latest on this, please see our EECC tracker, which monitors EECC implementation across the EU/EEA and in the UK.

Consumer protection represents one of the central themes of the EECC which has extended the 'traditional' consumer regime to small businesses and non-for-profit organisations and - in certain limited cases - also to large businesses. Key EECC consumer protection measures involve the following rights:

1. **Access to information for disabled users**

   Existing requirements have been extended to ensure that all important communications relating to communications services are available in a format that is accessible to end-users with disabilities.

2. **Pre-contract information and summary of key contract terms**

   New information obligations aim to ensure customers are provided with clear and comprehensive information about their communications services and the terms and conditions that apply to them before they

[21] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code).

enter into a binding contract with service providers.

3. **Exit rights**

Customers have stronger rights to exit their contract if providers choose to make changes to their contractual terms during the term of the contract unless such change is (i) exclusively to the customers' benefit, (ii) purely administrative in nature with no negative effect on the customer, or (iii) required by law.

Providers will be also obliged to notify customers before the expiry of any commitment period and allow them to terminate their service/ contract on one month's notice without incurring any costs.

4. **Maximum duration of a contract**

The requirement that the maximum duration of a contract/ commitment period must not exceed 24 months will now apply to all elements of bundles. Providers also need to ensure they have alternative offers available which have a commitment period of no more than 12 months.

5. **Usage notifications**

Customers must be notified when a service included in their tariff plan is fully used up.

6. **New rules on bundles**

The new regime extends to bundles, with the aim to further limit possibilities for customers to be "locked-in". This involves elements of a bundle of telecoms (i.e., voice or internet) and certain non-telecom services being regulated.

7. **Switching and porting**

New requirements apply for porting numbers and switching (including for internet access services), where the new/ gaining provider leads the switch with the aim of ensuring the shortest possible timelines (which in most cases should not exceed one working day).

8. **Remedies in case of Quality of Service (QoS) failures**

National law should provide for appropriate remedies in the case of "significant, continuous or regularly recurring deviations in speed" between the actual performance of internet access services and the performance stated by the provider.

The EECC's end-user protection measures require maximum harmonisation, which means that Member States should not deviate from them (i.e., they cannot give 'more' or 'better' rights to consumers or small businesses in addition to the level of protection granted by the EECC).

Our experience with national rules so far, however, shows that even the purportedly fully harmonised consumer protection rules seem to be largely divergent. The application of these rules varies between individual Member States depending on, inter alia, the definition of micro-enterprise, small enterprise and not-for-profit organisations as well as other categories of enterprise customers that have been introduced into national legislation. Individual Member States also differ in how they have applied these rules (e.g., with length of time periods that differ from the EECC when applied in a national law context - where, for example, the EECC requires a month, some jurisdictions have decided to extend this to 45 days or 60 days.).

One example of this is the termination right triggered by unilateral contract modifications, where national laws may impose additional restrictions as EECC rules must be read in the context of wider civil law regimes in certain EU jurisdictions. The impact of new pre-contract information requirements on the validity and conclusion of an enforceable contract also varies. Whilst in Germany, a failure to provide this information does not affect the validity of the contract/ subscription, in the UK, it renders the contract/ subscription invalid/ not effective. Italy also takes a different approach on this, with the use of certain sales channels allowing for more flexibility for a provider as pre-contract information can be provided after the subscription interaction (i.e., tele-sales) and the contract becomes effective only once pre-contract information has been provided to and accepted by the customer. Another variation area concerns waivers available under EECC to providers for the new category of micro and small enterprise and not-for-profit organisations customers, where

wiggin

again we have seen various national law flavours affecting their use.

In light of these different national approaches to implementing EECC, operators offering services across the EU/EEA cannot rely on a uniform application of EECC rules and will have to engage in a detailed country-by-country analysis to adjust their contract terms and associated processes or models.

We have also noted that the non-traditional telcos, like UcaaS and VoIP providers, appear to date to have largely ignored the new developments as they might be under the impression that they do not apply to them. This is likely to expose their contracts and standard terms even when they serve exclusively enterprise customers.

EECC implementation in the UK

Although the UK left the EU on 31 January 2020, under the terms of the Withdrawal Agreement, the UK remained under an obligation to implement EU Directives into domestic law until the end of the Brexit transitional period, which expired on 31 December 2020. As a result, the new rules on consumer and small businesses' protection in the UK introduced by changes to the Communications Act 2003 and new General Conditions of Entitlement issued by Ofcom, largely mirror the EECC.

There is however one important general exception to the EECC transposition in the UK, as the UK Government decided against extending the scope of regulated electronic communications services by number-independent interpersonal communication services (NI-ICS) such as internet phone and messaging services – e.g., provided by Over-the-Top (OTT) players. It is not excluded that this decision would be revisited at a later stage.

Recent examples of consumer protection developments in Asia and APAC

We expect that EECC implementation may trigger (or run in parallel with) a wave of consumer protection reforms around the globe – which may be inspired either by EU developments or based on local experience.

- **Korea**

  Under the Telecommunications Business Act (TBA), telecoms providers that provide basic telecoms services (e.g., telephone service, mobile service, internet access service) are required to report their terms of use (ToU) to the Ministry of Science and the ICT (MSIT).

  In November 2021, a bill amending the TBA was proposed to the National Assembly.[22] The bill proposes (i) to enable the MSIT to refuse the acceptance of a ToU report if the ToU is unreasonably disadvantageous to users, and (ii) to enable the MSIT to propose standards for the payment of damages caused by the disruption of telecoms services and to recommend the settlement of such damages payments between the telecoms service provider and users.

- **Australia**

  In August 2021, the Australian Government published draft legislation aimed at strengthening protections against unfair contract terms, including measures for the small enterprise segment to:

  - Make unfair contract terms (UCT) unlawful and give courts the power to impose a civil penalty (including providing more flexible remedies to a court when it declares a contract term unfair);
  - Increase the eligibility threshold for protections from less than 20 employees to less than 100 employees, and introduce an annual turnover threshold of less than $10 million as an alternative threshold for determining eligibility: or
  - Improve clarity around the definition of a standard-form contract, by providing further certainty on factors such as repeat usage of a contract template, and whether the small business had an effective opportunity to negotiate the contract.

  This followed an earlier step taken in July 2021, where the government significantly increased the value threshold for consumer protection from 1 July 2021 to $100,000 AUD. This change is designed to ensure that

[22] https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_S2F1K1T1R0G9I1P3P2N0I4F9J7W0V0.

wiggin

consumer protection legislation and regulations continues to be fit for purpose, acknowledging the increased price of consumer goods driven by inflation and other economic drivers. It is also designed to ensure minimum standards of protection for business consumers, as well as ordinary consumer purchases.

Consumer Internet of Things (IoT)

2021 has witnessed numerous governmental initiatives aiming to protect customers against cyber-threats and attacks, as well as the intrusion of privacy or personal data issues when using consumer IoT services and devices. Some of them also aimed to tackle competition concerns relating to potential obstacles for the sector, including lack of interoperability or common standards, or issues around access and use of data generated by IoT devices.

EU competition inquiry

In September 2021, the European Commission published the preliminary results of its competition sector inquiry into markets for consumer Internet of Things (IoT) related to products and services in the European Union.[23] Their final report was published at the end of January 2022.

The Commission has noted that consumer IoT products are rapidly growing but the cost of technology is a key barrier to entry and expansion, alongside interoperability, access to data and regulatory hurdles. The Commission has also highlighted that interoperability and integration processes are largely driven by the leading smart mobile devices and voice assistant providers and that interoperability agreements are typically made on standard conditions that are rarely negotiated. Other key findings of the Commission included that devices and services rely on a combination of open standards, and that there were no industry wide standards for privacy policies and contractual arrangements for collecting and sharing data. The Commission also had concerns that leading voice assistant providers can limit data access and use for third parties, while having extensive data access themselves.

To address concerns in this area the Commission has noted it may decide to open case specific investigations under Article 101 and 102 of the TFEU[24] (i.e. the key provisions on prohibited agreements and concerted practices as well as on abuse of dominance) which means that certain problematic practices may soon be under further scrutiny.

Upcoming UK consumer IoT security legislation

In the UK, between July and September 2020, the government ran a consultation on proposals for legislation to regulate the cyber security of IoT products. In April 2021, the Government published its response[25], announcing upcoming consumer connected IoT product cyber security legislation.

The central focus of the UK's proposed legislation will be protection of consumers from insecure connected products. The regulation will apply to all consumer connected products such as smart speakers, smart televisions, connected doorbells but also smartphones. A number of devices will be exempt due to the specific circumstances of how they are constructed and secured, including desktop computers and laptops. The security requirements will align with international standards that should be familiar to all manufacturers and other relevant parties across the industry. An enforcement body will also be equipped with powers to investigate allegations of non-compliance and to take steps to ensure compliance.

India's Code of Practice for Consumer IoT

The Indian Telecommunication Engineering Centre (TEC), which forms part of the Department of Telecommunications at the Ministry of Communications has issued a Code of Practice for Securing Consumer IoT (CoP)[26] which provides the baseline requirements for IoT manufacturers, service providers (companies that provide services such as networks, cloud storage and data transfer which are packaged as part of IoT solutions), mobile application developers, and

[23] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2884.

[24] Treaty on the Functioning of the European Union.

[25] https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation; https://www.gov.uk/government/news/new-cyber-security-laws-to-protect-smart-devices-amid-pandemic-sales-surge;

[26] https://tec.gov.in/pdf/M2M/Securing%20Consumer%20IoT%20_Code%20of%20pratice.pdf.

wiggin

retailers, based on Security by Design principles and international best practices.

The TEC is also working on principles for security by design and a National Trust Centre (NTC). The NTC will serve as a central mechanism to register devices and ensure customers can distinguish between good and rogue devices. The guidelines for baseline standards cover the following:

- No universal default password
- Implementation of a means to manage reports of vulnerabilities
- Keeping software updated and maintaining integrity of software
- Secure storage of sensitive security parameters
- Secure communication
- Minimisation of exposed attack surfaces
- Ensuring security of personal data
- Making systems resilient to outages
- Examination of system telemetry data
- Incorporating ease for users to delete user data
- Making installation and maintenance of data easy
- Validation of input data

wiggin

Encryption vs. data protection

Security is becoming more important to consumers when using communications services - as it always has been for corporate customers. Recent consumer shifts towards services with high encryption standards such as Signal and Telegram demonstrates how much the public values privacy and secure communication services.

Systems that use End-to-end encryption (E2EE) protect consumers from financial fraud and other harms. However, encryption restricts the detection of harmful content and presents a challenge from an online safety and law enforcement perspective, as secure communications also provide a harbour for criminal activity and risk exposure, especially to children.

We predict that this year the ongoing conflict between these competing interests, especially in the field of child safety, will come even more to the fore.

Current situation across the globe

UK

Divided opinions between E2EE and Data Protection are evident with the recent 'No Place to Hide' campaign, funded by the Home Office, which warns of dangers of end-to-end encryption for private messaging on plans to pressure Mark Zuckerberg's decision to introduce E2EE on Facebook and Instagram, particularly child sex abuse that could go undetected. The UK's Information Commissioner's Office (ICO), on the other hand argues that E2EE serves an important role in safeguarding privacy and online safety, and that the government should continue to maximise law enforcement techniques instead of seeking to weaken encryption: *"Having access to encrypted content is not the only way to catch abusers," Statement from Mr ICO's Executive Director Stephen Bonner*[27]

We also see potential obligations under UK technical capacity notices (TCNs) that could theoretically mandate reductions in the protections afforded by encryption. However, these confidential mandates will do little to increase guidance or transparency for industry in this regard and on-going soft pressure on the major players is likely to continue.

During 2022, we can expect developments of new tools and applications proposed by the winners of the Safety Tech Challenge Fund, a UK government fund initiative in the fight against child abuse in E2EE communications, which has resulted in five projects in artificial intelligence and other technologies, that can scan, detect, and flag illegal child imagery without breaking end-to-end encryption. The aim is that such tools can become available in the market sometime this year.

The organisations involved include Edinburgh-based police technology start-up Cyan Forensics and AI firm Crisp Thinking, which will work in partnership with the University of Edinburgh and the Internet Watch Foundation to develop the plug-in app. Cyber-safety firm SafeToNet is looking at how to use AI in video-moderation; while T3K-Forensics, an Austrian mobile data extraction firm, is working on implementing its AI-based child sexual abuse detection technology on smartphones in an E2EE-friendly way[28].

The progress of these developments during the year may be the answer to government debates on upholding privacy freedoms and ensuring procedures for the detection of criminal behaviours that threaten the safety of children online are in place.

[27] https://www.bbc.co.uk/news/technology-60072191

[28] https://www.computerweekly.com/news/252509763/UK-government-announces-safety-tech-challenge-fund-winners

wiggin

EU

The same debate exists across Europe where encryption is considered an appropriate measure to ensure a high level of security for the protection of fundamental rights and data, and to strengthen cybersecurity.

The EU Commission considers that there is no possibility to warrant government accessing encrypted data for law enforcement purposes without undermining encryption and moreover the freedoms of users. The Commission have proposed several concrete non-legislative measures to support law enforcement in overcoming challenges posed by encryption in the context of criminal investigation. Perhaps the most notable is the strengthening of Europol's technical capabilities to deal with encryption, including a transfer of EUR 5 million to the agency to enhance its existing capability to help law enforcement overcome the challenges posed by encryption in criminal investigations. Europol launched its innovative decryption platform in January 2021, developed in close cooperation with the European Commission's Joint Research Centre, which will increase Europol's capability to decrypt information lawfully obtained from communications providers in criminal investigations.

During 2022, the EU Home Affairs Commissioner also plans to present new legislation on yet-to-be agreed new powers for Europol which will put the institution at the forefront of innovation and research for law enforcement, as set out in a Europol Programming Document 2021 – 2023[29].

The new ePrivacy regulation is also expected to reinforce privacy freedoms, recognising the importance of encrypted communications as a crucial element to the compliance of privacy regulations in the exchange of communications, as set out in a statement by the European Data Protection Board. The regulation, however, is not expected to come into force until 2023.

USA

There is no legislative power which can be used to require telecommunication or online service providers to facilitate the decryption of encrypted communications in the United States. However, the debate is ongoing as legislation requires all telecommunications carriers to ensure that their equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate or direct communications have certain capabilities which includes interception of communications and delivering intercepted communications to the government, where the government obtains a court order or there is some other lawful authorisation.

A long line of law enforcement officials have tried to pressure Congress to introduce legislation to provide exceptional access to the government to access encrypted communications. However, a group of civil societies, organisations and technology companies have come together to oppose such legislation. The argument is the same: if backdoors were introduced into encrypted systems, malicious actors will exploit those system's vulnerabilities, steal the keys held by law enforcement, national security agencies, or companies, and move their communications to non-US platforms that are outside the reach of US law enforcement.

In several criminal cases in the USA involving the use of Apple devices, in Pensacola (Florida) and San Bernardino (California), the FBI has used techniques to crack the encryption without the assistance of the provider or a built-in backdoor.

Currently, telecoms carriers cannot be required to decrypt, or to ensure the government's ability to decrypt any communications which are encrypted by the subscriber or customer unless the encryption was provided by the carrier, and they are able to decrypt it.

No developments in federal state law are expected this year, however at the state level the full implementation of the California Privacy Rights Act (CPRA) is expected by mid-2022 and Virginia and Colorado's new laws will come into force over the next 18 months. Another half a dozen new states also plan to pass privacy legislation. So far, we know that the scope of the CPRA is to strengthen privacy protection and control data processing, implement measures such as conducting annual cybersecurity audits and risk assessments and further guidance is expected to follow for telecoms providers to comply with such requirements[30].

[29] https://www.europol.europa.eu/cms/sites/default/files/documents/europol_programming_document_2021-2023.pdf

[30] https://iapp.org/resources/article/the-california-privacy-rights-act-of-2020/

wiggin

China

In China, the situation is quite different. In 2020, the first comprehensive law regulating encryption technologies came into force, providing a range of restrictions on the manufacturing, import, export and use of encryption.

First, it requires manufacturers to obtain approval for the type and model (including key length) of their encryption products and a license for the import and export of encryption products. This means organisations and individuals may not distribute encryption products produced abroad as only products that have received government authorisation may be used.

Second, commercial companies are required to maintain backdoors or key escrows to preserve government access to data for public security and intelligence gathering, which has discouraged the widespread adoption of commercial encryption. It has also long demanded the encryption industry prioritise the development of 'secure and controllable' encryption, which has impeded the industry's growth.

Telecoms providers must however be prepared for changes with regards to processing data as Chinese regulators brace for a busy year with the implementation of the new Personal Information Protection Law which came into force 1 November 2021, impacting the way both domestic and multinational companies process or use personal information of individuals located within China. The legislation provides clarification in terms of the legal bases for processing personal information; lays down the obligations and responsibilities imposed on processors; and imposes stricter requirements on data localisation, safeguarding China's interests in the case of cross-border transfer of personal information[31].

What lies ahead in 2022?

It will be interesting to see how this area develops in 2022. Most countries are divided on the subject. Governments are concerned on law enforcement for the purposes of criminal investigation and technological organisations could face sky-rocketing costs if they are required by law to create 'backdoors' for encrypted communication. Changes in legislation could mean significant financial challenges for telecoms providers, not to mention the impact on the freedoms of consumers to communicate and exchange information privately.

[31] https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/

wiggin

Net Neutrality – what next?

The Net Neutrality principle has been upheld as an international human rights standard. However, as we grow into a more digitalised world, net neutrality is becoming more of an issue to keep up with.

A recent study by the Internet Service Providers Association in UK suggests that during the COVID-19 pandemic between March 2020 and March 2021, internet usage surged by 78%. As a consequence of the pandemic, the increase in home working has seen daytime internet access traffic increase by three-quarters, suggesting the playing field for internet access is changing.

Net neutrality across the globe

UK - The Post Brexit Scenario

In September 2021, the UK regulator of communications service providers OFCOM commenced a review of existing UK net neutrality rules which are designed to ensure no serious blocking or slowing of access to legal websites or internet services by broadband ISPs and mobile operators). Among the reasons for review is the innovative and emerging technologies in residential and business contexts. These are underpinned by catalysts such as the emergence of 5G technology and the accelerated move to the cloud. There are also increasing capacity demands from people and businesses. Initial findings of the review are expected during Spring 2022 and will help determine if the UK decides to depart from the European Union's approach on net neutrality[32].

European Union

In the EU, an approach upholding the principle of net neutrality seems unlikely to change in the near future. In October 2021, the EU set out to review and reform one of the biggest loopholes in the EU's framework: Zero-Rating: a practice by which telecoms companies discriminate between online services by making some data traffic more expensive than other such traffic. Prompted by three judgments of the Court of Justice of the European Union, the Board of European Regulators for Electronic Communications (BEREC) has acknowledged that their previous 2016 Guidelines on how to enforce the Net Neutrality Regulation need to be overhauled. The practice of zero-rating has enabled communications service providers to offer customers zero-rating bundles that exempt certain websites or streaming services from counting towards a data allowance. Problems have arisen in practice where telecoms providers have zero-rated their own services to create a competitive advantage. Certain providers across the EU still engage in zero-rating practices but that looks set to change soon.

United States

The principle of Net Neutrality has also been a controversial topic in the United States. During the Trump administration, the Federal Communications Commission's Restoring Internet Freedom Order became effective in 2018, overturning requirements on net neutrality and placing primary jurisdiction over internet service providers' network management practice under the Federal Trade Commission, which also pre-empted states from enacting similar ISP network legislation. The U.S Court of Appeal, however, concluded that the FCC had no legal authority to issue its Pre-emptive Directive. Since then, and after the change in administration to Biden, several states such as California, Oregon and Washington have enacted and passed net neutrality legislation which prevents the blocking of lawful traffic, slowing lawful traffic, paid prioritisation, getting paid zero-rating, etc. Most federal states have proposed net neutrality

[32] https://www.ofcom.org.uk/consultations-and-statements/category-2/call-for-evidence-net-neutrality-review.

legislation already, so changes can be expected across the nation very soon.

South Korea

A proposal by the South Korean parliament to amend the Telecommunications Business Act would allow the world's first law mandating paid prioritisation, which is set to erode the principal of net neutrality in contravention of international standards regarding access to the internet. The proposal, if passed, would allow Korean internet providers (ISPs) to impose financial barriers to network access by content providers (CPs). Content Providers such as Naver, Kakao, Netflix and Google would have to pay Korean ISPs termination fees based on network usage to have their content be sent to the ISP's customers. The outcome is still to be seen, as the parliament has received enormous pressure from civil society groups opposing the new legislation.

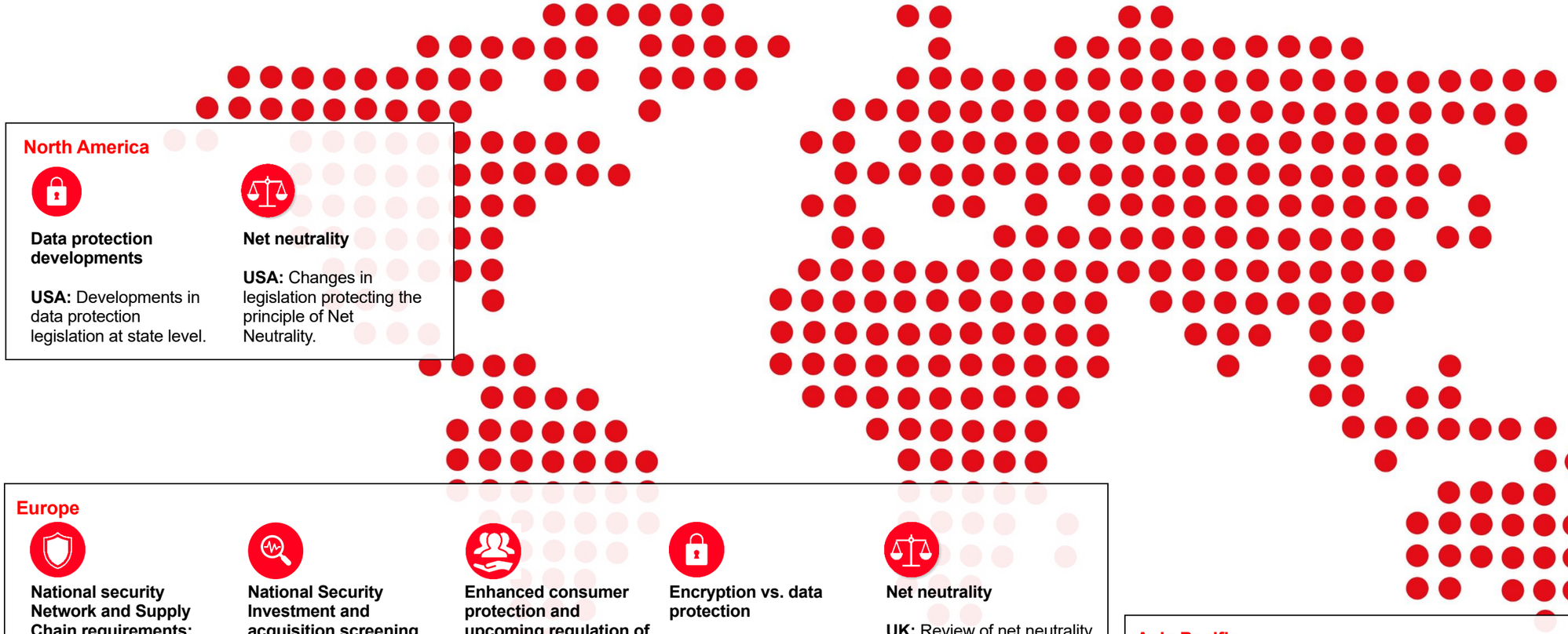
Future global developments

Views are divided on the benefits of net neutrality; some argue it preserves free speech by prohibiting internet service providers from blocking content, protects consumers from ISPs speeding or slowing, or charging higher fees for selected online content and foremost, promotes competition for new providers. However, existing companies may be discouraged from offering certain costly services if they aren't able to charge higher fees.

Big telecoms providers such as AT&T, which has been offering 'Data Free TV' to customers for years, are in the process of re-evaluating this service as the current state-by-state approach operated in the US is unworkable. Hence, the changing scenario across the globe may mean opportunities for some providers and losses for others.

wiggin

Global heatmap 2022



North America

Data protection developments

USA: Developments in data protection legislation at state level.

Net neutrality

USA: Changes in legislation protecting the principle of Net Neutrality.

Russia

National security Network and Supply Chain requirements: implications for TMT providers

Changes in data storage rules.

Potential measures on traffic flow on the internet for service providers.

Europe

National security Network and Supply Chain requirements: implications for TMT providers

UK: Strengthened legal duties on telecoms providers to increase the security of networks and services.

Belgium: New possible localisation and security requirements for 5G networks.

Ireland: New legislation to exclude high risk vendors.

Switzerland: Enhanced security for electronic communications networks.

National Security Investment and acquisition screening

UK: National Security and Investment Act in force – operators to face tougher reviews and sanctions for non-compliance.

Denmark: Legislation on Screening of Foreign Direct Investment in force.

Enhanced consumer protection and upcoming regulation of consumer IoT segment

UK: Developments in legislation to regulate the cyber security of IoT products.

EU: Competition inquiry noted increasing costs of technology barrier for IoT related products and services to enter the market. Further investigations to follow.

Encryption vs. data protection

UK: New technological developments to scan and detect illegal child imagery without breaking end-to-end encryption.

EU: New e-Privacy regulation expected to reinforce privacy freedoms and recognise the importance of encrypted communications.

Net neutrality

UK: Review of net neutrality principle may change net neutrality approach.

EU: Zero-rating bundles look set to disappear.

Asia Pacific

National security Investment and acquisition screening

India: 100% of Foreign Direct Investment on network operators subject to compliance with security and licensing conditions.

Indonesia: Subsidiaries of foreign investment companies that have the status of a domestic investment company to convert to a foreign investment company.

Enhanced consumer protection and upcoming regulations of consumer IoT segment

Australia: Developments in legislation aimed at strengthening protections against unfair contact terms.

India: Code of Practice for Securing Consumer IoT in place.

Encryption vs. data protection

China: Implementation of new Personal Protection Law.

Net neutrality

South Korea: Proposal for first law mandating paid prioritisation.

wiggin

Contacts

Gordon Moir
Partner

Gordon.Moir@wiggin.co.uk
+44 (0) 7414 267467

Victoria Harris-Honrado
Partner

Victoria.Harris-Honrado@wiggin.co.uk
+44 (0) 7485 399179

Marcus Bagnall
Partner

Marcus.Bagnall@wiggin.co.uk
+44 (0) 7485 383148

Michaela Lodlová
Consultant

Michaela.Lodlova@wiggin.co.uk
+44 (0) 7826 798110

Christina Gleeson
Consultant

Christina.Gleeson@wiggin.co.uk
+44 (0) 20 3290 2947

Cecilia Lovell
Senior Paralegal

Cecillia.Lovell@wiggin.co.uk
+44 (0) 7485 383143

Graeme Brink
Paralegal

Graeme.Brink@wiggin.co.uk
+44 (0) 7826 798347