the global voice of the legal profession

Communications Law

Newsletter of the International Bar Association Legal Practice Division

VOLUME 22 ISSUE 1 JUNE 2016

IN THIS ISSUE

Contributions to this newsletter are always welcome and should be sent to the Newsletter Editor, Vittorio Noseda, at the address below:

Vittorio Noseda
NCTM, Milan
Tel: +39 02 72551.1
Fax: +39 02 72551.501
vittorio.noseda@nctm.it

International Bar Association
4th Floor, 10 St Bride Street, London EC4A 4AD
Tel: +44 (0)20 7842 0090 Fax: +44 (0)20 7842 0091
www.ibanet.org

Terms and Conditions for submission of articles

1. Articles for inclusion in the newsletter should be sent to the Newsletter Editor.
2. The article must be the original work of the author, must not have been previously published, and must not currently be under consideration by another publication. If it contains material which is someone else's copyright, the unrestricted permission of the copyright owner must be obtained and evidence of this submitted with the article and the material should be clearly identified and acknowledged within the text. The article shall not, to the best of the author's knowledge, contain anything which is libellous, illegal, or infringes anyone's copyright or other rights.
3. Copyright shall be assigned to the IBA and the IBA will have the exclusive right to first publication, both to reproduce and/or distribute an article (including the abstract) ourselves throughout the world in printed, electronic or any other medium, and to authorise others (including Reproduction Rights Organisations such as the Copyright Licensing Agency and the Copyright Clearance Center) to do the same. Following first publication, such publishing rights shall be non-exclusive, except that publication in another journal will require permission from and acknowledgment of the IBA. Such permission may be obtained from the Director of Content at **editor@int-bar.org**.
4. The rights of the author will be respected, the name of the author will always be clearly associated with the article and, except for necessary editorial changes, no substantial alteration to the article will be made without consulting the author.

This newsletter is intended to provide general information regarding recent developments in communications law. The views expressed are not necessarily those of the International Bar Association.

Greetings from co-chairs to the Communications Committee

Jukka-Pekka Joensuu
Cinia Group OY, Helsinki
jukka-pekka.joensuu@cinia.fi

It is with a great pleasure that I write this editorial for the Communications Law Committee newsletter. When I entered the telecoms market in 1998, the industry had just been liberalised by the first directives. After that, we had several packages and discussions about ex ante and ex post regulation. In those days, we also talked a lot about what the market could look like and what Web 2.0 could bring to us. Back then we had no idea that it would create such huge market players, such as Google and Facebook.

As we are now entering the digital market with the Communications Committee in the forefront, the committee's leadership is discussing a proposal to change the committee's name to reflect the transformations that have taken place over the last few years, where communications have been fully integrated into the digital world. We have a very good message for the legal industry, we want to pursue the digital market and communications law has been a tremendous game changer. We welcome our members' comments and feedback with respect to these developments.

We also have a great event coming up in Amsterdam and I urge all members to join in, as well with as our dedicated sessions at the IBA Annual Conference in Washington. Events are made by people participating in the conferences, and I really would like to see old and new friends joining in.

The last year has been quite a journey personally, completing a major project for the digital single market in Europe and a major infrastructure investment. As it has been said, new networks are the backbone for the digital economy and the way the communications industry is changing is remarkable.

I have written a small introduction to the newsletter about the Sea Lion project and what it can bring to the society. As lawyers, we do not do this just to have a day job; we do this in order to build a better future and better society.

Finally, I would like to thank, also on behalf of my Co-Chair, Camila Lefevre, all contributors to this particularly rich and wish you a very bright future in the world of communications law.

With regards,

Jukka-Pekka Joensuu
Co-Chair
Communications Law Committee Newsletter

Vittorio Noseda
NCTM, Milan
vittorio.noseda@nctm.it

From the Editor

Dear Communications Law Committee members,

I am extremely pleased to present a sparkling and vibrant edition of the IBA Communications Law Committee newsletter 2016 containing contributions from more than 25 authors, ranging from representatives of authorities and academies to members of worldwide leading law firms.

We will hear about developments and experiences from more than 15 jurisdictions and well-known law firms; the Communications newsletter 2016 deals with the latest hot topics.

Pascal Dutru, Regulatory Authority of Qatar and Prof Stefano Quintarelli, MP, set the path with highly innovative and authoritative opinions on regulation of digital platforms and electronic communications: it will be important to follow these opinion-makers for a better understanding of the way forward.

IoT, self-driving cars and Smart Cities, a very hot topic, are comprehensively addressed in our newsletter with articles dealing with the point of view of international, EU, Korean, Bulgarian law and, with respect to Smart Cities, UAE laws.

Roaming is another key topic. Contributions analyse the well-known EU Roaming Regulation IV, as well as the wider international scenario. For once, the EU is ahead but let us see future international developments.

Other extremely interesting topics range from the new Telecom Catalogue in China, to net neutrality in India, the new US FCC privacy rules, the bid for the fourth telco in Singapore, Spectrum sharing, the EU General Data Protection Regulation, important decisions for OTT in Germany, Uber and other transport apps, Cloud Computing, etc.

The Communications newsletter 2016 offers an extremely updated and broad ranging set of highly informative articles which any player in the digital communications industry should be eager to read and comment upon.

I wish to thank the IBA Communications Law Committee Co-Chairs and all contributors for their outstanding articles, and do hope to see you all, inter alia, at the incoming IBA Communications Law Committee events in Amsterdam and Washington.

Vittorio Noseda
Newsletter Editor
IBA Communications Law Committee

Committee Officers

Co-Chair

Camila Borba Lefèvre
Vieira Rezende Advogados, São Paulo
clefevre@vrbg.com.br

Co-Chair

Jukka-Pekka Joensuu
Cinia, Helsinki
jukka-pekka.joensuu@cinia.fi

Senior Vice Chair

Anne Vallery
VVGB Advocaten / Avocats (VVGB-EU CVBA), Brussels
Anne.Vallery@vvgb-law.com

Vice Chair

Chung Nian Lam
WongPartnership LLP, Singapore
chungnian.lam@wongpartnership.com

Secretary

Alfonso Silva
Carey, Santiago
asilva@carey.cl

European Forum Liaison Officer

Violetta Kunze
Djingov Gouginski Kyutchukov & Velichkov, Sofia
violetta.kunze@dgkv.com

Membership Officer

Timothy Cowen
Preiskel & Co LLP, London
tcowen@preiskel.com

Conference Coordinator

Rehman Noormohamed
DWF LLP, London
rem.noormohamed@dwf.law

Young Lawyers Liaison Officer

Blanca Escribano
Olswang Spain LLP, EPE, Madrid
blanca.escribano@olswang.com

Website Officer

Laurent De Muyter
Jones Day, Brussels
ldemuyter@jonesday.com

Newsletter Officer

Vittorio Noseda
NCTM Studio Legale, Milan
v.noseda@nctm.it

Latin American Regional Forum Liaison Officer

Alfonso Silva
Carey, Santiago
asilva@carey.cl

LPD Administrator

Susan Burkert
susan.burkert@int-bar.org

Jukka-Pekka Joensuu
Cinia Group OY, Helsinki
jukka-pekka.joensuu@cinia.fi

A maritime cable from Finland to Central Europe-Baltic Sea area becoming a new Data Hub and connecting European Single Market

Background

Finland holds a unique position in the EU, with the Baltic Sea connecting to continental Europe and geographically connecting northeastern Europe with Eurasia and Asia. This has been true in relation to telecommunications and data networks. Traditionally, due to close relations in business and the building of business links, Finland has been connected to Sweden through various networks. This has been the way for Finnish companies establishing pan-Nordic business, and also creating data connectivity towards central Europe. In the late 1990s, due to rapid increase of telecommunications traffic, this also became a highway connecting east to west, and today most of the internet and telecommunications traffic is carried through Finland and Sweden towards main European internet hubs to serve the demands of the capacity needs of Russian, Asian and international carriers and businesses. Connectivity to the Baltic states and routes through Baltic Sea countries were also created in early 2000.

In 2010, the Finnish Ministry of Traffic and Communications began to look for ways to create new connectivity between Finland and Germany and increase the demand for a new era of telecommunications data traffic. The emergence of OTTs like Google and Facebook building their data centres, together with Russian Yandex, started the new face of development. In 2013 a feasibility study was conducted by Pricewaterhouse Coopers Oy (PWC), the results and a wide consultation process paved the way for new investment to build a maritime cable from Finland to Central Europe.

The Finnish Government and Prime Minister's Office made an important decision in late 2013 to purchase a company called Corenet, running backbone railway telecommunications networks and making the sea cable project, Sea Lion, one of the most expensive governmental initiatives. The project, including the transformation, was expected to have a budget of €100m with the sea cable costing between €60-80m.

Public-private consortiums leading the way to new European digital highway

As the European economy is undergoing a major transformation while facing very rapid digitalisation, there is need for new kind of thinking. A traditional way of financing and building vast infrastructure projects needs a more holistic approach to neutral networks which can carry vast amounts of data and provide a platform for innovativeness, new services and mobility.

The Sea Lion project was built to meet the demands of this new era and combine industrial know how and strong governmental support with public funding and private actors. A wide public consultation provided an open and transparent process, leading the European Commission to accept the application from the Finnish Government to build the Sea Lion project with €20m funding, including public support, to build the sea cable with cybersecurity, redundancy and promotion of Single Digital Market in Europe.

The support of the EU for the project was one of the key elements to the institutional funds and financial market and, after approval on 16 September 2014, the project progressed rapidly. By the end of October 2014, after several discussions with interested parties, a private consortium of Ilmarinen and OP Group were chosen to meet the matching equity investment of Governia's public €20m

investment. Then, in early December 2014, after a thorough tendering process, a French company ASN Submarine Networks was chosen as turnkey provider to deliver this challenging project. Corenet was renamed Cinia Group, and a separate SPV C-Lion1 Oy was created to own and operate the sea cable system.

Delivering the project

The project had a very demanding 16-month project plan to study the final route, build the cable, apply for permits in the Baltic Sea territorial water owners and under economic zones, and to lay the cable in the seabed.

The Baltic Sea is a shallow water area and laying a 6-8 fiber pair system has several challenges. These include mines, archeological and other nature reserve areas, a very rocky seabed (especially in the northern part of the Baltic Sea) and winter conditions, which, in the worst case scenario, could have created serious hurdles for the project.

With the professional organisation of ASN, wide capabilities in delivering the projects and the dedication of the Sea Lion team, the project was ready on time and in budget. The Finnish Government and stakeholders of the cable system now have a 144 tbit/s system in use, and the European economy can utilise the green energy markets in the Nordics to build data centre connectivity and data centres to meet the demands for the European SMEs, corporate and public organisations and connect European hubs with Asian and western data hubs.

What's next?

The maritime cable system has a life cycle of over 30 years and will experience several development phases. In less than 15 years we have seen the emergence of the Big Data, cloud providers and business growing more and more digital. This cable creates a bridge between Northern Europe and Central Europe through the Baltic Sea and will open new possibilities between the continents.

Therefore, aiming for the future is the Arctic Connect. Building a physical data connection from the top of Europe through Northeast Passage will connect the Asian and European continents and enable a new silk route to emerge. This should be the next goal for the Nordic countries and Barents Region and will make a truly global digital economy possible. Neutral networks, connectivity and data security are building a better society for business and for people.

We also believe that the Sea Lion project is an example of combining private and public funds to build an open access network with high focus on data security and neutrality and the inclusion of carriers, OTTs and all players in the system to fuel the digital economy and build better society.

Laurent Benzoni,*
TERA, Paris
benzoni@tera.fr

Pascal Dutru,**
Communications Regulatory Authority, Qatar
pdutru@cra.gov.qa

Towards an overarching regulation of electronic communications

The world is in the midst of what many call the second digital revolution, led by new and exciting trends such as big data, cloud computing, and the 'Internet of Things'. Digital technologies are transforming our cities, our businesses, our social lives and our nation – and they are key to an innovative, diversified and robust economy with high standards of living for people.

As we rely on increasingly sophisticated systems and advanced telecommunications networks, the challenge is to refine appropriate policies and support laws that allow societies to seize the opportunities that new digital technologies offer. While the evolution of telecommunications networks has enabled a complete shift in market dynamics, opening each country to international exposure, this new era requires new business models and creates challenges.

The role of the regulatory authorities is to support and enable this dramatic change.

The impact of new technologies

The standard telecommunications regulation framework was developed when telephones still had cords and televisions had antennas. The main challenges lay in opening a monopolistic sector to competition and promoting new infrastructure. Therefore, for the last 30 years, regulation has focused on providing incentives for the rollout of competitive telecom network infrastructure and regulating access to infrastructure for better and cheaper services for consumers. In this 21st century, technology has driven telecommunications into households, with wireless phones and access to the internet. In 2014, global internet traffic was 16,144 GBps and it is expected to grow to 51,794 GBps in 2019.[1] With this evolution of technologies and especially the development of full internet provider ('IP') fixed and mobile networks, regulation needs to go beyond the physical layer of the network and enter the digital world.

Today, communications and services are delivered through numerous routes and platforms, which are outside of traditional telecom operators. For example, users of WeChat can create a group of contacts and, in some countries, select a restaurant, make a reservation, select the best route to reach a given location, pay for dinner, share photographs or videos, and leave a review. Teachers are creating groups for each of their classes, connecting pupils together, following up and correcting assignments, etc. All this is achieved seamlessly online through a single application. The creation of the groups, their size, the density of communication inside the group is unbeknown to the telecom operators and yet the members of these groups are the operators' subscribers. The traditional model is broken. In the old model, all communications between operators' subscribers were managed, controlled and the service was billed to the operators' own clients. In today's model, infrastructure and services are more and more separated. New intermediaries capture the value created by services: the digital platforms, the so-called 'Over the Top' ('OTT').

Businesses are also directly impacted by these evolving technologies. For some time already, large corporations have had to use communication services enabling them to expand beyond each nation's borders. These same services should be available worldwide. To do this, businesses need to develop integrated information systems or purchase worldwide communication services which connect their branches anywhere in the country or in the world, organise private video conferencing between subsidiaries, store data in a single location (with backup in another safe location), to begin with.

Similarly, smart cities will integrate communication and information technology solutions to transform the way our cities are organised and managed.

More broadly, the 'Internet of Things' ('IoT') is becoming a reality. All devices will

be connected, and flows of data will be stored and managed to provide services that are yet to be invented.

Customer trends and behaviours have also evolved significantly and erased frontiers between interpersonal communication and dissemination of information by broadcasting and creating new markets and intermediaries. The rules of the game and value chains – the activities though which companies add value at every step of their processes – have changed. Social media is more than a communication tool; it is a means to trade, broadcast, exchange, transfer, or even do business.

Most importantly, new intermediaries have popped up between consumers, content providers, telecom operators (telcos) and platforms. Diverse and innovative content and services are now just a click away. In the beginning, consumers and telcos alike welcomed this change. With time, however, new issues have arisen: such as integrated online payment, personal data protection, power concentrated by a few global internet players, and piracy.

While yesterday's telco controlled the value chain, from content to handset, today's electronic communications are driven by digital platforms and applications, sparking a major power shift. This shift has pushed telcos and digital platforms into a symbiotic relationship. To provide services and content to customers, platforms and applications must access the telcos' local loop. Yet telco's are selling data plans that are more comprehensive, making it easier and cheaper for customers to access digital platforms' services and content. This relationship is uneven: platforms are global and agile players, while telcos are bound by authorisations (licences) granted by national governments, and subject to a comprehensive set of ex ante regulatory obligations. In this new environment, telcos could merely become providers of volume-based data (broadband) plans to customers with limited added value to the service, while digital platforms may be prevented from offering content and services to customers.[2]

Although the regulatory framework has moved forward to embrace these changes, the paradigm shift caused by these new technologies and new behaviours has changed too much to adapt to this digital transformation. Thirty-year-old rules and practices no longer meet the needs of the new realities, and regulatory practices can no longer be confined to telecom networks and services.

Regulation must adapt to this new reality and look to the future.[3]

A call for a renewed approach to regulation

The traditional regulatory approach relies mainly on the assessment of telecom service providers' capacity to control the physical access to their infrastructure (wholesale level), and the assumption that this control results automatically in market power at the retail level – and can justify regulatory intervention ('ex ante remedies') requiring the dominant service provider to fulfil specific obligations to prevent – the logic of ex ante - potential abuses[4] (eg, non-discrimination, cost orientation, etc.). This ex ante regulatory intervention enables the progressive development of a competitive environment. Assessing market power, however, has become more and more fundamentally flawed. Such approach does not take into consideration the new reality of multi-sided markets where, for instance, customers are not paying for the service or content provided to them and service providers' revenues flow from advertisements or bundling, where communication services are part of a much larger array of services. Regulation must, consequently, adopt a wider approach that considers convergence of technologies and access ubiquity, and assesses whether economic bottlenecks result from multi-sided markets or bundle of services that underpin the dynamics of digital platforms (or OTT service providers).

The Communications Regulatory Authority ('CRA') must address regulation differently. As expressed by a number of researchers and specialists[5] regulation should contribute to maximising the benefits of networks. For instance, the more value a communication network has, the more value it provides for an individual and the more people this individual can communicate with using this network. Economists qualify these benefits as 'positive network externalities' (the more a network is used, the more value this network has for its members and the more benefit each member gets out of the network). These 'positive network externalities' mitigate against 'club effects', where a service provider creates artificial barriers for people to communicate or access services outside of the network. Regulators should instead favour open networks, which include favoring an

'open' internet - uninhibited access to legal online services and content.[6] This also implies that regulators must extend their activities to digital platforms to avoid economic bottlenecks that allow one or a few players to manipulate network externalities and capture the networks' full benefits.

With hindsight, most of the behaviours currently at stake relate to the digital platforms' ability to internalise to their advantage the positive network externalities, and, in doing so, increase their market power to a point where they become virtually impregnable for a given type of Internet service.[7] In the meantime, tight oligopolies will become the de facto market structure for telcos due to their large fixed network costs, in a never-ending cycle of network investments.[8]

Today's regulatory perspective needs to consider the end-user from the beginning of his/her journey to the end, when he/she accesses his/her desired content or service. Accordingly, regulation should address the digital means by which a given content or service is delivered to the end-user. This approach leads to define infrastructure and services using any communication network, including the internet, as the 'digital media' that allows end-users (individuals, firms, public institutions) or connected objects to access the service (or content). In other words, this definition goes beyond traditional digital broadcasters, to encompass all technical means (physical or logical) involved in providing an 'internet service' as illustrated below.

Figure 1 – The scope of regulation: the digital media value chain (Tera Consultants)

Therefore, the regulatory approach needs to:

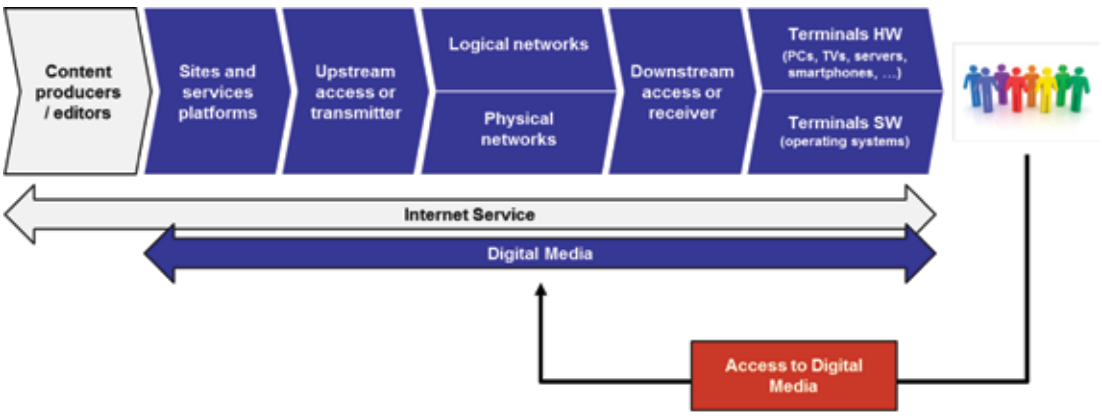
- aim at preserving the long-term interest of end-users;
- be dynamic and reactive;
- focus on behaviours more than on dominant players;
- favour an end-to-end approach, considering both the physical and logical network, service platforms, devices, software, algorithms and applications;
- ensure that the quality offered to the end-user corresponds to the requested service, both in terms of speed, latency, but also in terms of scope, incorporating more or less intelligent services (storage, cloud virtual private network);
- ensure the security of services to preserve the integrity of communications and personal data; and
- promote the ubiquity of access and the full migration of personal data between the platforms.

Consequently, a responsive and non-intrusive approach to regulation may combine:

- controlling or assessing behaviors, contractual agreements, and tariffs ('ex post' intervention); and
- imposing ex ante remedies on powerful actors in predefined relevant markets ('ex ante' regulation).

This control shall focus on wholesale products, but also include pricing practices in retail markets such as 'bundling' (associating various services which cannot be purchased independently of one another), 'zero-rating' (tariff practice where the service provider does not charge end-users to use certain applications or services when a customer subscribes to another service) or 'sponsored data' (selling data packages at low prices or for free subject to the subscription of a bundle of service).

In this context, the regulator aims to



deal with any competitive bottleneck. The market power of an actor could be measured primarily by the share of traffic that is sent or controlled at any level of the digital media value chain (including all the means necessary to access the end-user desired service or content). This means addressing competitive bottlenecks through imposing on whatever player, whether a telecom service provider, a transit service provider, or a digital platform, etc, preventive, corrective and/or protective measures for end-users. The regulator could also consider any contractual agreement to favour any powerful player in the access to the digital media value chain. For instance, 'zero rating' agreements could be assessed, as well as agreements between telecom service providers and digital content distributors. Conversely, the portability of IP addresses or of profiles and personal data between applications could also fall under the responsibility of the regulator in the same manner as the current portability of phone numbers. Indeed, the regulator could coordinate with the various relevant authorities, when required, and each country can develop a consistent governance approach.

Regulation and governance will go beyond a national approach and incorporate a transnational dimension. Global players offering digital media services to users distribute them across countries and continents. In practice, a more or less restrictive regional coordination may be required to tackle issues such as net neutrality, security of data in the IoT or data protection, as was the case with international roaming tariffs.

In addition, a geographically fragmented regulation may prevent each country from reaping the benefits of the digital economy. As a minimum, national regulators must identify the areas and the issues that need to be addressed on a regional level to avoid additional costs for service providers due to regulatory heterogeneity between the countries - the discrepancies between national regulations would generate additional development costs and limit economies of scale for new services. Regional governance would also ensure greater transparency and better predictability in the laying down the rules for all market players.[9]

Putting the regulatory approach into action

To ensure that end-users take full advantage of communications and access the most advanced and innovative services, ranging from IoT, IoE, Smart cities, Smart cars, e-Health, or e-Education, among others, access to services and content needs to be seamless, instantaneous and ubiquitous. To achieve these objectives:

End users can access the services and content of their choice, under conditions providing efficient access

Allowing service providers to organise restrictions on the types of service means service providers can exercise their clout by creating access bottlenecks to other providers willing to offer services or content to their subscribers. More broadly, telecommunications service providers should not be able to choose or exclude digital media suppliers at the consumer's expense.

To ensure a fair, non-discriminatory and effective access to digital media to all end-users (individuals, firms, public institutions), the regulator must develop a net neutrality regulation to be rigorously implemented by telecommunications service providers for each class of traffic (eg, communication, messaging or video services). Accordingly, discrimination is not possible within a given class of traffic and a service provider cannot be able to offer a hierarchical priority access within a class of services, let alone throttling or blocking any content and service platform provider's traffic.

As a matter of consequence, the regulator can measure the quality of service ('QoS'), as often as possible, including the type of content, the source and destination, and collect all information from telecommunications service providers pertaining to traffic management. To this end, regulatory authorities shall review their QoS framework. Further, regulatory authorities should control traffic discrimination and monitor, for instance, fast-lane agreements between telecommunications service providers and OTTs. More broadly, regulatory authorities should assess the impact on competition of agreements between telcos and digital platforms.

In addition, regulation can facilitate the evolution of business models. For instance,

a typical strategy for a service or content provider is to offer an increasingly wider array of services to customers, in an attempt to keep them within their platform. Introducing a simple and secure means of payment for these services and content becomes paramount. WeChat is once again an interesting example, as the service allows subscribers to pay directly through the WeChat application wherever they are.

These new models are also establishing authentication, end-to-end cryptography, personal data and 'profile' portability as major matters to address.

This regulation could promote service and content diversity, promote competition between telecom service providers and digital platforms and ensure innovation for the consumers.

However, to be efficient, this regulation needs to be coordinated with other countries through new regional governance models and under the auspices of international governance bodies.

Each country needs to be strongly and securely connected to the world

Requirements in terms of international connectivity will continue to increase significantly in the future. Today's requirements only represent a small amount of what would be required to sustain the growth and diversification of the economy. Quality of service will have to improve significantly, especially in terms of latency and stability of the services provided. For instance, effective autonomous cars or e-health services cannot be contemplated everywhere as long as broadband services do not fulfil high quality and very low latency standards. The same applies to e-education, where immediate interaction between several locations will be paramount. More broadly, customers' expectations will increase steadily as services diversify.

Network integrity and security of communications, including international connectivity, will be paramount to develop trust in the new communication services.

Thus, the regulator can support initiatives enabling services or content to be located as close to users as possible. This could for instance, include fostering the development of independent data centre capabilities open to all service providers and end-users. In any case, localising services and content would increase QoS by nature - the less distance and the fewer intermediaries required to access the service or content of the consumer's choice, the less access will be prone to disruption. This would also have a direct impact on latency, and hopefully security.

Regulation can favour future investments while preserving choice of service providers for end-users

The overall telecom sector remains healthy. Given the communication industry's fast innovation cycles, the regulator can develop incentives to favour continuous investments in local access.

To this end, two sets of measures can be envisaged: (1) ensure that charges at the wholesale level include a premium to favour investment in infrastructure rather than access to existing networks; and (2) support local service providers in their negotiations with digital platform or transit service providers to ensure fair and non-discriminatory peering agreements.

These measures could also contribute to efficient wholesale offers, providing better economies of scale for service providers, for instance, through appropriate leased lines and Bitstream/VULA offers.

New services also require huge IT developments, whether in offering efficient and simple invoicing solutions, including third party solutions, developing new customer relationship management ('CRM') solutions, or in creating interfaces and interoperability between the various platforms and/or services and/or devices. Innovative data 'hubs' to make 'big data' even more efficient should be also considered in conjunction with enhanced security of personal data and network integrity.

Regulation can contribute to building trust on services to ensure take off/end-user adhesion to a smart nation

Without trust, services cannot themselves develop. Trust in the service to be delivered according to agreed standards, trust in the delivery of goods, trust in the protection of personal data, etc. Trust must underpin all exchanges and communication. Data protection, privacy and business secret concerns need to be addressed at all levels. Payment solutions need to be more secure and cryptography more reliable.

Once again, proper and effective governance models can be developed in coordination with other countries at least

through regional governance bodies.

Conclusion

Regulation can evolve to provide value to consumers and protect the long-term interests of end-users. To this end, regulators can consult and work with all stakeholders – including service providers and end-users – to address gaps in regulation and stakeholder concerns. We look forward to a productive collaboration.

Notes

* Professor of Economics at Sorbonne University (Paris 2) and President at TERA Consultants, www.tera.fr.

** PhD, Attorney at Law (Paris bar).

1 http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html.

2 Some digital platforms, such as Google, are very active in overcoming this bottleneck through the development of their own access network, at least in part of the world. Google has even started offering fixed telecom services in the United States.

3 L Benzoni, P Dutru, 'De l'accès aux infrastructures à l'accès aux moyens numériques : nouvelle frontière pour la régulation des communications électroniques', online: espace d'inter-régulations, ed. M A Frison Roche série Régulations, Dalloz, Paris, 2016.

4 The approach of regulation through competition law principles found its full expression with the 2002 'Telecoms Package'. However, competition law has been underlying any major global regulatory framework over the last 30 years. The future European regulatory framework currently consulted upon is no exception.

5 See, for example: N Curien, 'Innovation & Régulation 2.0', Cahiers de l'ARCEP, June 2014; R Feasey, C Pennings, U Stumpf, N Van Gorp Eds, A review of SMP regulation - Options for the future, Communications et strategies, Special Issue, N°98, 2nd Quarter 2015; International Telecommunications Union, Trends in Telecommunication Reform. 4th Generation Regulation: Driving Digital Communications Ahead, Genève, 2014; S Soriano, 'Barbariser la régulation pour réguler les barbares', Huffington Post, 5 November 2015; etc. The Communications Regulatory Authority has also engaged in a full review of its regulatory practice to align it with its mandate as per Emiri Decree 42 of 2014 encompassing access to digital media, ICT, telecom and post.

6 Nonetheless, digital platforms may attempt to create another 'walled garden' through standards, exclusive rights, or even offers. For instance, see in that regard Apple, Google or Facebook practices, and the concerns raised by India regarding Facebook foundation's internet access offer for free.

7 By activating direct or indirect externalities between end-users, digital platforms trigger snowball effects that drive up their activity: the more users of a given service, the more valuable the service, and therefore the more new users it attracts (Metcalfe's law). This dynamic of growth, based on network externalities and snowball effects, features two major trends in markets structuration: monopolisation, and conglomeration.
The 'Winner Takes All' phenomenon underlying the development of internet services implies that the biggest company on a given market eventually becomes quasi-monopolistic. Recent experience shows that such a growth happens either organically (ie, through market dynamics leading to a quasi-monopolistic position, see – eg - the growth of Facebook) or externally (ie, through acquisitions, see – eg – the acquisition of Waze by Google already controlling part of the market through Google maps). Therefore, the absence of ex ante or ex post rules leads inevitably to the fast concentration of players into a single dominant player. The rules apply not only to social networks and search engines (see figures below), but also to e-commerce services (Amazon), communications services (VoIP with Skype, microblogging with Twitter, etc.), classified advertising services (eBay), or collaborative intermediation services (Uber, AirBnB, Booking, etc.). The internet, place of openness, initiative and free competition, generates ultimately quasi-monopolies.
Network externalities generate also conglomerates. Once a player has become a quasi-monopolist on a market, it can capitalise on its customer base to expand its range of services. The initial service is enriched progressively with new services and the player transform itself into a service platform, ie, a bundle of service more or less related to the initial service, but with specific portability functions, frequently turning such platforms into closed ecosystems (customer lock-in). For instance, a new event on Google Agenda will generate email notifications on Gmail. The event may also be shared immediately with contacts whose agenda will automatically be updated with the event. They may also display its address on Google Maps by a simple click. The platform becomes the gatekeeper of the end-user content and services.
This generates a thriving thirst for acquisitions: more than one per month by Google for nearly 15 years, one every two months for Facebook (in particular, Facebook bought WhatsApp on 19 February 2014, and Instagram on 9 April 2012 while having also developed numerous features on its social media network such as Facebook messenger). Microsoft is also present on different markets (Search engine Bing, VoIP communication services Skype, etc.). Despite some immediate and significant impact on the market, national competition authorities have always approved these M&A (re purchase of DoubleClick by Google in 2007 for $3.1bn).

8 In its report on oligopolies, BEREC raises clear concerns regarding the future of regulation, underlining the growing importance of tight oligopolies, and advocates transposing into the regulatory framework the 'Significant impediment of effective competition' ('SIEC') test used for merger cases. BEREC Report on Oligopoly analysis and regulation, December 2015, BoR (15) 195.

9 On this point, the competition law was the precursor for its ability to apply national law to foreign companies carrying on business outside this territory. Neale and Stephens, 'International Business and national jurisdiction', 1988, ICLQ; Roth, 'Reasonable extraterritoriality: correcting the balance of interest', 1992, ICLQ. The US initiated the process, giving rise to many challenges. However, this approach was soon followed by the European Union: Case 89/85 Ahlström c. Commission (Woodpulp I), 1988, ECR 5193, 4 CMLR 901.

Stefano Quintarelli
MP and internet Guru
stefano@quintarelli.it

Synopsis of 'citizen's rights and business' rights in a progressively more immaterial world'

Introduction

I consider it profoundly wrong to talk about *new* technologies to describe digital technologies which have existed for the past 20 years, and I also consider it semantically wrong to talk about real and virtual worlds. For this reason, I put special emphasis on using terms like 'material dimension' and 'immaterial dimension', in spite of 'real world' and 'virtual world'[1]. And the term 'dimension' emphasises that they are not alternative to each other, but rather complementary.

In the last few years, the online platforms and tools which handle our immaterial socio-economic relations have enjoyed a regulatory framework with limited constraints with regards to competition, starting from the eCommerce European directive,[2] which introduced an important exemption from responsibility for systems that simply transmit, host or cache contents. The underlying idea was that since the contents were provided by users, they should be accountable for them. Furthermore, the exclusion of an editorial liability was justified by the absence of human activity since the platforms were considered, *merely* a software. However, platforms have evolved through the years, and I doubt that the original *ratio* of the European directive is still consistent with the present scenario[3].

User interfaces in an immaterial dimension

In the context of the favourable regulation framework enjoyed in recent years, several platforms have grown and become the main interfaces of the immaterial dimension: the main system we interact trough, which is, in turn, rapidly becoming (and for some of us has already become) the main user interface of the material dimension.

We use tools of the immaterial dimension in order to complement and sustain our socio-economic relations in the material dimension. Since a system is characterised by its user interface, if a feature is not accessible in the user interface, that feature does not exist for the user. Therefore, when we are excluded from the user interface of the immaterial dimension, we tend to be increasingly disadvantaged and marginalised in the material dimension. It was[4] reported in the news that a mere change in Google's search algorithms resulted in a profit reduction for Ebay of about $200m. In turn, venture capital corporations invest billions in companies operating in the immaterial dimension, young businesses that rapidly grow and become world leaders in the field of new intermediation for the material dimension. The more people use tools in the immaterial dimension to nurture socio-economic relations in the material dimension, the more these new intermediaries achieve a position of extreme relevance.

There are very different rules: are they justified?

As opposed to what happens in the material dimension, where every business operation has marginal costs and requires time, information in the immaterial dimension moves at speed of light with negligible marginal costs.

While in the material dimension, economic returns usually decrease over time, as we have learned from Malthus onward, in the immaterial dimension they tend to increase over time, as explained by Brian Arthur, favouring the creation of oligopolies/oligopsonies, or worse, monopolies/monopsonies.

Since the deregulation of telecommunications, network rules for operators (which must bear extremely material infrastructural investments) have been designed to guarantee users' fundamental rights, and to favour competition.

As an example, we can recall:

- rules regarding universal access and service, to make sure that nobody is left behind;
- interoperability rules, to minimise network effects and to guarantee that customers of

smaller operators are not disadvantaged;
- rules pertaining to the conservation and protection of personal data, and similar rules to exclude other uses;
- rules to prevent from using utility bills to pay other goods and services;
- asymmetric regulations, to favour new entries against preexisting monopolists; and
- rules to favour the possibility of contending customers, allowing for number portability from one phone operator to another in just one day (something that was technically unfeasible, when the rule was introduced).

Similar pro-competitive, pro customer-contestability rules abound in many markets ranging from airline travel to insurances, from banking to healthcare. Venture capital companies quickly started to reward, with valuations of billions of dollars, the new immaterial intermediaries. The payback, if successful, is world dominance in a market, as such immaterial intermediaries enjoy an exponential growth thanks to the 'network effect' and, more than anything else, for the 'lock-in[5]' effect they deliberately adopted in their business model.

Interoperability and business models

When we think about the internet, we think about a world of freedom, a bit anarchic, where we can use any service, with any device, in any part of the world. In today's world, five to six digital platforms attract the vast majority of time spent online by users as well as of services/goods offered or intermediated; beyond these cases, there is a fragmented periphery, almost invisible if compared to these giants. The idea of the internet that many of us have is linked to open systems, like e-mails and the web. On the other hand, presently, few large digital platforms provide functions/services in a centralised and locked-in manner, not interoperable with other protocols and standards. Paradoxically, if someone invented e-mails today, they would be built by means of a centralised and locked-in service, in which only users duly registered on a specific platform would be able to exchange messages. Then, such a platform would make huge investments in marketing to attract users and, once the virtuous cycle has started, returns would increase as other users come for free.

As a user, if many users are on a platform and I want to message someone else, I would better get there too (eg, '*network effect*'). Once everybody is there, how can I leave? I would not be able to message anybody if I left (eg, '*lock-in*').

Since the birth of the internet, we have enjoyed a system that allows anybody to set up his own server inter-operating with other people's servers, and therefore can send and receive e-mails in an open system.

Why was e-mail born as an open system, and not as a centralised one? The answer lies in its origin. Email was born in an academic environment, not for business reasons, to foster exchanges between researchers and non-researchers.

The same was true for SMS, which were created in a context governed by rules established by telecommunication services with interoperability in their DNA. Today, a closed system such as WhatsApp has enjoyed a tremendous growth thanks to a very compelling user experience.

In short, the lack of interoperability in current services/platforms is not due to technical reasons, but rather to a business choice of the same platforms, in the absence of pro-competition rules requiring inter-operability.

Rules and politics

Rules for the material dimension have evolved over 10,000 years of history and pro-competitive rules in markets have been introduced by politics at some point.

In the immaterial dimension, a specific exemption from responsibility for intermediaries (ie, online service providers) has been created trough a light-regulation approach.

Given the new relationship between the immaterial and material dimensions, I think that we should start asking ourselves some – in my view, essential – questions:
- If a global social network is one of the main tools used by a teenager, can the choice of whether to exclude him or not from such platform be exclusively and without appeal on the private company that runs the platform?
- If an immaterial tool in an oligopolistic or monopolistic regime is the main way to acquire customers for a business entity in the material world, is it correct that a private operator that operates the platform could, de facto, enjoy a right of 'life or death' on such business entity? This is particularly critical when the operator, besides being the interface for the immaterial dimension, can also direct consumers' behaviour, gaining a direct advantage over a competing material activity.

Wouldn't it be better to grant some ex-ante defensive tools to such weaker business entity?

The state of New York[6] has declared Lyft (a service similar to UberEx, in which if you need a car ride, you can get it from a car owner even if he does not have a license for public transportation) illicit. Previously, the city of New York agreed on a settlement with AirBnB obtaining an economic compensation for having reduced tax revenues from people renting their homes without a license.

On the other hand, with respect to these immaterial intermediation services, who has the burden to verify and ensure, for example, the hygiene and security standards or the accessibility for disabled people? Or non discrimination on race, gender and religion?[7] In this respect, we could decide that it is socially desirable to eliminate these controls and guarantees introduced in the past decades by the public authorities, or that these burdens are to be borne by the new immaterial intermediaries. Or else.

The main issue is that the immaterial dimension is vastly deregulated, extremely fast, characterised by growing returns, and tends to grow into global monopolies or oligopolies in just a few years. Dominance positions in the immaterial service intermediation of the material dimension have been (and are being) created without applying the same guarantees and obligations envisaged for analogous 'former' intermediaries operating in the material dimension.

I think that politics should urgently think about this subject, with an open and inclusive approach.

Platforms: 'everything you might ever want, selected by us'

In this scenario, the evolution of the role of hardware manufacturers should be considered.

When we think about computers, we imagine a world in which we write the software we want, the way we want, we can distribute it through the channels we want, and give it to whoever wants it, at the economic conditions that we decide. The same applies to services. Analogously, we think that we can obtain software from any provider, at the economic conditions that he has set, and that we can install or uninstall it on any computer that we want. In terms of the internet, this idea is presently naive.

The freedom of choice and installation enjoyed by computers since the very beginning has been interrupted by the introduction of iPhones, which only enable installations of software available on Apple's app store. Certainly, the catalogue of available software for iOS is huge, but applications not compliant with Apple's standards are not admitted.

Therefore, Apple exerts control over all installed applications (a control which is even tighter where installation trends suggest high interest from users), it exerts censorship on content available on these applications, it limits prices to a few preset values and keeps a 30 per cent commission on the final sale price. The alternate 'store' cannot be installed, since the 'store' programme should be first installed through Apple's app store, but Apple rules specifically forbid alternate app stores. To install alternate software by removing this restriction, a very complex procedure called 'jailbreak' is required, but it is contractually forbidden by the user license for iOS. Users who have performed a jailbreak on their device in order to install software chosen by them have been judged guilty of copyright violation.

Copyright, born to protect authors of cultural products, is being used to ensure the closure of a system, limiting the users' traditional rights and freedoms, limiting competition in a fundamental aspect of software (app stores), reducing content and available software, forcing an economic transaction on the main (immaterial) user interface of the material dimension.

User experience and market control

The lock-in approach introduced by Apple has been subsequently followed by Amazon, Microsoft and Google (who moreover obtains this effect by leveraging ergonomics and the simple user experience, rather than the absolute technical barrier).

For a long time, Apple's license ruled that any commercial product/service consumed on an Apple device was to be sold by Apple, who would keep a 30 per cent commission.

Now the restriction has been loosened by the provision of a 'most favoured nation' option[8], which essentially allows to sell content on alternate systems, but only if it is offered at the same price in the App Store. For example, if a user wants to buy a tax book by Sole24Ore (a leading Italian publishing group), she could do it on the Sole24Ore's website too (where she will pay around two per cent commission for the credit card), but it should also be available on Apple's app

store (where Sole24Ore pays a 30 per cent commission to Apple).

What will she do? Will she obtain the product through a deceitfully disadvantageous procedure (complex for the user, but favourable for Sole24Ore), or will she buy it on Apple's app store through a very simple procedure (but economically very unfavourable for the publisher)?

From enablers to intermediaries

As stated above, the freedom to install any software has been 'taken away' from users and used to create, in a very short time frame, oligopolistic/oligopsonistic positions in the immaterial dimension.

The phenomenon is the substitution of local intermediaries operating in the material dimension, with multinational intermediaries operating in the immaterial dimension and which are able to impose their unilateral rules.

De facto, gate-keepers in the immaterial dimension significantly impact on the business developments and activities of the material dimension, where the loss of tax return is only one feature, and possibly not even the most relevant one.

This is an issue which I believe requires deep thought.

Telco's envy

Telco operators are the biggest losers in this profound transformation: they were dreaming of becoming digital intermediaries.

However, for example, the regulations aimed at protecting the banking payment systems prevented them from becoming *the* payment intermediaries. The personal data regulations prevented them from taking advantage of the users data they had (such as social graph or location) excluding the possibility they become marketing intermediaries.

The above occurred whilst at the same time pro-competitive and pro-user regulations sparked competition in their core business, reducing their margins.

This is the reason why telco operators now ask politicians and regulators to allow them to do business with the only remaining resource: the traffic flowing through their pipes.

Only this business opportunity could allow traditional telcos to re-position themselves as intermediaries instead of mere technical enablers.

Telco operators are also trying in turn to become as well gatekeepers and custodians of the internet access (in order to also control the material dimension).

Personally, I think that we do not need more gatekeepers, but fewer. And therefore we should think more at duly regulating oligopolies/oligopsonies, not at reducing the few rules that in Europe allow us to have landline access to the internet which is generally neutral.

Ex post or *ex ante* rules?

With respect to all above described cases, there are protective legal instruments, mainly by means of antitrust measures.

But antitrust claims require several years and, as I highlighted multiple times, these dominant positions have been built up very rapidly, and much faster than justice can react.

A noteworthy exception, because of its promptness, was the decision adopted by the then Commissioner Monti, who forced Microsoft to host alternative software because he believed that offering pre-loaded software in every copy of Windows would have altered the 'app' market. In that case, the distortion was limited to the economy of the immaterial dimension.

In my view, we are way beyond this, and with much more profound effects with respect to the economy of the material dimension. In fact, today, the immaterial dimension is the user's interface of the material dimension.

As said, I believe we should aim to have fewer gate-keepers and more open-market, and therefore we should favour some general pro-competitive ex-ante measures, fully protecting consumers and material business undertakings.

Ex post remedies are not appropriate in the present environment as they take time and damages have already occurred.

Someone might think that it is impossible to change rules to this extent. But in addition to the cited Microsoft case, let me remind you the (then) almighty AT&T decision to split in order to avoid antitrust intervention. And this was due, not because of illicit behaviour, but just for the fact that the excessive market share of the company was not considered socially desirable.

For all above reasons, I believe that, at the EU level, it's time to act.

Notes

1 Seeing things by this perspective, helps to understand that a teenager does not spend most of his time with his phone or on WhatsApp, but he spends its time with his friends and schoolmates, even when he is materially away.
2 2000/31/CE, accessed 8 June 2000
3 A recent social experiment analysed the impact on users' reactions of positive and negative messages, randomly selected on Facebook by an algorithm. For more information see <http://blog.quintarelli.it/2014/07/epic-epic-challenges-facebooks-manipulation-of-users-files-ftc-complaint.html> accessed 7 July 2014
4 < http://searchengineland.com/google-ebay-penalty-cost-197031> accessed17 July 2014
5 The 'lock-in' is a mechanism similar to a lobster pot, in which there's only one lane, almost automatic, to acquire a user, and it's impossible for such a user to leave the system.
6 <http://www.nyc.gov/html/tlc/downloads/pdf/industry_notice_14_30.pdf> accessed 9 July 2014
7 <https://goo.gl/QYL2IK> accessed 9 July 2014
8 Such contractual conditions are present in other business sectors as well, such as tourism. Booking and Expedia (the two oligopolists in the hotel bookings sector) prescribe that prices published by hotels on their platforms be the lowest among all of the hotel's published rates on internet and require between 20 per cent and 30 per cent intermediation.

Blanca Escribano, Olswang, Spain
Blanca.Escribano@olswang.com

Connected cars and other challenges in the EU IoT privacy ecosystem

Ecosystem, the state of play

There is no doubt that in the near future, automotive transport will be very different than it is today: cars will be connected (to the internet through an embedded SIM card), autonomous and, in most cases, shared (the collaborative economy is bringing new models for service delivery as car2go, Uber, BlaBlaCar, Zipcar, and so on).

The fact that the car itself is connected to the internet, to other cars, to everything, opens the door to several new business models[1] fed by thousands of apps and data flows stored in different clouds: for example, pay as you drive insurance policies, mobility as a service[2], predictive maintenance or 'infotainment'. Autonomous connected cars will allow drivers to use this connectivity while the car is self-driving, so vehicle passengers will have the same demand concerning connectivity performance in the vehicle as at home or at work. This is what some are calling 'information society on the road'.

A wide range of car sensors can send automatic status updates to different data systems: to the manufacturer's system in order to report on damages or defects; to the garage in order to make sure that the necessary replacement parts are in stock; to the emergency system (eCall or bCall in the EU, for instance).

Anticipated as the IoT full enabler, 5G will be used for cooperative automated driving so thousands of vehicles talking to each other can exchange information in real-time. Does it mean a social network of cars?[3] The way different automakers' digital platforms interact with third parties' apps and software will determine the market evolution. For that reason, in recent years the market has witnessed a number of alliances between car manufacturers and telcos and more recently, car manufacturers with IT and software companies.

Value of data

Thanks to context awareness and machine learning algorithms, the same car can offer a personalised customer experience to the driver and the rest of its passengers. A driver's identity and preferences can be moved from car to car, and cars will understand and adapt to their driver's behaviour and choices. Passengers expect to receive that personalised experience when moving from one vehicle to another (owned, leased or shared cars),

and data becomes the basis for the success of those new business models (pay as you drive insurance, predictive maintenance, etc). Data is the new horsepower and connectivity is the new chassis.[4]

Data and trust

The data that powers these new business models is often personal data. With the use of connected cars, will privacy and security challenges be more complex than those already existing with the use of smartphones? Smartphones have more information than most of our partners, relatives and friends have about us. Indeed, they already raise issues like localisation (location data from smart mobile devices is generally considered personal data since individuals can be directly or indirectly identified through their patterns of movement), navigation tracking, services consumption, and so on.

Then, what are the additional issues that we need to be aware of when analysing the privacy challenges of these 'new telecom devices' that cars are becoming? Profiles can be very precise through a combination of data coming from smartphones connected to different platforms and clouds, in-car cameras and sensors collecting data about what happens in and around the vehicle and what passengers are doing through biometrics like facial recognition and gesture analysis.[5] The processing of data may also concern data subjects who are neither subscribers nor actual users of the car services.

Respect for, and protection of, end-users' privacy is a critical success factor for the realisation of the prospects and growth of these services. If users do not trust that their data is being handled appropriately, there is a risk that they might restrict or completely opt out of its use and sharing, which could impede the successful development of IoT. The only way for the IoT to reach its full potential for innovation is with the trust of consumers. This statement is reiterated by FTC Chairwoman Edith Ramirez and EU regulators in every document published on IoT.

Moreover, self-driving cars that are permanently connected to the internet raise major security and privacy concerns. Indeed, together with e-health products and wearables, privacy and security in cars is key, as data breaches or security crises can lead not only to personal data being compromised, but also to lives being put at risk. For this reason, regulators have put the automotive industry on the top of the list of IoT verticals in which privacy and security call for special attention.

The challenge is finding a balance between the need to (re)use personal data for offering innovative services while complying with data protection obligations that aim to protect end-users' rights.

Privacy legal framework and regulators' approach to IoT

In the EU, the legal framework with regard to personal data collected and shared in the context of IoT services is composed by two different sets of rules: (i) the general relevant rules to assess privacy and data protection issues, Privacy Directive 95/46/EC, which is currently under review and will be soon replaced by the EU General Data Protection Regulation (GDPR[6]); and (ii) the specific provisions of the ePrivacy Directive, which is the sector specific regulation of privacy and data protection for the electronic communications sector in the EU.[7] In the light of the DSM Strategy[8], the Commission is also currently reviewing the ePrivacy Directive and there is a public consultation open until summer 2016.[9]

In addition to the data protection and privacy framework, European regulators have produced opinions on the specific challenges that IoT raises, stressing the importance of privacy and security as the cornerstone for success of the new internet phase. It is worth noting that in Europe and the US the regulatory authorities have been analysing this topic in parallel since 2013, when the FTC[10] and BEREC (Body of European Regulators of Electronic Communications) coincided in doing workshops on IoT on the same date.

In Europe there have been opinions from both data protection regulators and telecom regulators, at national and at EU level. In chronological order, from the European Privacy regulators network side (the so-called Article 29 Data Protection Working Party),[11] a very comprehensive Opinion on IoT was published in September 2014.[12] This Opinion focuses on some verticals, not the automotive,[13] but provides detailed principles that are exportable to IoT in general. It analyses the IoT ecosystem through new GDPR eyes. The new GDPR, that will replace the existing Privacy Directive 95/46/EC, includes a new framework of rights and obligations which intends to be more suited for the purpose of the new digital era.

Four months later, on 27 January 2015, again on the same date, the FTC[14] and this time the UK regulator OFCOM[15] published their first reports on IoT. More recently, the network of European telecom regulators, BEREC has published a report,[16] '*Enabling the Internet of Things*', which recognises that a consumer's acceptance of IoT services depends, among other things, on the information provided to them about the level of privacy, networks and data security and interoperability of services, devices and platforms.

All regulators concur in suggesting the same tools that are relevant for stakeholders in the IoT value chain to achieve compliance. Privacy by design and by default, data minimisation, transparency,[17] user friendly and innovative approaches to obtaining data subjects' informed consent, are highlighted by telecom regulators in Europe (ie, BEREC, OFCOM) but also by the FTC in the US. So far, the most comprehensive document that could help companies to understand the level of compliance that will be required in this IoT ecosystem is the Article 29 WP Opinion. This Opinion details the obligations that each of the stakeholders in the value chain is expected to implement in the EU though, as learnt from the Schrems case,[18] it can't be disregarded when providing services elsewhere through the Internet.

Introduced by the GDPR, the right to portability, considered part of the access right, will probably be one of the main impacting obligations for IoT providers across the value chain. It must be highlighted that the Article 29 WP considers that end-users should have access to raw data registered in IoT devices in order to give them capacity to port their data to another data controller and switch services. One important issue for enabling the auto and mobility business models guaranteeing data portability is solving the lock-in issues. Lock-in connectivity issues are being solved through e-SIM or network-agnostic SIM cards, and Over the Air (OTA) migration and software updating, and that will help competition as migration from one network provider to another will be easier. Interoperability of the operating system of the car with platforms such as Android Auto or Apple CarPlay will be as decisive for users as the brand reputation of the car (is this car iOs or Android?), especially in the light of the data portability obligations.

In addition, on the data subject's right to withdraw consent and to object to the use of their data, the Article 29 WP raises the issue of the 'right to be disconnected': '*data controllers should offer an option to disable the "connected" feature of the thing and allow it to work as the original, unconnected item […]. Data subjects should have the possibility to "continuously withdraw (their consent), without having to exit the "service provided*"'. But what is currently under discussion is the right to be invisible, disconnected from the 'connected living' idea, as was very graphically described[19] in '*the silence of the chips'*.

Most recently, on 18 April 2016, the EU Commission published the first communication[20] and the accompanying Staff Working Document[21] on Advancing the IoT in Europe (IoT Communication), within the context of the Digital Single Market (DSM) proposals.[22] This communication presents measures to reinforce the industrial and innovation pillar of the DSM Strategy.[23] The Communication is also related to initiatives already announced in the DSM Strategy such as the Telecoms Review and the 'European Free flow of Data'.[24]

One of the main objectives of the Commission is called 'a human-centred IoT', empowering people along with machines and businesses, thanks to high standards for the protection of personal data and security, visible notably through a 'trusted IoT label'. The communication strengthens the importance of data protection by design and by default as essential principles to incentivise businesses to innovate and develop new ideas, methods and technologies for security and protection of personal data. In particular, techniques such as anonymised or pseudonymised data will encourage the use of big data analytics. Used in conjunction with data protection impact assessments, the Commission considers that with data protection certifications and seals and marks, businesses will have effective tools to create technological and organisational solutions for the IoT. The Commission highlights possible work threads to clarify the GDPR obligations in the context of IoT:

- the adoption by the industry of specific data protection codes of conduct and certification schemes;
- elaboration of new Data Protection Impact assessment frameworks and guidance; and
- industry involvement in R&D activities for privacy by design and by default technologies and solutions.

Regulators and industry approach to connected cars

In addition to the above described non-sector specific IoT studies, there have also been some specific actions in the automotive market.

In the US, the Alliance of Automobile Manufacturers and the Association of Global Automakers agreed the Consumer Privacy Protection principles for vehicle technologies and services (12 November 2014).[25]

In Europe, the French Data Protection Agency (CNIL) is working with companies operating in the connected car market to build tools that are compliant with data protection law.[26]

On 14 April 2016, the EU Ministers signed the Declaration of Amsterdam (the 'Declaration') for *Cooperation in the field of connected and automated driving*. The Declaration states, 'Besides technological progress, there are further challenges and uncertainties related to development of connected and automated vehicles. There are important questions to be answered regarding security, social inclusion, use of data privacy, liability, ethics, public support and the co-existence of connected and automated vehicles with manually controlled vehicles.'[27]

All new vehicle model types approved in the EU from 31 March 2018 will be required to be equipped with eCall.[28] There are data protection obligations for manufacturers of eCall equipped vehicles. Indeed, having heard the recommendations from the Article 29 WP[29] and the EDPS,[30] the e-Call Regulation[31] introducing, among other obligations, data protection obligations for connected manufacturers.[32] In addition to general DP rules and principles as purpose, transparency,[33] data minimisation, quality of data (deletion when not necessary, automatically and continuously removed) and privacy by design,[34] manufacturers shall implement some specific and bespoke obligations to the specific nature of the connected car for the eCall functionality.[35]

A few words on security

As was echoed by the press, during the summer of 2015 a car was remotely hacked in the US just to show that it is possible to access a car's internal computer network without ever physically touching the car. As a result, the SPY Car Act 2015 (Security and Privacy in Your car), sponsored by senator Markey, was enacted in October 2015. The purpose of the Act was to 'ensure drivers won't have to choose between being connected and being protected' by introducing security and privacy standards and the cyber dashboard (National Highway Traffic Safety Administration in consultation with FTC) rating system that displays an evaluation of how well each automobile protects both the security and privacy of vehicle owners beyond minimum standards (presented in a transparent, consumer-friendly form on the window sticker of all new vehicles). Hence, it uses similar tools to the European GDPR to protect data subjects and for the agents in the value chain to demonstrate compliance.

In the EU the European Programme for Critical Infrastructure Protection (2006)[36] was adopted, followed by the Critical Infrastructure Directive 2008/114/EC,[37] the subsequent Critical Information Infrastructures package and the cyber-security strategy, which included a Network and Information Security Directive[38] (NISD), on which political agreement was reached in December 2015. This Directive calls for a cybersecurity solution in critical sectors, such as energy, transport,[39] health, finance, digital infrastructures and "digital service providers".[40] The NISD will require operators to be identified by Member States to take appropriate and proportionate technical and organisational measures to manage the risks passed to the security of networks and information systems they use in their operation. Those measures, which may be based on national or international standards, will be subject to audit by national authorities. The IoT Communication mentioned above suggests that 'operators using IoT may wish to adopt the Trusted IoT label as a demonstration of compliance, where relevant, to the NIS Directive's requirements. More generally, a Trusted IoT label could be developed for consumer products, providing transparency about different levels of privacy and security'. Such a labelling system has been implemented as regards energy-efficiency across the EU in a similar way as Safety Integrity Levels (SIL) are used across different industries on physical security. The Directive will also require them to notify the national competent authority or the Computer Security Incident Response Team (CSIRT) of incidents having a significant impact on the continuity of the essential services they provide.

In addition, under the new GDPR, data controllers should perform security assessments of systems as a whole, including

assessments at component level and applying principles of composable security. In the same way, use of certification for devices as well as the alignment with internationally recognised security standards could improve the overall security of the IoT ecosystem and minimise legal exposure. As mentioned above, in applying the 'privacy by design principle', most importantly, security needs to be by design as well, built-in from the very outset and be on top of standards.[41] For that purpose, the collaboration and alignment of regulators and certification entities is key, so companies across the whole value chain have comfort when manufacturing or commercialising software or apps.

Final thoughts

Summing up, privacy and security find a challenging field in the IoT with special sophistication in the automotive industry. Similar approaches are being taken in the US and in the EU. But the complex value chain and the seriousness of the cascade of liabilities that could emerge make this industry (together probably with e-health) the place where regulators should make the biggest effort to provide legal certainty when interpreting the way companies could be compliant in the most efficient way. The law has a challenge in exploring the new field of liabilities related to machine-to machine contracting, when bots or smart objects (cars) enter into contracts with each other on the basis of autonomous decisions.

The Amsterdam Declaration, the EU Commission IoT Communication and the eCall Regulation are good tools for understanding the state of play. However, where more interaction or pragmatic guidance will be needed will be when working on impact assessments, designing products and services or evaluating the state of the art and the costs of implementation in relation to the risks and nature of the personal data to be protected. *Knight Rider*, the American television series broadcast in the 80s and KITT, an advanced artificially intelligent, self-aware car, no longer seems to be science fiction.

Notes

1 5G Automotive Vision. 5G PPP, 20 October 2015

2 In this context, Ford CEO, Mark Fields announced at the MWC2016 that the company is evolving from an auto company to an auto and mobility company

3 See Oettinger's speech at WMC Roundtable on Connected Cars. 22 February 2016: 'The rollout of a cross-border virtual network based on 4G-LTE, and cooperating with ITS-G5 where available, dedicated to connected and automated driving. […] The virtual network would be extended and upgraded over time and the project would be opened up to additional companies'

4 Jack Palmer. Project Director Telematics Update (email news, 5 November 2014).

5 Telecom devices have evolved in a way that was difficult to imagine a few years ago. Smart meters, drones, cars, etc. How could these be a terminal device? They are telecom devices and this conclusion can be reached, walking through the MWC in Barcelona and getting into the dozens of cars exposed, but also, reading the EU Commission background to the public consultation on the evaluation and review of the Directive 2002/58/EC as amended by Directive 2009/136/EC (ePrivacy Directive), currently running. The Commission states that the notion of terminal equipment, mentioned by Article 5.3 of the ePrivacy Directive and defined in Directive 2008/63/EC, would include smart cars and smart meters, in addition to smart phones and computers. Consequently, the obligation of confidentiality of information stored in devices should extend to connected cars.

6 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). O.J.E.U. 4.5.2016

7 The ePrivacy Directive particularises and complements the general data protection framework, setting up specific rules concerning the processing of personal data in the electronic communications sector. At the same time, all matters concerning the protection of personal data in the electronic communications sector which are not specifically addressed by the provision of the e-Privacy Directive are covered by the Privacy Directive 95/46/EC, soon replaced by the GDPR

8 DSM strategy is composed by 16 initiatives that the EU Commission launched on 6 May 2015 <http://europa.eu/rapid/press-release_IP-15-4919_en.htm>

9 <https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive> the review aims, among other things, to review the scope of certain privacy and data protection requirements upon all terminal equipment attached to public telecommunication networks. Provisions related to security, traffic and location data and confidentiality of communications apply to such devices. The public consultation refers to IoT saying that 'more legal certainty may be needed with regard to the application of the e-Privacy Directive to the IoT solutions (Internet connecting devices among themselves), including to components, products, services and platforms that integrate everything in a communications network for digital processing'

10 Federal Trade Commission Staff Report on 19 November 2013 Workshop entitled 'The Internet of Things: Privacy and Security in a Connected World'. At that workshop, the FTC anticipated some best privacy practices, implementing the core principles of privacy by design, simplified consumer choice and transparency for the IoT world and announced then that its next step would be to prepare a report outlining recommended best practices for smart devices

11 The Article 29 WP is the independent EU Advisory Body on Data Protection and Privacy. It was set up under the Privacy Directive, and it is composed of a representative from the Data Protection Authority of each EU Member State, the European Data Protection Supervisor (EDPS) and the European Commission

12 Opinion 8/2014 on Recent Developments on the Internet of Things adopted on 16 September 2014. 14/EN WP 223

13 The Opinion focuses on three IoT developments: wearable computing, quantified self and home automation (leaving aside the specific problems of smart cities, smart transportation or M2M).
14 *Internet of Things. Privacy and Security in a Connected World.* FTC Staff Report, January 2015.
15 'Promoting investment and innovation in the Internet of Things. Summary of responses and next steps.'
16 12 February 2016, BoR (¡6) 39.
17 *'Transparency is crucial. As more and more of our devices become smarter and smarter, it is essential we know as much about them as they know about us – that we understand what information the devices are collecting and how it is being used or shared'.* Opening Remarks of FTC Chairwoman Edith Ramirez *'The Internet of Things: Privacy and Security in a Connected World'*, Washington, DC 19 November 2013.
18 Case C362/14, Judgment of the Court (Grand Chamber). 6 October 2015. Maximillian Schrems and Data Protection Commissioner
19 Bernard Benhamou
20 Digitising European Industry Reaping the full benefits of a Digital Single Market. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels, 19.4.2016 COM (2016) 180 final
21 SWD(2016) 110/2. COM(2016) 180
22 <https://ec.europa.eu/priorities/digital-single-market_en> accessed April 2016.
23 The Commission has launched work to facilitate and accelerate the deployment of connected and automated driving across the EU, including the work of the platform on Cooperative Intelligent Transport Systems and will deliver a masterplan in 2016.
24 The Free Flow of Data initiative aims to ensure that data can circulate without obstacles within the Union by removing unjustified restrictions to the location of data and by addressing emerging issues on data ownership (of non-personal data), (re)usability and access to data and liability among others in relation to the IoT. To deliver a single market for the IoT, the Commission services consider that it is essential to facilitate the flow and transfer of data across a series of steps: generation of data, transfer of data, storage of data, processing of data and provision of data services. This initiative will examine issues of ownership, interoperability, exploitation and access to data, including industrial data.
25 On March 2016, the US Department of Transportation's National Highway Traffic Safety Administration and the Insurance Institute for Highway Safety announced the commitment by 20 automakers representing more than 99 per cent of the US auto market to make automatic emergency braking a standard feature on virtually all new cars no later than NHTSA's 2022 reporting year, which begins 1 September 2022.
26 Annual report (94-page / 7.10MB PDF), Commission Nationale de l'Informatique et des Libertés (CNIL). On 23 March 2016, the Chairwoman of the French Data Protection Authority ('CNIL') opened proceedings that will lead to the release of a compliance pack on connected vehicles. The CNIL announced that the compliance pack will contain guidelines regarding the responsible use of personal data for the next generation of vehicles. It will assist various stakeholders in the industry prepare for the GDPR. Compliance packs are a new toolkit developed by the CNIL to identify and disseminate best practices in a specific sector while simplifying the formalities to register the data processing for organizations that comply with such practices. Therefore, compliance packs may include practical guidance, compliance tests and decisions issued by the CNIL laying down requirements to benefit from a simplified registration procedure. Compliance packs are drafted after consultation with multiple industry participants.
27 The Amsterdam Declaration includes actions to be taken by the EU Commission and by the industry. Among those corresponding to the industry are (i) to continue the initiatives taken by the automotive and telecoms industries to identify areas for possible cooperation to support investment in broadband communications and ensure network coverage and reliability; (ii) to investigate which performance and safety requirements should apply to mobile communications networks to facilitate connected and automated driving, in conjunction with short-range communications (ITS-G5) to facilitate hybrid communication.
28 'eCall' means an in-vehicle emergency call to 112, made either automatically by means of the activation of in-vehicle sensors or manually, which carries a minimum set of data and establishes an audio channel between the vehicle and the eCall PSAP via public mobile wireless communications networks.
29 Article 9 Working Party Working Document data protection and privacy implications in eCall initiative adopted on 26 September 2006. 1609/06/EN WP 125
30 Opinion of the European Data Protection Supervisor from 19 October 2013 on the proposal for a Regulation of the European Parliament and of the Council concerning type-approval requirements for the deployment of the eCall system and amending Directive 200//46/EC. EDPS recommendations were focused on the extension of eCall privacy obligations to private eCall and added value service. As a result, whereas (15) of the Regulation states that 'The mandatory equipping of vehicles with the 112-based eCall in-vehicle system should be without prejudice to the right of all stakeholders such as car manufacturers and independent operators to offer additional emergency and/or added value services, in parallel with or building on the 112-based eCall in-vehicle system. However, any additional services should be designed in such a way that they do not increase driver distraction or affect the functioning of the 112-based eCall in-vehicle system and the efficient work of emergency call centres. The 112-based eCall in-vehicle system and the system providing private or added-value services should be designed in such a way that no exchange of personal data between them is possible. Where provided, those services should comply with the applicable safety, security and data protection legislation and should always remain optional for consumers'.
31 Regulation (EU) 2015/758 of the European Parliament and of the Council of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service and amending Directive 2007/46/EC.
32 Article 6 states that the e-Call framework is without prejudice to data protection regulations, and that any processing of personal data through the 112-based eCall in-vehicle system shall comply with the personal data protection rules provided for in those rules.
33 Paragraph 9 of Article 6 states that 'Manufacturers shall provide clear and comprehensive information in the owner's manual about the processing of data carried out through the 112-based eCall in-vehicle system. That information shall consist of: (a) the reference to the legal basis for the processing; (b) the fact that the 112-based eCall in-vehicle system is activated by default; (c) the arrangements for data processing that the 112-based eCall in-vehicle system performs; (d) the specific purpose of the eCall processing, which shall be limited to the emergency situations referred to in the first subparagraph of Article 5(2); (e) the types of data collected and processed and the recipients of that data; (f) the time limit for the retention of data in the 112-based eCall in-vehicle system; (g) the fact that there

is no constant tracking of the vehicle; (h) the arrangements for exercising data subjects' rights as well as the contact service responsible for handling access requests; (i) any necessary additional information regarding traceability, tracking and processing of personal data in relation to the provision of a TPS eCall and/or other added value services, which shall be subject to explicit consent by the owner and in compliance with Data Protection Directive.'

34 Whereas (23): 'When complying with technical requirements, vehicle manufacturers should integrate technical forms of data protection into in-vehicle systems and should comply with the principle of 'privacy by design'.

35 The 112-based eCall in-vehicle system must not be traceable and not subject to any constant tracking. The e-Call in-vehicle system remains dormant (that means not connected to the mobile phone network) until a serious accident happens, and therefore, no tracking or transmission of data takes place during the normal operation of the system. Secondly, the Regulation limits the sharing of data processed through the 112-based eCall in-vehicle system and the Third Parties or private eCall in-vehicle systems and other added value services. Refusal of the data subject to give consent to the processing of his or her personal data for those third parties shall not create any adverse effects on the use of the 112-based eCall in-vehicle system.

36 Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection [COM(2006) 786 final – Official Journal C 126 of 7.6.2007].

37 Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

38 Network and Information Security Directive (2013/0027(COD).

39 The definition of transport given by the Directive does not include automotive, but includes traffic management control operators.

40 Online marketplaces (which allow businesses to set up shops on the marketplace in order to make their products and services available online), cloud computing services and search engines.

41 The Alliance for Internet of Things Innovation (AIOTI) has analysed most of the relevant work on IoT related to standardisation. The EU Commission has identified five areas for standardization efforts for achieving the DSM: 5G, Cloud Computing, the Internet of Things, Data technologies and Cybersecurity. On connected cars, in February 2014 ETSI and CEN already completed the basic set of standards requested by the European Commission to make connected cars a reality. The norms which they have adopted ensure that vehicles made by different manufacturers can communicate with each other.

Doil Son,
Yulchon, Seoul, Korea
dison@yulchon.com

Sun Hee Kim,
Yulchon, Seoul, Korea[1]
kimsh@yulchon.com

Self-Driving Cars: New Standard for Data Privacy Internationally and in Korea

Introduction: artificial intelligence and self-driving cars

Many of you will recall the historic match of Go (in Korean, 'Baduk') in March this year, between AlphaGo (a computer Go program developed by Google DeepMind) and Lee Sedol (South Korean, top professional Go player) which took place in Seoul, Korea.

In the five-game match, AlphaGo won all but the fourth game. According to Google, AlphaGo was trained on 30 million moves from games played by human experts until it could predict the human move 57 per cent of the time. Then, AlphaGo learned to discover new strategies for itself, through a process known as reinforcement learning.

AlphaGo's victory was a major milestone in artificial intelligence research, which has already started to transform our daily lives. The most notable example is in the automotive industry, in the form of autonomous cars (otherwise known as 'self-driving cars' or 'driverless cars'). The autonomous car is a classic example of artificial intelligence, in that the car uses its sensors to learn about its surroundings, and using its control algorithm, interprets the data and makes its own decisions to safely drive to its destination.

Major automotive companies (including Tesla, Audi, Hyundai, Jaguar Land Rover, Toyota) and Information Communications Technology ('ICT') companies (Google, Apple) are known to have made significant progress in the development of self-driving cars.

Legal discussions regarding autonomous cars usually involve civil and criminal liabilities in case of an accident, product liability exposure of vehicle manufacturers, insurance, legal requirements of the car, and data security issues. Among them, in particular, data protection

and cybersecurity issues will become of paramount importance, as the automated vehicles will have a high level of computer technology on board, and will be connected to the internet, other vehicles and their surroundings. In addition, autonomous vehicles will inevitably collect, process and store huge volumes of personal data.

Developments in the legal framework and government initiatives

In Korea, the Ministry of Land, Infrastructure and Transport (the 'MOLIT') announced its plan to commercialise autonomous vehicles by the year 2020, and designated six highway sections as testing grounds. Further, in July this year, a small city in the outskirts of Seoul (named 'Zero-City') will be designated as the testing ground for autonomous cars. This is known to be the first of its kind globally, in that an actual city will be used as the testing ground (other facilities, such as the 'M-city' of Michigan University, are known to be 'closed' test facilities, with access limited to only those involved in testing and research). For this reason, many global automotive manufacturers are known to have expressed an interest in testing their cars in 'Zero-City'.

The recently amended Vehicle Management Act of Korea (effective on 12 February 2016) provides the legal grounds for the issuance of temporary licences for the purpose of testing autonomous cars. In March, Hyundai Genesis acquired the first temporary licence.

The conditions for the temporary licence include, among other things, that the vehicle should be equipped with: (1) visual recording devices (resolution of 1280x720) which enable views of the front and the rear of the vehicle; (2) a vehicle function recording device; and (3) the technical measures to prevent unauthorised access or remote control of the car.

Below we will discuss data privacy concerns triggered by autonomous cars, followed by cybersecurity issues for the protection of the vehicle users.

Data privacy issues triggered by collection and sharing of data

Unlike Korea, some states of the United States (Nevada and California) do not require a visual recording device in the autonomous vehicle. United Kingdom law does not require, but permits, the installation of visual and sound recording devices in autonomous vehicles.

However, regardless of the legal requirement, it is possible that the vehicle manufacturers and/or insurance companies will require the visual and/or sound recording devices, for the purpose of analysing the cause of accidents, due to their increased exposure to liability. In the absence of human control, occurrence of an accident may often be seen as prima facie evidence of a defect in the vehicle.

The recording devices installed in autonomous vehicles will inevitably collect personal information of the vehicle users, as well as unrelated people passing by. The collected data may include, for example, visual images, voices, location, driving habits, and travel destinations. Any information which may be used to identify a person, either independently or in combination with other information, are generally defined as personal data. For this reason, the data recorded by the vehicles may also be considered to be personal data.

Of course, this issue is already in discussion to some extent in relation to the so-called 'car black box' in various countries. However, the scope of the collected data will not be comparable to the existing 'car black box', once the autonomous vehicle becomes commercialised. Also, the scope of data sharing will be unprecedented, as the collected data may be shared with government agencies, research institutions, and insurance companies. Vehicle manufacturers will need to transfer the data to offshore headquarters and data centres. Data may also be shared in the process of 'vehicle-to-vehicle' communication while driving.

In the face of new technology, the existing laws will become inadequate to regulate all aspects of the new environment created by the technology. For example, privacy regulations in many jurisdictions including Korea require prior written consent of the data subject, in order to collect, use, or transfer their personal data. An exception to the rule may be in respect of CCTV, where prior consent may be replaced by a noticeboard. However, it is practically not possible to obtain consent from the people passing by the driving car. Also, it may not be realistic to post a noticeboard outside the car.

Therefore, it will be necessary to specify in the law the nature of the personal data collected through the recording devices in the vehicles, and clearly regulate the scope

and method of collection, use, storage, and transfer of such information. Such rule should specify, among other things, the extent of information which may be shared in different circumstances. For example, the scope of information permitted to be shared with government agencies, insurance companies, and in 'vehicle-to-vehicle' communication must be regulated differently.

In this connection, the concept of pseudonymous data may be considered. In the case of the European Union, pseudonymous data and anonymous data are treated differently. 'Pseudonymising' means replacing the data subject's name and other identifying features with another identifier, in order to make it impossible, or extremely difficult, to identify the data subject. The encoded data is then treated as non-personal data, as long as its holder has no access to the 'key' to decode the data. We believe the same concept may be applied to ensure the safety of the personal information while allowing the vehicle manufacturers, governments and/or insurance companies, to utilise the data as required.

Safety of the car closely linked to data security

A few years ago, the notion of hacking a car over the internet to control steering and brakes seemed like science fiction. Today, the security research community has proven it to be a real possibility, and in July 2015 the first ever bill was introduced in the US addressing the automotive cybersecurity standards.

The bill would direct the National Highway Traffic Safety Administration to establish minimum security levels for any vehicle software in contact with physical driving controls, and requires car manufacturers to establish real-time monitoring to 'immediately detect, report, and stop' hacking attempts in their cars. The bill also requires the ability to disable data collection as it pertains to marketing and vehicle tracking. However, car manufacturers should prevent disabling of key functions, such as navigation, or vehicle safety systems like the Event Data Recorder used for tracking airbag deployment and other vehicle information in a crash.

The Korean data protection law is, generally speaking, considered to be one of the most stringent data protection laws in the world. However, the current data protection law does not contemplate the data security issues which may rise in relation to autonomous cars. The amended Vehicle Management Act and related government regulations also do not specifically address the cybersecurity standards for self-driving cars.

In the near future, the data protection laws will need to be reviewed and updated to ensure that the autonomous cars are equipped with the level of cybersecurity technology required to protect the vehicle users and third parties.

Closing remarks

Self-driving cars show the pinnacle of integration of state-of-the-art technologies in the ICT sector, including artificial intelligence, big data, and the Internet of Things ('IoT').

There is great anticipation that the commercialisation of self-driving cars will offer unprecedented benefits to humankind through drastic reduction in accident rates, not to mention the convenience of being freed from the steering wheel.

At the same time, data protection and cybersecurity will become growing concerns. The laws and regulations must be adapted in response to the increased challenges posed by autonomous cars.

However, if the car manufacturers must meet different privacy and security standards for each jurisdiction, the heavy compliance and cost burdens may actually deter the growth of the industry.

For this reason, we believe that there should be a uniform global standard concerning data protection and security for autonomous vehicles.

Note

* Doil Son is co-chair of the ICT Practice Team of Yulchon in Korea. Sun Hee Kim is a partner in the same team.

Connected cars – the Bulgarian perspective

Milka Ivanova
Djingov, Gouginski, Kyutchukov & Velichkov, Sofia, Bulgaria
milka.ivanova@dgkv.com

For some time now the automotive industry has been the next playing field for the new technologies. One such enterprise entering into this new area is the connected cars and related services industry. Such entry, irrespective if driven by the aspiration of the automotive industry to abandon the status of pure product provider or by the ambitions of the IT companies to develop new services (including autonomous cars), has a lot of business, policy-making and consumer potential. Yet it generates implications as well. The global market size for connected car components is estimated to equal €31.88bn in 2015 and is expected to reach €115.26bn in 2020,[1] but the development and implementation of connected cars and the related services involves a considerable number of players (the automotive industry integrating connected car solutions into the vehicles, the networks operators enabling high speed connectivity, the IT and software companies providing the hardware and software for the connected car features, consumers, various policy-makers), as well as a number of related issues, a significant part of which are subject to national and international regulation (eg, spectrum use, electronic communications services, road traffic regulations, personal data processing, consumer protection). Such complexity, combined with the market megatrends for safety, energy efficiency and the personalised experience of the new Generation Z drivers requires common understanding and clear rules – a need that is hampered by the involvement of many national regulators and their policy-making strategies.

In Bulgaria, as in many other countries, technical and economic development is always a step ahead of the legal regulatory regime. The issue creating a challenge to the Bulgarian telecoms regulator in the context of connected cars and related services is the unclear strategic approach in relation to qualifying those services from a communications regulation point of view. In theory, those services match the characteristic features of electronic communications services but do not fully fit in to the currently effective Bulgarian electronic communications framework, which is defined around more straightforward services and concepts for connectivity.

Connected car services as (potentially) regulated services

The Bulgarian Electronic Communications Act ('ECA') defines an electronic communications service ('ECS') as 'a service, usually provided for remuneration, which consists wholly or mainly in conveyance of signals over electronic communications networks, including transmission services, provided through broadcasting networks, excluding services, related to content and/or the control over it.[2] In the light of such definition a service would be qualified as ECS where such service meets two basic criteria, that is, where a service involves 'wholly or mainly' the 'conveyance of signals' through an electronic communications network. On the other hand, the analyses of those two criteria is contingent on many factual elements related to the technical set up of the particular service (eg, the detailed technical process by which the signals are conveyed from the vehicle to the corresponding equipment) and the regulator's approach as to the connotation of 'wholly or mainly' (eg, with respect to the quantitative and qualitative benchmarks of the service needed to qualify it as consisting wholly or mainly of conveyance of signals). In view of such legislative criteria, the Bulgarian telecoms regulator - the Communications Regulation Commission ('the CRC') - has developed a case-by-case approach to determining whether the conveyance of signals relates to the whole or the main part of the service.

Connected cars are vehicles that use connectivity (conveyance of signals) in order to optimise a vehicle's own operations and maintenance and to enhance the customer's overall in-car experience. In that respect the connectivity is a crucial part of connected car services. It might be provided either by the connected car services provider (under

such circumstances the connected car service provider should have the capacity of an ECS provider as it will be engaged in the conveyance of signals) or by a third-party provider. In practice the provision of ECS services is not a usual part of the automotive industry scope of activities. Therefore, in order to avoid the burdensome regulations in the telecommunications area, most companies do avoid providing the connectivity themselves and rather project their services using third party connectivity. Based on such a factual set up, where the data and voice connectivity inherent for the connected car services are technically provided by an ECS provider (eg, a mobile service provider) and the provider of connected car services is not engaged in the conveyance of signals, the connected car services should not qualify as an ECS under Bulgarian law.

Yet this is rarely the reality. The connected car service is a complex service that could hardly fit in to the straightforward model of a single entity providing a single service. Therefore, the CRC would have to assess the service in accordance with the currently existing statutory rules which categorise it as either an ECS or a non-ECS service. To begin with, irrespective of the fact that the connectivity is actually provided by a third party (a mobile network operator) the connected car services provider offers the service to the end customer as its own service, with the underling technical telecommunications functionalities (the connectivity provided by the MNO) being an integral part of such service. In view of this, in case the CRC chooses to assess whether from a functional point of view the service includes conveyance of signals (ie, the 'technical' approach), there is huge potential to claim that the connected car service is an ECS. Such approach would be supported also by the fact that connected car services use connectivity that under Bulgarian law would be qualified as electronic communications services per se. This is because the data transfer services are part of the services listed in the *list of the networks and services by virtue of which electronic communications services under general rules shall be provided.*[3] In addition, connected car services are chargeable (a fee is paid to use the service) and offered on a commercial basis (they are part of the service offered with the purpose to generate profit), while Bulgarian law qualifies as 'undertaking providing public ECS' any legal entity that carries out electronic communications in a commercial manner.[4] In the light of the above legal reasoning, it is not at all impossible for the Bulgarian regulator to substantiate that connected car services do have the characteristics of electronic communications services.

Challenging the 'technical' approach

As a general rule the CRC is not among the most active regulators[5] where challenges of the new technologies are concerned or where a particular position on a legal matter should be stated officially or publicly. Furthermore, no public records for court practice, public discussions, legal research under Bulgarian law, or the official position of the regulator as to the qualification of services similar to connected car services can be identified. Irrespective of this, the position that under Bulgarian law connected car services are not ECS and should not fall under the relevant regulation has grounds under the following theoretical legal reasoning.

Connected car services are not ECS in nature or in scope

All connected car services - the potential for autonomous driving, safety and entertainment features, wellbeing and vehicle management features, mobility management and home integration - are services using underling technical telecommunications functionalities. Although integral and necessary, such telecommunication functionality is not the main part (or the key feature) of the connected car service. Given the description and purpose of the various connected car services, they, as a service, are focused on the content (real time traffic information is aimed at gathering information and using such information (usage data) with the purpose to manage the mobility), rather than on the connectivity (mobile connectivity is only the technical means for transfer of the data that is gathered or used for purposes other than the mere conveyance of signals). If viewed from such perspective as a contrast to the 'technical' approach, the connected car services should not be comprehended as a service consisting either 'wholly or mainly' in conveyance of signals.

Connected car services are not necessarily public ECS

Pursuant to Bulgarian law 'public electronic communications' means ECS available to the entire society. Indeed, the term 'entire society' in a very broad sense might be interpreted as 'to any third party' (ie, not for the undertaking's own needs). On the other hand, it seems that (at least for a certain period) connected car services would be available not to the 'entire society', but only to a particular set of customers – currently those customers that have purchased a vehicle made by a particular manufacturer that has 'organised' the complexity of relations enabling the connected car service, which vehicle, in addition, is equipped with the necessary equipment (including that which will enable the connectivity).

Given such purely theoretical legal reasoning, the position that under Bulgarian law connected car services are not subject to electronic communications regulation might be considered. Indeed, given the service is rather new and constantly evolving, the basis for such legal reasoning might prove to be inaccurate from the point of view of the factual and technical set up of the particular service. Yet in view of the would-be implementation of the eCall service and the input gathered during the public consultation on the evaluation and the review of the regulatory framework for electronic communications networks and services[6] held by the European Commission in the end of 2015, the CRC sooner or later will have to align itself to one side or the other because sitting on the fence will no longer be an option.

Notes

1 Viereckl, Ahlemann, Assmann & Bratzel, 'Racing ahead & The connected C@r 2014 study' (2014) Strategy& Formerly Booz & Company; available at http://www.strategyand.pwc.com/media/file/Racing-ahead.pdf.
2 The definition has been set forth in s 17 of the ECA's Additional Provisions.
3 Issued by the regulator and published in the State Gazette # 63, dated 17 August 2012.
4 As per the definition of s 50 of the ECA's Additional Provisions.
5 Unlike other regulators in Bulgaria the statutory acts and the internal rules and regulations regulating the activity of the Communications Regulation Commission does not provide for giving opinions or issuing guidelines and therefore the regulator rarely feels compelled to clarify its regulatory approach.
6 https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-regulatory-framework-electronic.

The Dubai example: can dedicated regulation foster the development of more efficient /safer networks and cities?

Diane Mullenex, Pinsent Masons, UK
Diane.Mullenex@pinsentmasons.com

Guillaume Bellmont, Pinsent Masons, France
Guillaume.Bellmont@pinsentmasons.com

Although the concept of what a smart city is varies across countries and regions, traditionally it was construed as a place where the population gains from infrastructure and services increasing in efficiency, particularly through the use of telecommunication and technology. Recent investments in smart cities in the Middle East demonstrate how ubiquitous the issue of connectivity (and backbone networks) is, but also provide an interesting example of a regulatory attempt at addressing societal changes.

Amongst the myriad of smart city projects across the globe, the Dubai initiative, simply labelled 'Smart Dubai' constitutes a unique example of how the reflexion about dedicated regulation of smart services may set a benchmark for future similar projects across the globe.

A holistic approach in the design of the smart city

Whereas many projects around the globe (in Peterborough, Amsterdam, etc) have been

focused on certain aspects of what a smart city can be (and mostly on smart grid and energy efficiency), the Dubai Smart City project is particularly interesting in the way that it took a very global approach to the objectives to be met and the type of services which may form part of the new city.

For telecom lawyers, the most striking feature of this project is the important role left to regulation, which has been considered as a core issue of the project and which resulted into specific regulation being adopted to cover the future use of services within the smart city, as well as anticipating the benefits of rolling out such a big project.

An increased focus on data privacy: from big data to open data

The Dubai Data Law (Dubai Law No. 26/2015) was published last December in an attempt to steer the Emirate further towards its goal of being the smartest city – a motive of which is made fundamentally clear in the objectives of the law, the first of which is to 'enable the Emirate to achieve its vision in transforming Dubai into a smart city' (Article 4(1)).

This law anticipates that a smart city cannot just be a juxtaposition of 'hermetic' smart services but ought to be a forum for all smart services to communicate with one another so that the greater output and benefits can be extracted from the infrastructure and smart services. Dubai has therefore created the legal framework promoting data sharing at city level, anticipating the need for open collaboration between authorities and private stakeholders.

In more details, the law provides that Dubai data shall be classified into open and shared data, and open data is defined as 'Dubai-related data which may be published without restrictions or with the minimum restrictions specified by the competent authority in this regard'. The law is still very much in its early stages and we are unaware of the full extent of its application; however the Dubai-specific law is a clear indication of Dubai's recognition of the need for legislation to continuously evolve and mirror the progress of a smart city.

The law guarantees the right to privacy of individuals (Article 13). What can therefore be anticipated is that data to be shared shall be anonymised. However, aggregated anonymised data collected by shareholders shall be shared and made available publicly or amongst stakeholders.

This can be anticipated to be an issue for public authorities, which will have to be cautious about the type of data they thus send in the cloud. This will require on their side a thorough classification exercise of their data to ensure that the most secure information is not to be shared and potentially accessible by any third party.

A practical and technical framework for data sharing should be progressively built, as the Dubai Data Establishment (which is under the supervision of the Dubai Smart City Office) will progressively take its responsibilities.

Ultimately, although this framework fosters increased efficiency around all smart cities, it also increases the risks of network security and cybercrime issues, given the number of information sharing points. Those will need to be further addressed in the local regulations.

Network security and cybercrime regulations

The exponential exchange of data on individuals and businesses is likely to attract cyber-criminals. This is likely to further foster discussions on communications regulations and the extent to which data can be accessed and/or monitored by law enforcement authorities for the prevention of crimes. Will it have an impact on the definition of lawful intercepts? Will it result in on-going monitoring or filtering of information? If the question to the above is uncertain at the moment, the development of smart cities has nonetheless already triggered a review of cyber security regulations in the region.

Although the latest developments on open data are fairly recent, many smart services have been available for a few years (mostly since 2013). The current trajectory shows that a number of services have improved as a result of the implementation of smart systems: connectivity is the neural network of any smart city and the UAE has one of the most advanced fibre optic networks; building information modelling is streamlining projects and preventing disputes in the booming construction sector and Dubai's commitment to smart initiatives is facilitated by the Dubai Smart City Office, an entity specifically established to aid the advancement of ICT infrastructure.

Cybercrime has long been a security threat to the Middle East, and the rise of a smart city can be a hotbed for crime as cyber criminals find it easier to attack internet infrastructure. The UAE is increasingly facing these attacks and has responded to

the threat through Federal Law No. 5/2012 (the 'Cybercrime Law'). This bolsters the older Information Technology Crime law (Federal Law No. 2/2006) (the 'Old Law') by imposing higher penalties, ranging from fines to imprisonment, on wrongdoers. Under the Old Law, a 'wilful act' was required create an offence for illegally accessing an electronic site. The Cybercrime Law removes the intent element and lowers the standard of wrongdoing to anyone who 'gains access to a website, an electronic information system, computer network or information technology means without authorisation or in excess of authorisation or unlawfully to evidence wrongdoing' (Article 2). Misuses of social media as well as gambling activities and materials that 'prejudice public morals' have been incorporated into the purview of the law.

Creating additional categories of cyber crimes and further defining the classifications for violating the privacy of others is a nod to cyber criminals that the authorities remain vigilant against cyber attacks. However as with much recent UAE legislation we are yet to see the full extent and application of the law in the context of high-level cyber crime. Instead we have seen the law applied in relation to day-to-day activities, where individual's have been charged for offences ranging from possessing a photo taken without the subject's consent; posting insulting remarks on social media or any form of electronic abuse through personal forums such as Whatsapp.

With the backdrop of the World Expo 2020 and Vision 2021 in mind, a number of projects are in the pipeline to enhance the development of the UAE's smart city initiatives. While a more defined and thorough regulatory framework could provide greater transparency and help build a culture of awareness in light of the vast amounts of data that is currently held on data collection platforms; the UAE's progress on a whole is remarkable for a country that is only 44 years old.

Even more, the Middle Eastern example, where smart city projects and regulations evolve in parallel, may illustrate a more global need for dedicated regulations ahead of the project. Regulatory constraints shall be anticipated and evaluated from the onset of the project, as part of the master planning, so that authorities are in position to enact appropriate legislation to regulate on the usage of the networks and services to be rolled out.

EU roaming regulation IV: implementation challenges ahead

Laurent De Muyter
Jones Day, Brussels, Belgium
ldemuyter@jonesday.com

Henry de la Barre
Jones Day, Brussels, Belgium
hdelabarre@jonesday.com

Introduction

On 30 April 2016, the fourth Roaming Regulation 2015/2120, adopted on 25 November 2015, ('the Regulation') becomes applicable across the European Union. The key concept introduced by the Regulation is simple: no more roaming charges. However, implementation may prove much less simple. The Regulation introduces concepts such as the 'roam like at home' ('RLAH') principle and other rules, which raise questions as to their proper implementation, even if the Body of European Regulators for Electronic Communication's (BEREC's) updated Roaming Guidelines of February 2016 already provide certain clarifications.[1] This paper will first summarise the Regulation's main changes and, second, will discuss some initial practical issues raised by its implementation.

Key changes under the Regulation

RLAH

The Regulation's centrepiece is the abolition of roaming surcharges as of 15 June 2017, subject to (1) a transitory period between 30 April 2016 and 15 June 2017, establishing a

new maximum retail price cap; (2) a review of the regulation of wholesale roaming charges; and (3) two exceptions that will apply after the transitory period.

TRANSITORY PERIOD

As of 30 April 2016, new maximum retail roaming prices will be imposed via two price caps:

- A maximum surcharge cap (ie, the maximum charge to be added to the domestic price for the provision of the roaming service), constituting: 5 eurocents/minute for calls made, 1.14 eurocents/min for calls received,[2] 2 eurocent/SMS sent, and 5 eurocents/MB used (all VAT excluded). This is equivalent to the wholesale price caps already applicable since July 2014.
- A maximum total price (ie, domestic price + the surcharge), constituting: 19 eurocents/minute for calls made, 1.14 eurocents/min for calls received, 6 eurocents/SMS sent, and 20 eurocents/MB used (all VAT excluded). This is equivalent to the retail price caps already applicable since July 2014.

In addition, SMS received should be free of charge. Recital 30 of the Regulation indicates that such changes do not trigger the right for consumers to anticipatively terminate their contracts. Such tariffs are applicable by default to all customers. Still, operators can also offer alternative roaming tariffs, provided that customers can switch back to regulated tariffs at any time.

REVIEW OF WHOLESALE ROAMING

For RLAH to be fully applicable in 2017, the Commission must adopt legislation that will revamp wholesale roaming charges. Such process started with a consultation in November 2015,[3] including a BEREC Report on the wholesale roaming market, published on 12 February 2016[4] and will continue with a Commission report and legislative proposal on 15 June 2016. The Commission also launched a study of the cost of wholesale roaming.

EXCEPTIONS

Even when RLAH is applicable, two exceptions will remain:

1. Fair use policy
   To prevent abusive or anomalous use of retail roaming services by customers (eg, for purposes other than periodic travel), the Regulation provides for the possibility to include a fair use policy in the contracts, including a quota of the roaming units (minutes/SMS/MB) and roaming surcharges to units used in excess of those quotas. The Regulation further sets out that, in such a case, the two pricing caps discussed above for the transitory period will apply.
2. Sustainability of the charging model
   After obtaining authorisation from their national regulatory authority, operators may apply a roaming surcharge, even above the pricing caps, if, and to the extent that, the surcharge is necessary for the sustainability of their domestic charging model. However, this can only be done in 'specific and exceptional circumstances'. The Commission is expected to issue implementing decisions in relation to these exceptions.

Transparency obligations

Existing transparency obligations have been extended to include (1) information on any applicable fair use policy or surcharge under the sustainability exception when a customer enters another Member State (but not outside the European Economic Area), and (2) an obligation to inform the customer when the applicable fair use volume is fully consumed or any usage threshold is reached, as well as to communicate the applicable surcharge once that volume or threshold is reached.

Abolition of de-coupling for voice and SMS

Under the Regulation, the de-coupling obligation, whereby operators were required to enable customers to access voice, SMS and data roaming services provided by alternative roaming providers, is now limited to data roaming services.

Practical issues

Several questions and issues have already emerged with respect to implementation of the Regulation, including in relation to (1) the notion of 'domestic price'; (2) 'price caps'; (3) calls to special numbers; and (4) transparency obligations.

Domestic prices

In practice, identifying the 'domestic price', which must serve as the reference for roaming tariffs, can prove difficult. This is

especially complex in the context of tariff plans offering different on-net and off-net tariffs, or tariff plans offering unlimited or free volumes of calls.

Article 2(2) r of the Regulation defines 'domestic price' as the operator's domestic per unit charge applicable 'to calls made and SMS messages sent (both originating and terminating on different public communications networks within the same Member State) and to data consumed by a customer'. In case of different on-net/off-net pricing, the 'domestic price' is the off-net tariff.

With regard to bundles, the Regulation further states that 'in the event that there is no specific domestic retail price per-unit charge, the domestic retail price shall be deemed to be the same charging mechanism as that applied to the customer for calls made and SMS messages sent (…) and data consumed in that customer's Member State'. This means that for tariff plans including unlimited or free minutes/SMS/volume, roaming calls should be included in such free minutes/SMS/volume. As long as such minutes are not consumed, only the roaming surcharge may be charged (where applicable).

A potential consequence of this approach is to favour on-net/off-net differential at domestic level, as the Regulation would allow applying low or free domestic on-net tariffs while still benefiting from higher roaming tariffs (based on off-net calls) for such on-net (roaming) calls. Such development seems at odds with the Mobile Termination Rate ('MTR') Recommendation 2009/396/EC, which precisely aimed at reducing on-net/off net differentials.

Price caps

The two price caps referred to above are cumulative, in that (1) the first applies to the roaming surcharge only, and (2) the second to 'the sum of the domestic retail price and any surcharge applied'. Consequently, in cases where no roaming surcharge is applied, it would be possible to apply a retail roaming tariff exceeding the total price cap. In other words, an operator could set its roaming tariff as high as it wished, as long as it remained equivalent to the domestic tariff. This is a simple reflection of the fact that the Regulation does not regulate domestic tariffs.

Calls to special numbers

Where roaming tariffs are set at the level of the domestic price, the question arises as to the applicable tariffs for roaming calls to special numbers, such as for voicemail, prepaid reload services, customer services, and value-added services ('VAS') or premium-rate services ('PRS'):

VOICEMAIL CALLS

Domestic calls to voicemail are often free. Nonetheless, they trigger wholesale costs for the operators when used in roaming. Article 6e of the Regulation states that 'roaming providers shall not apply any surcharge to a regulated roaming SMS message received or to a roaming voicemail message received. This shall be without prejudice to other applicable charges such as those for listening to such messages'. Although the Regulation does not clarify such 'other applicable charges', calls to access voicemail are likely to be considered as regular roaming calls, and thus subject to the Regulation's general pricing scheme (surcharge during the transitional period, and domestic tariffs subsequently).

RELOADS/CUSTOMER SERVICES

Domestic calls to prepaid reload services or to customer services are generally free. Again, however, these can trigger wholesale costs when used abroad. The Regulation provides no specific rules for such calls. Such communications are thus to be considered as regular roaming communications and are therefore subject to the Regulation's general pricing scheme, including the possibility of a surcharge (when applicable). As an exception however, Article 14 of the Regulation provides that operators must make available, for free, a number for obtaining detailed roaming tariff information and information on accessing emergency services.

VAS/PRS

Domestic calls to VAS/PRS are often much costlier than off-net domestic calls, as they must reflect the costs incurred by operators to the benefit of the content service providers. Recital 43 of the Regulation specifies that it does not apply 'to the part of the tariff that is charged for the provision of value-added services but only to the tariffs for the connection to such services'. This means that price caps for voice calls, SMS and data services are limited to the price

of the connection to the VAS and are not applicable to the service of the content provider itself. The BEREC Roaming Guidelines confirm this and advise that if operators offer VAS, they 'should ensure that consumers are informed about how any premium rate services (PRS) expenditure is tariffed, charged and controlled'.

'Customer' to be informed for transparency obligations

The Regulation's transparency obligations essentially benefit 'customers'. In some cases, however, identifying the 'customer' raises difficulties. For example, for corporate or family contracts, the contracting party and the actual holder of the SIM card are often two different persons. However, while the EU framework defines the notions of 'user', 'consumer', and 'subscriber', it does not define 'customer'. BEREC's Roaming Guidelines (BoR (16) 34) recognise this and suggest that operators 'may construe it to mean the contracting party or an individual SIM holder', provided that operators clearly indicate the chosen interpretation (eg, as set out in the contract, on their website, etc.). Some flexibility exists as to the person who is to be considered as the beneficiary of the transparency measures. However, we believe that the customer should be identified on the basis of the purpose behind the type of transparency obligation.

INFORMATION WHEN TRAVELLING SHOULD BE DELIVERED TO THE SIM CARD HOLDER

The Regulation states that a customer must be provided with pricing information: (1) by Message Service for voice calls and SMS when he enters another Member State; or (2) on the customer's mobile device for mobile data every time the customer initiates a data roaming service for the first time in another Member State. The purpose of such obligation is 'to help roaming customers make decisions on the use of their mobile devices while abroad' (Recital 82 of the Regulation). Thus, the SIM card holder should logically receive the information on his mobile device (and not the contracting party).

INFORMATION 'WHEN SUBSCRIPTIONS ARE TAKEN OUT', AND 'EACH TIME THERE IS A CHANGE IN THE CHARGES' SHOULD BE DELIVERED TO THE CONTRACTING PARTY

Such obligations seek the provision of information that must 'be clear, understandable, permit comparison and be transparent with regard to prices and service characteristics' and can 'be provided on the invoice' (Recital 83 of the Regulation). Thus, this set of provisions appears to relate to the actual subscriber, that is, the contracting party.

INFORMATION ABOUT VOLUMES AND FAIR USE

Such obligations seek to 'monitor and control expenditures' (Recital 84 of the Regulation), as well as to 'provide customer information on how to continue using data services' (BoR (16) 34). Thus, it is unclear whether such notification could be sent to the SIM card holder or to the contracting party. Both options therefore seem possible, provided the operator makes its choice transparent.

Notes

1 BoR (16) 34.
2 Commission Implementing Regulation 2015/2352.
3 The results of the consultation were published in March 2016; available at https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-review-national-wholesale-roaming-markets-fair-use-policy.
4 BoR (16) 33.

International roaming: should it be regulated by NRAs and its cost reduced?

Alfonso Silva
Carey y Cia Ltd,
Santiago, Chile
Asilva@carey.cl

Raúl Mazzarella
Carey y Cia Ltd,
Santiago, Chile
rmazzarella@carey.cl

Introduction

One of the most common issues for travellers during their trips abroad is the high price of voice calls and mobile data transmission services outside the geographical coverage area of the network of their local Mobile Network Operator ('MNO'), by means of using a visited network of a foreign MNO in a seamless and secure manner. This is the so-called 'International Roaming Problem'.[1]

In order to find a solution to this problem, some travellers often decide to buy a SIM card of a foreign MNO in the foreign country; others only use their devices with a Wi-Fi connection, and others enter into special agreements with their local MNOs in order to diminish, as much as possible, the cost involved. Mid-market and large companies also try to diminish their costs in this regard, modifying mobile employees' behaviour in ways that allows the lowering of their usage of voice calls and data roaming when they are travelling abroad.[2]

The questions that immediately arise about this problem are: why is the cost for international roaming often considered so high by customers? Can this cost be reduced? Does this cost need to be reduced in order to increase consumer protection?

The telecommunications authorities across the globe have taken different approaches regarding these questions. Some of them have already taken measures and adopted plans that have contributed to effectively diminish the roaming cost and others have opted or preferred to avoid the issue.

The debate about the cost of international roaming

MNOs often claim that infrastructure and range are expensive assets and that they need to be financed. They also argue that the interconnection costs and the wholesale rates they charge each other - to allow subscribers' access to each other's networks - also implies a high cost for them. Likewise, they state that, to the extent that the retail market is competitive, the prices are competitive, too.[3]

Opponents of the high price of international roaming argue that margins of profit on domestic data services are often low because of the high level of competition within each country, so that the MNOs then overcharge their customers when they travel abroad in order to make some extra profit.[4]

They also set forth that large MNOs benefit more from this system, due to the fact that they are more likely to have other operators' customers using their networks than the other way around. In this regard, they claim that the customers of these large MNOs are more likely to use the network of the same MNO in different countries, in which case these MNOs would be negotiating the wholesale roaming prices with their affiliates companies; however, the roaming cost of such customers will not be reduced.[5]

In the same manner, some minor MNOs have argued that it is true that MNOs do need to incur additional expense to provide international data roaming, but such roaming retail prices have no direct correlation with the real costs of the data transport.[6]

Some of the possible solutions proposed by the opponents to the high price of international roaming are: more competition; the possibility of licensing more foreign mobile virtual network operators ('MVNOs'); a global roaming regulation, among others. Some of them have been vociferous in promoting the latter and have stated that 'directly regulating roaming prices may be the only way to guarantee that consumers are not unreasonably charged. The aim of this intervention should be to protect consumers and remove international barriers for trade and travel.'[7]

Some MNOs have counter-argued these arguments, stating that years of this debate has led customers to approach international roaming with a very defensive attitude. They claim that around a third of travellers using

international roaming turn their phones off and most of them use it a lot less than at home. In practice, this has reduced a relevant portion of the international roaming demand. MNOs suggest that people think that roaming is more expensive that it actually is. They state that international roaming has been heavily decreasing its prices in recent years and, for this reason, the possible solution – in their opinion – would be to exhibit more transparency in the prices they already charge (eg, with alerts and cut-off limits) because the application of price caps by specific regulation has not stimulated activity in retail voice roaming and are quite difficult to apply to retail data services. Also, excessive protection of the consumers in this matter could affect the innovation and competition between MNOs. Other MNOs state that competition is the only remedy for this situation and that the only way to achieve it is by letting the customer buy roaming services from an MNO (national or international) different from its local usual MNO. This is called 'separation' of services.[8]

Finally, others have said that any regulation in the international roaming market will lead to an increase of the prices of local MNOs services, which would obviously have a very pernicious effect for the relevant market.[9]

These are just some of the arguments put forth in relation to this interesting issue and reflect that the debate is still far from being settled.

NRAs point of view

As a general rule, international roaming is not regulated by the National Regulatory Authorities ('NRAs') worldwide and its prices have been freely determined by the market.

The most relevant exception has been the European Union. Since 2007 the retail roaming and the wholesale rates that companies charge each other have been reduced in the EU. The latest regulation in this regard is the 2012 European Commission Regulation (Regulation (EU) N°531/2012 of the European Parliament and of the Council).[10] This regulation takes a side in the debate and sets forth that, for consumers, the high level of prices 'acts as an obstacle to using their mobile devices when travelling abroad within the Union and is a matter of concern for consumers, national regulatory authorities, and the Union institutions, constituting a significant barrier to the internal market.'[11] The regulation also states that:

> 'the excessive retail charges are resulting from high wholesale charges levied by the foreign host network operator and also, in many cases, from high retail mark-ups charged by the customer's own network operator. Due to a lack of competition, reductions in wholesale charges are often not passed on to the retail customer. Although some operators have recently introduced tariff schemes that offer customers more favourable conditions and somewhat lower prices, there is still evidence that the relationship between costs and prices is far from what would prevail in competitive markets.'[12]

The final objective of the regulation seeks to increase competition between the MNOs in the EU internal market.

On 25 November 2015 an amendment of the Regulation (EU) No 531/2012 was adopted by means of the issuance of Regulation (EU) 2015/2120[13] of the European Parliament and of the Council. One of the most relevant aspects of this modification is that it states that roaming charges will be abolished in the EU as of 15 June 2017. From that date, the domestic retail price shall apply for this kind of services. However:

> 'roaming providers should be able to apply a 'fair use policy' to the consumption of regulated retail roaming services provided at the applicable domestic retail price. The 'fair use policy' is intended to prevent abusive or anomalous usage of regulated retail roaming services by roaming customers, such as the use of such services by roaming customers in a Member State other than that of their domestic provider for purposes other than periodic travel. Any fair use policy should enable the roaming provider's customers to consume volumes of regulated retail roaming services at the applicable domestic retail price that are consistent with their respective tariff plans'.[14]

Regarding this debate, it is interesting to note that during the discussion of this modification, Jean-Claude Juncker, European Commission President, in an interview with a German newspaper regarding this matter said: 'now it is up to the Member States if they want to be the lawyer for the citizens and consumers or for the telecom companies'[15].

At the same time, Eastern European countries, where local prices are cheap, were worried that their MNOs would be forced to increase local prices if

international roaming charges were removed prematurely, since such MNOs pay wholesale charges to other operators when their customers travel abroad.[16]

International Roaming in Chile

The new EU regulation has reopened this debate around the world. In Chile, just like in most of the other countries, there are no regulations regarding this matter. However, minor companies like VTR or WOM (former Nextel) have openly showed their opposition to the current price structures of international roaming.

Chris Bannister, CEO of WOM has stated that the prices are 'absurd and abusive'.[17] He has also declared that he has offered to most operators a wholesale price of US$30 for British pound, but with a very limited response so far. He claims that if prices are reduced to just US$50 for British pound the MNOs would anyway have a profit of five times the local tariff. He has also declared that travellers seek other types of connectivity in their journeys due to the high roaming prices, a reason why new alternatives for connectivity could arise affecting the international roaming business. In his opinion there are three solutions to this problem: (1) to regulate the matter, just as in the EU; (2) to include the Global System for Mobile Communications Association (GSMA) in the discussion and; (3) to make an industry agreement.[18]

The head of our Undersecretary of Telecommunications (the Chilean NRA or 'Subtel'), Pedro Huichalaf, has said in this regard that:

> 'Today, there are no economic or technical reasons for the high prices of international roaming. It is worth noted that the price of international roaming is established by the MNOs in collaboration agreements between them. We, as the authority, cannot regulate roaming prices but if this is not resolved soon, a statutory or regulatory initiative should be considered.'[19]

Subtel is currently negotiating with Argentina and Peru the elimination of international roaming between Chile and those countries.

The debate will continue, but MNOs should be aware that if they continue with their current market practices and do not voluntarily reduce their international roaming tariffs to reasonable levels, international roaming will most likely be regulated or even abolished by NRAs in the next few years, following the EU pattern, and such tariffs substantially reduced or eliminated, ending the international roaming business model known to date.

Notes

1 *'The International Roaming Problem: How to Balance Cost, Connectivity, and Security Concerns' commissioned by Truphone (Study of November 2012), available at https://www.truphone.com/Global/Whitepapers/CCMI%20Truphone%20Midmarket%20Whitepaper%20Nov%202012.pdf.*
2 *Ibid p 2.*
3 'Symposium on International Mobile Roaming' (presentations and background documents) available at https://www.wto.org/english/tratop_e/serv_e/sym_march12_e/sym_march12_e.htm.
4 *'Why data roaming costs too much' (Press release, 29 March 2011) available at http://www.zdnet.com/article/why-data-roaming-costs-too-much/***.**
5 *Ibíd.*
6 *Ibíd.*
7 OECD (2010), 'International Mobile Roaming Services: Analysis and Policy Recommendations', OECD Digital Economy Papers, No. 168, OECD Publishing. http://dx.doi.org/10.1787/5kmh7b6zs5f5-en OECD, **at p. 5.**
8 See n 3 above.
9 'Europe split on abolition of mobile roaming charges' (Press release, 3 June 2015) available at http://www.euractiv.com/section/digital/news/europe-split-on-abolition-of-mobile-roaming-charges/.
10 Regulation (EU) No 531/2012 available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32012R053.
11 *Ibid.*
12 *Ibid.*
13 Regulation (EU) 2015/2120 available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015R2120.
14 Regulation (EU) 2015/2120 available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015R2120.
15 'Greece and Bulgaria against the abolition of roaming in the European Union' (Press release, 3 June 2015) available at http://www.grreporter.info/en/greece_and_bulgaria_against_abolition_roaming_european_union/12797.
16 See n 9 above.
17 'Wom propone rebajar tarifas de roaming a niveles de Europa' (Press release, 31 March 2016) available at http://www.litoralpress.cl/design3/lpi/mostrarjpg.asp?id=36564782&idT=181&carp=&ve=0.
18 *Ibid.*
19 'Eliminar el roaming en Sudamérica' (Press release, 31 October 2015) available at http://www.nexchannel.cl/Nex/noticias/noticia_video.php?nota=13366787.

Sajai Singh
J Sagar Associates, Bangalore
sajai@jsalaw.com

Net neutrality: prohibition on differential pricing

India had recently witnessed a flurry of debates around the topic of net neutrality, all of which were put to rest with the issuance of the Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016 (the 'Regulations') by the Telecom Regulatory Authority of India (TRAI). The Regulations are the product of widespread objection to telecom service providers' (TSPs) inclination towards charging users different prices for data services on the basis of the accessed content.

On 9 December 2015, the TRAI released a consultation paper on *Differential Pricing for Data Services* (the 'Consultation Paper'), detailing the pros and cons of adopting a content-based differential pricing methodology, and inviting comments from the general public and stakeholders on questions that were raised in this regard.[1] Naturally, TSPs were in general agreement with the implementation of the proposal. However, the vast majority of users, in addition to several corporates and organisations, recorded their objections.

Highlights

The Regulations appear to be in consonance with the public view and expressly prohibit TSPs from charging discriminatory tariffs for data services on the basis of content (website, application, platform or other types of content) being accessed by the user. The Regulations further mandate that TSPs cannot enter into arrangements, such as zero rating and reimbursement of data used on certain websites, that have the same effect as charging discriminatory tariffs, thus also restricting indirect circumvention. In view of the said prohibition, projects such as Facebook's Free Basics and Airtel Zero, which purported to restrict the user's internet experience, cannot be implemented in India.

The Regulations, however, do make a provision for review after expiry of two years from the date of their enforcement. It remains to be seen whether a more comprehensive net neutrality regulation will replace the current Regulations at such a time.

Intent

The key contention behind introducing such a prohibition is that a discriminatory tariff framework would violate basic regulatory principles of non-discrimination, free and fair competition and transparency, and may lead to predatory pricing. This can also create entry barriers for startups and infringe on the freedom of speech and expression, including the right to information, of users by restricting their internet experience.[2]

Furthermore, TSPs could use this as a tool to manipulate the market in a manner that would benefit them most by providing free access to content for which they receive financial benefits. This may result in creating entry barriers to content providers and adversely affecting competition and innovation.

While analysing the Regulations, the TRAI remarked that any proposed change in business models and commercial practices must be seen in the context of the need to preserve the unique architecture of the internet as a global communications network. Given the fact that users are also content providers and that the global internet is an amalgamation of several interconnected networks, it could be said that allowing a particular TSP to charge differentially could potentially change the architecture of the internet.

Limitations

It is interesting to note that the Regulations do not prohibit other forms of online discrimination that are independent of content or price. For example, speed-based discrimination (where TSPs could decide which applications or websites load faster than others: fast lane, slow lane, etc)[3] has not been expressly prohibited under the Regulations, thereby leaving scope for TSPs to consider other alternatives for discriminatory net usage.

Net neutrality regime: the need of the hour

While the Regulations reflect a positive step towards net neutrality, it is nonetheless important that we recognise the need to move towards a more comprehensive net neutrality regime, which is not just confined to content-based differential pricing, but also addresses the numerous aspects of consumers' online behaviour and freedom of choice, while equally accounting for TSPs' business considerations.

TSPs claim that the current regime permitting over-the-top services, such as WhatsApp and Viber, to operate in India is causing unsustainable revenue losses to them. It is likely that the TSPs perceive such arrangements based on differential pricing or other discriminatory internet practices to help them recover this lost revenue. Given that the telecom sector is a major contributor towards revenue and growth, it may be time for the government to enter into a meaningful dialogue with TSPs and the TRAI, and if required, renegotiate the terms of TSP licenses to align it with the changing times.

As quoted by the TRAI on a different occasion, the two extremes – strict net neutrality and no regulation – are inherently flawed. Banning all discrimination is over-inclusive and restricts the evolution of the network, while allowing all discrimination can lead to exclusion, effectively making the rule against blocking meaningless. The intention should now be to find a middle path that protects the regulatory principles of non-discrimination, transparency and free and fair competition, and at the same time, addresses commercial factors around which TSPs operate.

Notes

1 The questions raised in the Consultation Paper were as follows:
- Question one: Should the TSPs be allowed to have differential pricing for data usage for accessing different websites, applications or platforms?
- Question two: If differential pricing for data usage is permitted, what measures should be adopted to ensure that the principles of non-discrimination, transparency, affordable internet access, competition and market entry and innovation are addressed?
- Question three: Are there alternative methods/technologies/business models, other than differentiated tariff plans, available to achieve the objective of providing free internet access to the consumers? If yes, please suggest/describe these methods/technologies/business models. Also, describe the potential benefits and disadvantages associated with such methods/technologies/business models?
- Question four: Is there any other issue that should be considered in the present consultation on differential pricing for data services?'

2 Tariff proposals are scrutinised by the TRAI in the background of regulatory principles including the following:
- non-discriminatory: Clause 2(k) of the Telecommunication Tariff Order, 1999 (the 'TTO') issued by the TRAI defines 'non-discrimination' to mean that the service provider shall not, in the manner of application of tariffs, discriminate between subscribers of the same class and such classification of subscriber shall not be arbitrary. Clause 10 of the TTO provides that no service provider shall, in any manner, discriminate between subscribers of the same class and such classification of subscribers shall not be arbitrary;
- transparency: the TRAI has issued several directions to the TSPs with a view to provide consumers with the opportunity to make a free and informed choice, and to protect them from subscribing to or being billed for any service due to lack of proper information or understanding;
- non anti-competitive;
- non-predatory;
- non-ambiguous; and
- non-misleading.

3 The EU has recently passed regulations in favour of internet fast lanes and slow lanes. See http://arstechnica.co.uk/tech-policy/2015/10/net-neutrality-eu-votes-in-favour-of-internet-fast-lanes-and-slow-lanes/. By contrast, the Federal Communications Commission of the government of US has proposed that net neutrality should be upheld and no internet fast lane or slow lane should be permitted. See www.washingtontimes.com/news/2015/feb/5/net-neutrality-new-fcc-rules-propose-no-fast-or-sl/?page=all.

Tim Cowen
Preiskel & Co, London
tcowen@preiskel.com

Ofcom strategic review of digital communications: from baby steps to giant leaps?

Ofcom's strategic review of digital communications

In March 2015, the Office of Communications (Ofcom) announced its Strategic Review of Digital Communications.[1] It was billed as being the first review in ten years. Careful short steps were announced toward a change of direction.

Casual observers might be forgiven for thinking that constant monitoring and reviewing market developments is, and assessing whether the strategy needs to be reviewed or changed is, or should be, the stuff of daily work for Ofcom. Nevertheless, the review was intended to be a new policy vision, and an indication of a new policy direction that Ofcom will be taking in the future. So, Ofcom has since then been provoking thought and managing expectations for some time. It first started getting the attention of all stakeholders with a discussion document published in July 2015. The conclusions were announced on 25 February 2016. For a swift-footed regulator already attuned to the fast moving technology industry, that may have been thought to be enough time to reach definitive conclusions. However, Ofcom is still not being definitive and the strategic review indicating only 'interim conclusions' and next steps.

In summary, the strategy focuses on five areas:

- the guarantee of universal broadband availability at a sufficient speed to meet modern consumer needs;
- support for investment and innovation in ultrafast broadband networks (such as fibre to homes or businesses) by giving BT's competitors improved access to its infrastructure;
- improvements in the quality of service delivered by the whole of the telecoms industry, including Openreach, BT's access network division;
- increased independence of Openreach from BT so that it is more responsive to all of its customers; and
- consumer empowerment so that people can understand the array of choices available to them and are able to switch to the best value deal easily.

This is close to saying that Ofcom needs to be very careful not to change existing regulation and undermine investment, indicating that Ofcom's proposals could well affect investment by BT and others. The problem here is that it's attractive to suggest that BT should supply everyone with high quality fibre at low prices, but there are different ways in which that can be done and different companies, whether using fibre or mobile technology, are already busy building alternative networks to BT's. So, forcing BT to provide more, particularly in those areas that are competitively supplied, could in fact reduce the amount of competitive supply and cause investors, and investing, to freeze up. However, as we shall see below in relation to its review of business connectivity markets, recognising this as important in a high level policy sense does not necessarily mean that Ofcom properly understands the issue when it comes to maintaining business confidence for investment.

The strategy document also claims to set out how Ofcom will step back from regulation where consumers and businesses no longer need it. Industry is understandably sceptical of regulators claiming they will regulate less.

One of the central issues that has come out of the strategic review has been whether to break up BT or not. One side of the argument was that break up was needed to secure better quality of service. Much discussion was created over BT's quality of service, particularly when supplying its competitors. Various industry players claimed that break up would improve things, while others pointed out that changing the structure of BT would not on its own be a cure for quality of service problems. Huge debate took place over 'BT Break Up'. Shortly before the announcement of the February conclusions on the strategic review, amid

press reports that BT would indeed be broken up, further press reports suggested that Gavin Patterson, BT's CEO, was offering to invest a further £1bn on Openreach if he was allowed to keep it, provoking questions about why the money had not been spent before.

Sharon White, who heads Ofcom, was clear that while 'BT Break Up' was, and remains on the regulatory agenda, it would not be required any time soon.

Industry response

BT's response was to focus on 'Investment Incentives' and argue that Pay TV customers should enjoy the same benefits as telecoms customers when it comes to non-discriminatory access, pointing out the lack of a level playing field for BT in access to content, with a clear dig at Sky. BT stated:

> 'We want the Ofcom regime extended to pay TV so that it covers Sky more fully and brings down prices in pay TV.
> We would like to see government help to ensure access to premium TV content on a regulated wholesale basis in the same way that other operators can access BT's network. BT has invested in sports rights with BT Sport. This has been funded entirely from the free cash-flow of the BT Consumer business.'

BT is also seeking to ensure that: 'People can switch services away from Sky and Virgin as easily as from BT and TalkTalk.'

BT's share price rose on the day, presumably showing an increase in confidence that the shadow has passed across the sun and the regulatory forecast is now all sunshine and clear skies.

In fact, there may be dark clouds ahead and, as ever with communications regulation, the way forward is far from clear. For example, the European Union is looking at its Digital Single Market proposals, which are likely to significantly alter the regulatory position.

Sky used the announcement to emphasise three main points:

- the increasing dominance of high speed broadband services by BT, which risks unwinding the benefits of years of strong competition in broadband services;
- the inadequate quality of service delivered by Openreach – and its significant impact, every day, on large numbers of UK consumers and businesses; and
- the level and type of investment in the United Kingdom's fixed line communications infrastructure. In particular, it is evident that, at a time when fibre-to-the-premise ('FTTP') networks are being rolled out around the world – in places like Sweden, Lithuania, New Zealand, Spain and Portugal – BT's focus is on incremental upgrades to the old copper network. There are real questions to be addressed about whether the UK risks being left behind in terms of 21st century connectivity compared to other countries around the world.

Ofcom proposals

Headline conclusions from the strategic review are:

- BT must open up its network, so competitors can connect fibre to homes and offices;
- reform of Openreach to better serve UK consumers and businesses; and
- better quality of service for all customers, including automatic compensation.

In more detail the initial proposals include the following.

A strategic shift to large-scale investment in more fibre

Ofcom will help create more choice for people and businesses, while reducing the country's reliance on Openreach. A major strategic shift will encourage the roll-out of new 'fibre to the premise' networks to homes and businesses, as an alternative to BT's planned innovation in copper-based technologies. As part of this, BT will be required to open up its network, allowing easier access for rivals to lay their own fibre cables along BT's telegraph poles and in its underground cable 'ducts'.

A step change in quality of service

Ofcom will publish service quality performance data on all operators, and look to introduce automatic compensation for consumers and small businesses when things go wrong. Ofcom intends later this year to introduce tougher minimum standards for Openreach with rigorous enforcement and fines for underperformance.

Reforming Openreach

Ofcom intends to reform Openreach's governance and strengthen its independence from BT. In future, Openreach should be governed at arm's length from BT Group, with greater independence in taking its

own decisions on budget, investment and strategy. Openreach management will be required to serve all wholesale customers equally, and consult them on its investment plans. Greater independence could be achieved by 'ring-fencing' Openreach (for example, Openreach becoming a wholly owned subsidiary with its own purpose and board members). Full 'structural' separation remains an option.

The right to broadband

Ofcom will work with the UK Government to make decent, affordable broadband a universal right for every home and small business in the UK. The universal right should start off at 10Mbit/s for everyone, and then rise in line with customer demand over time. Ofcom will work with the Government to deliver it. Ofcom will also look to improve mobile coverage by including new obligations on operators seeking new licences for spectrum (the radio airwaves which transmit mobile signals).

Empowering consumers to make informed choices

Ofcom will give consumers real power to exercise choice through much more accessible and engaging information on the services available to them. Ofcom will continue to make switching easier for more services so customers really can exercise choice.

Deregulate and simplify while protecting consumers

Ofcom will step back from regulation where people and businesses no longer need it, including when there is a real prospect of competition. The ultimate goal is to improve communications services for everyone, not to increase regulation.

Ofcom's new approach in practice: a cherry picker's charter?

Following the cautious steps announced in its strategic review, Ofcom recently, on 23 March 2016, published its review of business connectivity markets 2016 (BCMR 2016). In the Business Connectivity Market Review ('BCMR'), taking the strategic review on board, Ofcom has proposed the following changes:

- opening up access to BT's national dark fibre network;
- opening up access to BT's passive infrastructure (ducts and poles);
- changing the BT Charge control and cutting Ethernet prices (by about 12-13 per cent); and
- requiring BT to deliver and install circuits more quickly.

Ofcom's[2] BCMR review[3] indicates that the next steps are being taken with increasingly broader strides, if not leaps into the unknown. In particular, its proposals for passive infrastructure access provide alternative operators with options for using BT's dark fibre or using, where possible, BT's ducts and poles. This means BT would have to give competitors access to its fibre-optic cables, allowing competitors to control the service. This is often referred to as 'dark fibre', because BT is not offering a service over its fibre optic cables as such, and the cables are not 'lit' using BT's electronic equipment. Instead, they will be 'lit' by the competitor installing its own equipment at either end of the optical fibre.

BT is already required to offer wholesale leased line products, which bundle the optical fibre and BT's own network equipment, at regulated prices to competitors. BT would still be required to provide these services, but the new proposal would go further, allowing operators to use BT's fibre optic cables with their own equipment, rather than rely on BT's equipment.

This is, in the regulatory world, a major change and one which runs the risk of cutting across the policy position that recognises the role of alternative infrastructure operators. The policy, which is mandated at EU level, recognises that competition from alternative infrastructure players will stimulate and encourage BT to sharpen up its own service or risk losing customers. The position taken under telecoms regulation to date has thus encouraged alternative infrastructure operators to build their own networks and install their own optical fibre. Now, under the newly announced BCMR approach, if Ofcom's regulated access for passive access to dark fibre and ducts and poles is set at the wrong level by comparison with the level needed by alternative operators to generate a profit, it will undermine the economic opportunity and incentives for third parties to build their own networks.

In addition to passive remedies BT will be required to supply its leased lines more quickly. Ofcom's consultation states that BT has been 'taking too long to install leased

lines and is not providing adequate certainty that the services will be provided by the date first given to the customer.'

Jonathan Oxley, Competition Group Director at Ofcom, is reported to have said, in relation to the BCMR:

> 'All of us depend on high-speed, fibre optic lines. Businesses use them to communicate, and they also underpin the broadband and mobile services used by consumers at home and on the move.
>
> BT is relied on by many companies to install these lines, and its performance has not been acceptable. These new rules will mean companies across the UK benefit from faster installation times, greater certainty about installation dates, and fast repairs if things go wrong.'[4]

Ofcom has now also proposed that for 'Ethernet' services, installation times should be reduced (reaching 40 days after April 2017, instead of today's 48-day wait).

	Performance in 2011	Performance in 2015	Requirement from final statement to end March 2017	Requirement from April 2017	Requirement from April 2018
Time to install leased lines (mean average)	40 working days	48 working days	46 working days (maximum)	40 working days (maximum)	
Orders completed by initial contract date	n/a	71%	80% (minimum)	85% (minimum)	90% (minimum)
Faults fixed within five hours	93.1%	n/a	94% (minimum)		

A BT spokesperson is reported to have said, among other things:

> 'Dark fibre is a flawed piece of regulation that introduces an unnecessary layer of complexity and will deter others from building their own fibre networks. It is at odds with Ofcom's recent statements about increasing competition at the infrastructure level. It is a cherry pickers' charter benefiting those who don't invest in networks at the expense of those who do including BT, Virgin Media, Cityfibre and Zayo.'[5]

Ofcom's Strategic Review put pressure on BT to address the issues posed by quality of service failure. Following this through it might be thought that BT would be set strict timetables for delivery and installation and allowed to spend more and employ more people to make that happen. It is a challenge to understand how the imposition of increased charge controls, coupled with obligations to supply every component of its network on an unbundled basis will address this problem. Installation is something that naturally requires work to be done by BT in a given timeframe. BT could spend more, automate more or employ more people and increase the number of installations processed in a given timeframe. That now looks less likely if its returns are capped at a lower level. Indeed, threatening to force the divestiture of Openreach seems somewhat beside the point if the issue is quality of service and increased delivery and installation.

Ofcom is currently seeking a final resolution by the end of 2016. The proposed changes to charge controls will be implemented in May 2016 but dark fibre will take longer to implement. Oddly, this raises the risk that customers will take existing leased line products at lower prices, further reducing opportunities for alternative operators to use BT's dark fibre products. In the meantime, BT have been told to publish a draft dark fibre 'reference offer' *by* 1 September 2016. Much remains to be done and Ofcom should be encouraged to tread carefully and both solve the problems of delivery and installation while continuing to support alternative infrastructure and investment.

Notes
1 http://stakeholders.ofcom.org.uk/telecoms/policy/digital-comms-review/.
2 http://www.ofcom.org.uk/.
3 http://stakeholders.ofcom.org.uk/consultations/bcmr-2015/statement2016/.
4 http://media.ofcom.org.uk/news/2016/bcmr-2016/.
5 http://commsbusiness.co.uk/news/ofcom-demands-better-service-from-bt/.

Rob Bratby, Olswang, London
rob.bratby@olswang.com

A broadband universal service obligation for the UK

In common with many jurisdictions, the scope of the universal service obligation in the UK was last considered before the internet was a reality for consumers and the 'killer app' for telecoms was traditional fixed voice telephony. As a result, the scope of the current UK universal service obligation in respect of data is limited to providing dial-up internet access. While the government has progressed a number of initiatives, mostly notably by Broadband Delivery UK, to enhance the availability of broadband access across the UK, the universal service obligation had remained in the age of dial-up modems.

In November 2015, David Cameron, the UK Prime Minister, announced[1] the UK government›s intention to introduce a broadband universal service obligation to the UK. Subsequent announcements have clarified that his 'ambition' is that the minimum speed is set at 10 Mbps for consumers and small businesses.

On 23 March 2016, the UK's Department for Communications, Media and Sport (DCMS) issued a consultation on their proposed approach to implementation[2]. Their proposal (on which they invite comments) is to introduce enabling primary legislation, with details being set out in secondary legislation and Ofcom responsible for implementation. DCMS are also considering a power for the government to direct Ofcom to review the USO as required in the future. That consultation is still open and runs until 18 April.

In parallel, DCMS wrote to Ofcom on 22 March[3], commissioning Ofcom to undertake detailed analysis of the key factors that would help inform the design of the USO.

On 7 April Ofcom published a (for once short!) 'call for inputs'[4] to help inform their analysis. Interested parties have until 23 June 2016 to respond[5], with Ofcom aiming to deliver their report to DCMS by the end of the year. Ofcom are inviting comments from stakeholders on six topics:

- Specification and scope of the USO;
- Demand for the USO;
- Cost, proportionality and efficiency of the USO;
- The universal service provider or providers;
- Funding of the USO and potential market distortions; and
- Review of the USO.

Consideration of a broadband USO is also part of the European Digital Single Market review of the European telecoms rules[6] which, absent Brexit, will also have an impact on the UK's approach over the medium term.

As Ofcom has previously determined that the net cost of the current USO is zero, there are currently no mechanisms or frameworks in the UK used to fund the USO. If (as seems likely) the cost of a broadband USO is not zero, then the debate will rapidly shift from setting of the USO to its funding and impact that will have on market participants.

Notes
1 https://www.gov.uk/government/news/government-plans-to-make-sure-no-one-is-left-behind-on-broadband-access
2 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/510148/Broadband_Universal_Service_Obligation.pdf
3 http://stakeholders.ofcom.org.uk/binaries/consultations/broadband-USO-CFI/annexes/DCMS_Letter.pdf
4 http://stakeholders.ofcom.org.uk/binaries/consultations/broadband-USO-CFI/summary/broadband-uso.pdf
5 http://stakeholders.ofcom.org.uk/binaries/consultations/broadband-USO-CFI/summary/broadband-uso.pdf
6 https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-regulatory-framework-electronic

50 shades of network sharing/ cincuenta sombras de compartición de redes

Purvi Parekh, Olswang, London
purvi.parekh@olswang.com

Introduction

When Commissioner Ms Neelie Kroes was in charge of the digital agenda for Europe, she commented that the organisation of economy and of society would influence Europe's success in the digital age and that the key to such success was the underlying infrastructure network. While today's digital world continues to evolve and the pace at which we embrace the changes in how communication services are consumed remains rapid, the underlying fundamentals have not changed. The core asset is still the network; it is the competitive advantage. Infrastructure remains essential for delivery, and network differentiation can mean the difference between business success and failure.

Communication operators have explored ways to monetise infrastructure and assets for several decades, driven by the decline in legacy revenue streams. However it has only been in the last ten years that we have seen the emergence of deeper and more sophisticated service models, and a less protective and more open approach to the sharing of technologies. Indeed the importance of the capacity, coverage and functionality of the network has been reinforced with the arrival of 4G which has led to the growth in new data rich products and services. To support new digital services, mobile payments and internet of things, geographical expansion needs to happen quickly to meet consumer demand and secure first mover advantages. With 5G services on the horizon, network investment and innovation are at the heart of future communications strategy. An increasingly common approach to address these issues is sharing, whether this is the physical sharing of infrastructure, roaming agreements or the sharing of spectrum.

Whilst some shade of sharing exists in almost every country in the world, most regulators shy away from legally mandating it (there are exceptions, such as the UAE, Jordan, where sharing has been regulatory enforced). Instead most regulators actively promote it and rely that challenging economic climates will lead operators to independently conclude on the common sense of such an approach.

Advantages and challenges

The advantages of sharing arrangements are well understood – cost benefit, speed of deployment, coverage, and so on. However, interestingly, there remains a marked difference in sharing between operators in mature markets and those in emerging markets. Typically those in mature markets use sharing strategies to reduce operating costs and provide additional capacity in areas where there is limited space or where it is not cost efficient to build out two networks. Sometimes sharing can offer an additional source of revenue provided that core products and services continue to be differentiated. In newer markets – perhaps because voice revenue streams are still as important – the primary aim tends to be more about expanding coverage than reducing costs. Because coverage is often used as the service differentiator and as urban areas grow, these markets historically favour a more passive than active sharing approach.

Sharing has its challenges of course, as is the case with any arrangement between players operating in a regulated sector. Ultimately two or more competitors are becoming partners – in some cases the competitors have equal leverage, but more often than not there is a more dominant player and that dominant will want to retain as much control as possible. To succeed behavioural alignment is critical. The parties need to establish the limits of their roles and responsibilities with each other, as well as with those third party vendors, and service providers supporting and maintaining the infrastructure. To do this well, both sides need stakeholder buy-in; not just to the high

level concept but also to the operational nuances. Practical matters also need to be determined at the outset – site requirements, loading calculations, design capacity, antenna sizes, traffic use imbalances and late entrant access – all need advance consideration. The reality is that there are two separate businesses involved, each of which will be working to different priorities at any one time, be these achievement of coverage licence obligations, fulfilment of contractual commitments in customer deals or internal strategic drivers.

Types of sharing

Infrastructure sharing has many shades, ranging from reciprocal fibre lease capacity (as recently demonstrated in Bangladesh by Banglalink and Summit) and national roaming, to passive site and mast sharing. What started as a passive trend has evolved to sharing higher up the asset value chain and sharing of backhaul, RAN (radio access network), core network and spectrum are growing. The deeper the sharing, the more involved the regulators. While collaboration is smiled upon, collusion is not, and there is a fine balance to be struck in the sharing arrangements to ensure that the players involved stay on the right side of that line.

National roaming

Although national roaming does not technically involve investment sharing of physical infrastructure, operationally an operator's customer does 'share' and is routed through another operator's network. Increasingly, operators are including roaming arrangements as part of infrastructure sharing arrangements. Although not a new phenomenon in itself, as new technologies and new licence bands are opened up and as new entrants need to build out quickly to survive, national roaming collaborations are on the rise and can be strategically important for successful sharing.

MVNO access

The MVNO market and the mandating of more open capacity based MVNO access also has its role to play within infrastructure sharing and re-selling models. This is particularly the case where market consolidation – acquisition and sale – can take the number of mobile network operators down from four to three and there are perceived competition risks. This was demonstrated in Germany last year when Telefonica agreed to sell part of the combined network capacity to German MVNO Drillisch in order to get merger approval for its acquisition of KPN's German mobile network, E-Plus. However, combining mandated MVNO access models with named third party beneficiaries needs careful handling by regulators. There is a risk that such an approach inadvertently adds to the problem it is seeking to solve. New entrant access should be allowed to be innovative in their approach, and allowing remedies where MVNOs can become mobile network operators in their own right a more effective competitive approach.

Spectrum sharing

Spectrum sharing also has an increasingly important role to play, particularly because of the growth of data rich services. European operators have been slower to embrace the approach when compared to countries such as India where many of the big telcos, Reliance, Bharti, Aircel and Videocon have already embarked on spectrum sharing and trading deals.

European regulators are keen to improve the use of spectrum. At both a European Commission and domestic country level regulators are focused on implementing more effective spectrum management strategies. In the UK, Ofcom has already provided for the majority of spectrum licence classes are tradeable; however like most regulators they remain nervous about interference issues and as such restrict the ability for the sharing of spectrum without regulatory approval or wider consultation. From the other side mobile operators are happy to embrace spectrum sharing provided that they get to choose the terms on which that sharing happens and, crucially, at what price. For these players, sharing is acceptable only if it is within the boundaries of what they are capable of competing with. Mandating some level of spectrum sharing without imposing restrictions on use would enable the growth of a more competitive environment. However such obligation must come with guidance on the underpinning principles that will flow through into the commercial terms that exist between the sharing parties. Without such guidance there is a risk that a mobile operator's wider concern to protect its ground will unduly prejudice a process that is intended to create more competition.

With so many different shades of sharing and so many different countries and operators involved, a common comprehensive set of rules for sharing could not work. Sharing will continue to work because operators can choose how to invest, how to innovate, how to collaborate. Fifty shades of sharing (*cincuenta sombras de compartición de redes*), and more to come.

Purvi Parekh
(*Partner and Head of Olswang's International Telecom Practice; Co-author of the European Infrastructure Sharing Guide 2015*)

Reloading data protection: will the new EU Regulation really checkmate multinationals and revamp individuals' right to privacy once and for all?

Rocco Panetta, NCTM Studio Legale, Rome
r.panetta@nctm.it

Current EU data protection law, based on Directive 95/46/EC, has finally been sentenced to death: on 14 April, in fact, after four long years of negotiations at institutional level, the European Parliament adopted the data protection reform package, the so-called General Data Protection Regulation (GDPR), and marked a crucial milestone for the birth of a stronger European-wide right to privacy.

This fundamental step comes at a time where significant advances in information technology have been achieved and radical transformations to the ways in which individuals, organisations and public institutions communicate and share information between them.

Therefore, the divergent approaches in implementing EU data protection laws taken by Member States made the need to overcome widespread compliance difficulties more urgent than ever and pushed towards new and more effective ways to harmonise european privacy legislation.

Furthermore, European citizens' growing awareness on risks and dangers relevant to their personal data (ie also driven by recent global outrage for massive surveillance scandals and data breaches), fostered the approval of a common set of rules applicable within and outside EU borders.

Nonetheless, EU's legislators significant efforts to re-think the basis of european personal data privacy law, although appreciable since their start, had to shrunk from their original idealistic *ratio* of settling private and public stakeholders' interests after facing the hard truth: you cannot have the best of both worlds.

The final version of the package adopted on 14 April 2016 by the European Parliament – and then published on the EU Official Gazette on 4 May 2016 – is therefore the synthesis of the most suitable and viable compromise solution EU legislators could buy in bringing privacy law to a higher level of complexity, while setting aside controversial topics for future institutional talks, ie 'hot potatoes' including the e-Privacy Directive reform, employment issues and, last but not least, the new EU-US Privacy Shield.

In essence then, the reform package, as composed by a regulation (ie the General Data Protection Regulation or GDPR) and a directive (ie the Police and Criminal Justice Data Protection Directive), represents a fundamental keystone for the creation of the future european Digital Single Market and an important step towards greater legislative harmonisation on privacy and data protection issues across the continent.

The package will now enter a two years implementation period during which Member States will have to adapt domestic legislation to such changes and their relevant legal implications, by 25 May 2018.

In fact, over the course of this timeframe, organisations need to understand clearly what changes are most likely to affect their sector of activity and be prepared to assess their level of compliance with the reform's new requirements.

As for the definition of the traditional categories of players subject to accountability in EU privacy law's 'chain of responsibility' (ie, data controller and data processor), many of the core definitions from the previous Directive remain essentially unchanged.

At a national level, for instance, in Italy, the legislator and the Italian Data Protection Authority (ie the Garante), after having found themselves in front of the difficult task of balancing the reform package with the current domestic regulatory framework and adapting its lexicon to italian legal terminology, decided to maintain the current translation of 'data controller' (ie, *titolare del trattamento*) and 'data processor' (ie *responsabile del trattamento*) in order not to cause unnecessary interpretative burdens for public and private entities processing data.

Moreover, the entry into force of the GDPR will definitely cause major concerns to private and public institutions operating in several areas (for example, from banking to health care) because of stricter and more pervasive privacy obligations to comply with.

Where the Regulation will be deemed to be applicable to a business entity processing personal data, for example, that company will need to provide clear evidence of its full compliance with the new rules to either national Data Protection Authorities and the future European Data Protection Board, which will replace Article 29 Working Party's role and functions.

Same thing will apply to the public sector and, for the very first time, also to data controllers and processors based outside the EU but conducting businesses (ie, processing data) within EU borders.

Currently, if a data controller is established in any Member State, it is considered subject to the discipline enshrined by the Directive as implemented by national laws and regulations of that legal system, however under the GDPR this distinction will fall apart.

The Regulation, in fact, will only apply in case that legal entity, either public of private, offers goods or services to data subjects in the EU or monitors their behaviour within european borders.

For instance, a business established in the US that markets its products directly to the European single market but has no physical presence in the EU, will now be subject to the requirements of the GDPR as if it was established on European soil.

This important aspect, along with others (for example, the obligation to conduct regular privacy impact assessments, the new privacy by-design and by-default principles or the duty to appoint a data protection officer and a national Representative where prescribed), well express the strategy behind EU's legislators will to regulate and adequately circumscribe the power of telecom and digital multinationals processing personal data of european citizens through a borderline approach to privacy compliance.

In fact, the entry into force of the GDPR will indeed force big companies that have previously regarded non-compliance with EU data protection law as a 'calculated risk' to re-evaluate their position especially in light of the substantial new fines (ie, up to €20m or four per cent of the annual worldwide turnover) and increased enforcement powers given to national Data Protection Authorities (for example, total ban on processing and in depth investigative capacity above all).

On the other hand, the same companies processing personal data, either from within the EU or outside, will benefit from a significant degree of autonomy in dealing with Member States' data protection authorities through the new one-stop-shop mechanism, which will connect controller and processor with a single 'lead authority' on the basis on the location of its 'main establishment', that is, the place where the main processing activities take place.

It is now clear how difficult has it been for EU legislators to combine civil society's push for a stronger protection of individuals' right to privacy with companies' legitimate interests to collect and process personal data, nonetheless an important compromise solution has been successfully achieved.

With a greater simplification and a substantial de-bureaucratisation of some privacy obligations (ie, same rules apply in all EU Member States with no need to contact 28 national DPAs), comes the revamped focus on data protection in all corporate policies and regulations as a guarantee of stronger and deeper protection to individuals' rights.

As for Italy, the Garante's serious approach to the new rules will surely show a reasonable and sound approach in choosing how to better integrate the letter of the GDPR with the Italian Data Protection Code (ie, Legislative Decree no 196 of 30 June 2003).

In conclusion, only time will tell us whether more stringent and incisive privacy rules have been enough to raise and consolidate european and global data protection standards and made IT compliance and cyber security a number one priority for all companies and public institutions.

There is still a long way to go for the full implementation of the GDPR and legislative misalignments can always occur, however the recognition of privacy compliance as a real strategic asset for the private and the public sector alike has finally found a starting point and the birth of a corporate culture of data protection social responsibility might be closer than it seems.

The FCC dives in to the deep end on data privacy

Nancy C Libin
Jenner & Block, Washington, DC, United States
nlibin@jenner.com

Leah J Tulin
Jenner & Block, Washington, DC, United States
ltulin@jenner.com

In the United States, the Federal Trade Commission ('FTC') is the principal regulator of commercial privacy at the federal level. The agency uses its enforcement authority under section 5 of the Federal Trade Commission Act (the 'FTCA') to police companies' data privacy and security practices, holding companies accountable when they engage in 'unfair or deceptive acts or practices'[1] – that is, when they do not abide by their privacy policies or when they fail to adopt and implement reasonable data security safeguards.

Recently, however, another federal agency has got in to the act. Specifically, last year, the Federal Communications Commission (the 'FCC'), which is responsible for regulating interstate and international communications by radio, television, wire, satellite, and cable, adopted an order (the 'Open Internet Order') establishing new open internet rules.[2] In so doing, the FCC also reclassified broadband internet access services as a 'telecommunications service' - and, by extension, internet service providers ('ISPs') as 'common carriers' - under Title II of the Communications Act of 1934, as amended (the 'Act').[3] Because the FTCA explicitly prohibits the FTC from regulating the practices of 'common carriers',[4] the Open Internet Order arguably had the effect of precluding the FTC from regulating the privacy practices of ISPs.

The FCC is seeking to fill that gap. In the Open Internet Order, the FCC took its first step toward broadband privacy regulation by announcing that it would scrutinise the conduct of ISPs under section 222 of the Act, a statutory provision that was enacted for and previously applied only to voice telephony services. On 31 March 2016, the FCC went a step further by proposing a comprehensive set of new rules that would expand both the scope of information covered and the types of practices currently regulated under section 222. If adopted, these rules would impose more restrictive requirements on the data privacy and security practices of ISPs than the FTC currently applies to other entities in the internet ecosystem.

This article provides background information about section 222, explains the FCC's proposed data privacy rules, and analyses the implications and problems associated with applying these types of rules to ISPs.

Background of section 222

Unlike other privacy laws, which typically govern 'personal information' or 'personally identifiable information', until recently section 222 had been interpreted to limit the use and disclosure of a particular kind of customer information that telephone voice services carriers collect - namely, customer proprietary network information ('CPNI').[5] CPNI is a limited category of data that includes only the following: 'information that relates to the quantity, technical

configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship' as well as 'information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.'[6] Importantly, information that typically would be considered personally identifiable information under other privacy laws - including a customer's name, address, and phone number - is not considered to be CPNI under section 222. Likewise, carriers' obligations under section 222 are triggered when they use or disclose 'individually identifiable' CPNI.[7]

When the US Congress passed section 222 as part of the Telecommunications Act of 1996, its goal was twofold: (1) to foster competition among telephone voice service providers in the wake of the breakup of AT&T, which for decades had enjoyed a monopoly over such services;[8] and (2) to protect the confidentiality of a certain category of information to which carriers had access solely by virtue of providing telephone services to their customers. Specifically, the statute was intended to prohibit incumbent carriers that were formed after the breakup of AT&T from using CPNI obtained through their provision of services to gain competitive advantage in the nascent market for voice services. It also was meant to protect legitimate customer expectations of confidentiality regarding certain individually identifiable information – CPNI - to which carriers had access by virtue of providing telephone services.

The FCC's proposed rules

The FCC's proposed rules depart dramatically from the language of section 222 and would significantly expand the category of customer information subject to regulation. Unlike section 222, which focuses - with respect to customer information - only on CPNI, and unlike the current CPNI rules for telephone voice service providers, which do the same, the FCC's proposed rules would cover CPNI *and* a new category of information that neither appears nor is defined in the statute: 'customer proprietary information'. The FCC has proposed to define customer proprietary information as the combined categories of CPNI *and* 'personally identifiable information', which it in turn defines broadly. Specifically, 'personally identifiable information' would include 'any information that is linked or linkable to an individual', and would include information that can be used 'on its own, in context, or in combination to identify an individual or to logically associate with other information about a specific individual.'[9]

The proposed rules seek to apply three privacy principles to this new category of customer proprietary information: transparency, choice, and security.

Transparency

The FCC's proposed rules would require providers to disclose the following in their privacy policies: (1) what information the provider collects and for what purposes; (2) what customer information is shared and with what types of entities; and (3) how customers can opt in or out. The FCC also requests comment regarding whether the final rules should require a standardised notice or uniform template, or instead should require providers to create a consumer-facing privacy dashboard.

Choice

The FCC's proposed rules would create a tiered approach to choice:

- Inherent approval: ISPs would be permitted to infer customer consent to use and share customer data in order to provide the broadband service (eg, to ensure that a communication destined for a particular person reaches that person).
- Opt-out approval: The FCC proposes that ISPs (directly or through affiliates that provide communications-related services) be permitted to use customer proprietary information to market other communications-related services subject to opt-out approval. The opt-out mechanism must be clearly disclosed, easily used, and continuously available. 'Communications-related services' would not include edge services offered by the ISP. The FCC seeks comment regarding the scope of 'communications-related services', and the scope of the definition it ultimately adopts will have a significant impact on ISPs' first-party marketing activities.
- Opt-in approval: The FCC proposes to require opt-in approval before sharing customer proprietary information with

non-communications-related affiliates or third parties, or before using customer information directly for any other purpose.

Data Security and Breach

The FCC's proposed rules would require ISPs to adopt and implement certain baseline data security safeguards, such as a process to conduct regular risk assessments, implement adequate authentication mechanisms, and designate an employee responsible for data security. In addition, the proposed rules would require providers to notify customers within ten days of the discovery of a data breach.

Implications of the FCC's proposed rules

There are several problems with the FCC's proposed rules. At bottom, the statute that the FCC is seeking to apply to broadband through these new rules is inapplicable in the internet environment. As noted above, section 222 was drafted to promote competition and to protect the confidentiality of a certain, relatively narrow type of customer information – CPNI – in the telephone voice services market. The US Congress was concerned that incumbent carriers that had been part of AT&T and that already were in possession of CPNI would be able to leverage their control over this information in one market to perpetuate their dominance as they entered into other service markets. However, the online environment, in which the FCC seeks to apply these new rules to ISPs, is a very different marketplace. Unlike the closed market for telephone services, the internet ecosystem is open, dynamic, and depends on the free flow of digital information to create and sustain economic growth and foster innovation of new products and services.

Furthermore, ISPs do not have comprehensive or unique access to consumers' online information. In fact, their visibility into consumers' activity online is increasingly limited.[10] Unlike a decade ago, when users tended to access the internet from desktop computers, today, consumers use many different devices and internet connections, not just a single ISP.[11] Moreover, the rapid growth and adoption of encryption and use of virtual private networks further decreases ISPs' visibility, leaving edge providers, such as operating systems, web browsers, search engines, and apps, with more detailed and comprehensive data about users than ISPs have.[12] Indeed, edge providers are the market leaders in cross-context and cross-device tracking and in monetising user data, with just ten online companies accounting for 70% of online advertising revenues.[13] For all of these reasons, the public policy goals that drove the US Congress to enact section 222 in 1996 for the telephone voice services market would not be served through its application to broadband in the 21st century digital economy.

In addition, the FCC's proposed rule is out of step with other privacy laws and regulations – both in the US and around the world – that regulate the use and disclosure of data based on the sensitivity of the data. Consumer expectations, and privacy laws, typically are based on the sensitivity of the data collected, not on the identity of the service provider collecting the data or the particular products and services that a service provider wants to market using that data.

It would be far preferable for the FCC to take an approach to privacy consistent with the FTC's well-established privacy regime. Broadband privacy did not begin with the Open Internet Order. Before reclassification under Title II, ISPs operated under the FTC's flexible privacy regime, which governs all other online entities and balances strong consumer protection with giving industry the flexibility to innovate. By applying a prescriptive set of rules to one set of actors in the internet ecosystem (ie, ISPs), the FCC's proposed rules would create an asymmetrical regulatory framework for internet privacy and could limit consumer choice, reduce competition, and stifle innovation by precluding ISPs from effectively competing with edge providers to market new products and services. Asymmetrical privacy rules would also make it harder for ISPs to simplify their privacy policies and to provide consistent privacy controls. And they would confuse consumers, who could believe that by setting their privacy preferences with their ISPs, they have set their preferences with respect to all of the entities that they may encounter online, whether knowingly or unknowingly.

Notes

1 15 U.S.C. s 45(a)(1).
2 See generally: *Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 (2015).
3 *Ibid.*
4 15 U.S.C. s 45(a)(2).
5 30 FCC Rcd at 5822, 466.
6 47 U.S.C. s 222(h)(1), (3).
7 Although section 222(h) does not expressly define name or

phone number as CPNI, because section 222(c) applies only to 'individually identifiable' CPNI, the current CPNI rules will not apply unless the customer's name, phone number or other identifying information is included with the CPNI.

8 AT&T was the only telephone service provider for most of the US until 1982.

9 *In re Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, FCC 16-39 (released 1 April 2016).

10 See generally: Peter Swire, Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others, Institute for Information Security & Privacy, Georgia Institute of Technology (2016), http://peterswire.net/wp-content/uploads/Online-Privacy-and-ISPs.pdf.

11 *Ibid.*

12 *Ibid.*

13 *Ibid.*

Ning Liu, JungHe, Shanghai, China
liun@junhe.com

Yibo Wu, JungHe, Shanghai, China
wuyb@junhe.com

A Brief Analysis on the New Classified Catalogue of Telecommunications Services

In China, the Ministry of Industry and Information Technology ('MIIT') is responsible for overseeing the industry of electronic communications. This authority is granted by the Telecommunications Regulations of the People's Republic of China (the 'Telecom Regulations') effective as of 25 September 2000 and amended on 6 February 2016.

According to the Telecom Regulations, telecom refers to the activities of delivery, transmission, or reception of voice, text, data, image, and other forms of information via wire or wireless electromagnetic system or photoelectric system. Based on the Telecom Regulations, the MIIT further promulgated the *Classified Catalogue of Telecommunications Services* on 11 June 2001 which was amended on 1 April 2003 (collectively referred as the 'Old Catalogue'). The Old Catalogue classified and explained various types of telecom businesses, and has been treated as the basis of formulating lower-level regulations and issuing relevant telecom business licences.

Due to the rapid development of telecom technology, the Old Catalogue was insufficient to cover the scope of newly-emerging technologies and businesses. Therefore, the MIIT updated the Old Catalogue on 28 December 2015 and the updated version came into effect on 1 March 2016 (the 'New Catalogue').

Both the Old Catalogue and New Catalogue categorise the telecom business into two types: basic telecommunication services and value-added telecommunication services. The former refers to the business of providing public network infrastructure, public data transmission and basic voice communications services, and the latter refers to the telecommunications and information services provided through the public network infrastructure. Major revisions and amendments in the New Catalogue are summarised as follows.

The resale of cellular mobile communication services

Currently, only China Mobile, China Unicom and China Telecom are allowed to operate as cellular mobile communication service providers. To encourage the mobile communications resale business, the MIIT has promulgated the *Pilot Programme for Mobile Communications Resale Business* on 17 May 2013 and approved the first 11 pilot companies to operate as mobile communications resale businesses providers on 26 December 2013, including Beijing Jingdong 360 Degree E-Commerce Co, Ltd. ('JD.com'). As a pilot company, JD.com firstly purchases the mobile communication services from China Mobile, China Unicom or China Telecom, and then sells 'JD mobile' SIM cards in its own name on its own website. Customers can enjoy some preferential treatments when using such SIM cards, for example, visiting JD.com website free of charge. This is a typical business model for mobile communication resale businesses

and these enterprises are often called mobile virtual network operators ('MVNOs'). In the past two years, the mobile communication resale business has achieved an extensive presence in the market, but the Old Catalogue has no provisions for regulation of this business. To improve the regulation of this business model, the New Catalogue asserts that cellular mobile communication resale business will be treated as value-added telecommunication business. Enterprises engaging in this type of business will be required to obtain the telecom value-added business licence.

The reclassification of information services

The basis of classifying information services in the Old Catalogue is the type of telecom line to transmit information (fixed network, mobile network or the internet) and the relevant licences were issued accordingly as fixed-network licences, service provider ('SP') licences and internet content provider ('ICP') licences. With the development of telecom technology, the mixed use of telecom lines has become very common during the provision of information services. For example, when using our cellphones, we often switch the network mode from mobile network to the internet (Wi-Fi). To provide better regulation of information services, on the basis of the business nature of each service rather than the type of telecom line, the New Catalogue divides information services into five sub-categories, namely, service platforms for information publishing and delivery (such as ganji.com), services for information search (such as baidu.com), information community platforms (such as Weibo), instant message exchange services (such as WeChat), information protection and processing services (such as Qihoo360 mobile security). In our opinion, it is likely that the MIIT will issue value-added telecom business licences to information services uniformly. However, since the Administrative Measures for Internet Information Services (as amended on 8 January 2011) is still effective, an ICP licence shall still be required to provide internet information services in the future.

Strengthening regulation of mobile apps

In previous practice, regulation focused primarily on websites due to the lack of a solid legal basis to extend such regulation to mobile apps. Mobile apps may involve various kinds of services, including cultural services, cloud storage services, multi-party communication services, information services, etc. In the practice of some local governments, enterprises operating mobile apps were not required to obtain relevant licences. However, in the New Catalogue, as mentioned above, information services will be overseen according to the nature of the business. Considering these trends in regulatory practice, it is likely that the authority will adopt similar practices in overseeing websites by requiring all enterprises operating mobile apps to obtain relevant telecom business licences.

Extending regulations to cloud computing

The Old Catalogue did not provide a legal definition of cloud computing business, a business that has recently developed very rapidly. In practice, more and more internet data centre ('IDC') service providers under the Old Catalogue transformed their business model to cloud computing services. To cope with such business transformations, these kinds of businesses are described as collaborative internet resource services and are classified into the first category of value-added telecommunications services in the New Catalogue. However, it is worth noting that 'cloud computing' is not a legal term. The business model of cloud computing in practice is far more complicated, and collaborative internet resource services are only one type of cloud computing services. For example, the SaaS business, one type of cloud computing service, could be seen as information service, domestic multi-party telecommunication service, storage and forwarding service, or non-telecom service, depending on detailed analysis of the business model.

Content distribution network services

To improve the interface experience of internet users, especially the services of video websites with large volumes of data processed, many content distribution network ('CDN') service operators would provide accelerated access services. Under the Old Catalogue, there is no specific licence for CDN services, but in practice, some of these CDN service operators hold internet service provider ('ISP') licences, ICP licences or IDC licences. In overseeing these services most local MIIT authorities treat CDN services as

IDC businesses and there were no regulations or rules on CDN services specifically. In addition, due to the lack of unified regulation, some illegal websites or offshore websites indirectly engage in internet business domestically through CDN services operators. Considering that there are huge amount of data copies widely distributing in CDN services, more comprehensive oversight and higher standards of information security are required than those of IDC business. Thus, to promote the sound development of CDN business, the New Catalogue incorporates the definition of CDN business. On 5 April 2016, the MIIT promulgated the Technology Requirements for Information Security Management System of CDN Services. Based on our understanding, it is foreseeable that the MIIT will issue CDN licences uniformly to oversee the CDN business according to the aforesaid technology requirements.

The validity of issued licences after the enactment of the new catalogue

According to the interpretation of the MIIT on the New Catalogue, previously issued telecom business licences will still be effective within their original scope and term, and during the original term, enterprises may apply to re-issue a new telecom business licence when necessary. The MIIT can re-issue a new telecom business licence upon the application of the enterprise.

Michael Bergmann
Noerr, Berlin, Germany
michael.bergmann@noerr.com

Pascal Schumacher
Noerr, Berlin, Germany
pascal.schumacher@noerr.com

German and EU telecom regulation set sight on 'over-the-top' communication services

Over-the-top ('OTT') services such as email services or instant messaging or Voice over Internet Protocol ('VoIP') services have dramatically proliferated in the recent past, and are increasingly drawing voice and SMS traffic away from traditional telecom operators. Given the growing implications of OTT services for customer protection, privacy issues, carrier revenues, and for the long-term sustainability of network operators' business models, policy-makers, stakeholders and regulators struggle with the scope of regulation and its influence on competition.

The debate centres around whether and to what extent OTT services are currently, or should in future, be subject to the regulatory obligations set out in the European Union telecom framework and the German Telecom Act (Telekommunikationsgesetz, 'TKG').

Judgment of the Administrative Court of Cologne

In a judgment of 11 November 2015, the Administrative Court of Cologne has given a first answer to that so far unanswered and highly controversial question. The Court decided that, as provider of the email service Gmail, Google Inc. is a telecommunication service provider offering a telecommunication service within the meaning of section 3 no. 24 TKG. The Court ruled that Google is therefore subject to the notification duty set forth in section 6 (1) TKG.

The German Federal Network Agency (Bundesnetzagentur, 'FNA') had formally requested Google meet its notification duty under the TKG in 2012. Google however argued that Gmail was not a telecommunication service since the service provided by Google did not primarily consist in signal transmission as required by the TKG. Google explained that the use of the open internet as transmission route was characteristic for a service such as Gmail and that Google obviously had no control over the paths taken by the transmitted data packages via IP protocols before reaching their recipient. The FNA disregarded Google's opposing argument and held that

– even technically speaking (according to the Open Systems Interconnection layers' model) – the Google servers were providing transmission services and Google therefore had its own transmission technology and at least partial control over signal transmission.

Google filed an action in early 2015 which has since been dismissed. The Court followed the view of the FNA. However, the Court stated that the purely technical view was not decisive. The term telecommunication service in the TKG was rather open to a view based on a functional assessment. The Court however allowed a so-called 'leapfrog' appeal to the German Federal Administrative Court. Thus it remains to be seen if the higher instance courts will uphold the legal opinion of the Administrative Court of Cologne. If they do so, there will be far-reaching consequences for all OTT service providers and for the regulatory practice in Germany since OTT service providers would have to comply with the duties under the TKG then, with their compliance being subject to the supervision of the FNA. Such duties include, inter alia, specific data protection and customer protection rules, lawful interception and emergency call functionality.

Review of the EU telecom regulatory framework: EU digital single market

The timing of the judgment is critical since the question of how to classify or regulate OTT services also plays an important role in the European Commission`s current review of the legal framework for telecommunication services. The European Commission has recently completed a public consultation which raised a number of questions around the regulatory treatment of OTT services. In parallel, the Body of European Regulators of Electronic Communications (BEREC) has published a Report on OTT services (BoR (15) 142), in which it underlines the need to clarify the definition and scope of 'electronic communications services' under the EU framework directive. It is expected that the European Commission will publish a first proposal for a new telecom regulatory framework to which OTT communications service providers are held in the summer of 2016.

The 2016 IMT spectrum allocation exercise: paving the way for a fourth telco in Singapore

Lam Chung Nian
WongPartnership, Singapore
chungnian.lam@wongpartnership.com

Gareth Liu
WongPartnership, Singapore
gareth.liu@wongpartnership.com

The number of telecommunications companies in Singapore has steadily grown over the years as a result of the government's efforts in liberalising the telecommunications market. Singapore currently has three main telecommunication companies (telcos) – Singtel, StarHub, and M1.

With the rise in demand for mobile data services in Singapore, the telecommunications regulator (the Infocomm Development Authority of Singapore ('IDA') is focusing its efforts on facilitating a fourth telco to join the scene so as to introduce greater market competition.

The 2016 spectrum auction

On 18 February 2016, IDA issued its 'Decision on the Framework for the Allocation of Spectrum for International Mobile Telecommunications ('IMT') And IMT-Advanced Services and for the Enhancement of Competition in the Mobile Market'. The decision outlined the upcoming spectrum allocation exercise in which a total of 235 MHz of spectrum from the 700 MHz, 900 MHz and the TDD bands for 4G and/or IMT-Advanced systems and services would be made available for mobile services.

This spectrum auction (estimated to occur in the third quarter of 2016) is meant to facilitate the entry of a fourth telco, and will be split into two phases, a New Entrant Spectrum Auction ('NESA') for new entrants, and a General Spectrum Auction ('GSA') for incumbent mobile network operators ('MNOs') and the new MNO.

There will be a spectrum set-aside package offered at a discount which comprises 2 x 10 MHz of 900 MHz band and 40 MHz of 2.3 GHz TDD band (totalling 60 MHz of spectrum) for one new MNO in the NESA. Prior to the decision, IDA had conducted a public consultation outlining its plans for the auction and invited industry players to comment.

Responses from Incumbents

Singtel was generally critical of IDA's proposal to facilitate the entry of a fourth telco – it regarded Singapore's mobile market as being mature and competitive. Relying on an expert opinion commissioned from economists Professor Janusz A Ordover and Dr Allan L Shampine, it provided various reasons in its response to IDA's consultation paper to urge IDA to reconsider its stance:

Substantial costs in subsidising and facilitating entry of a fourth telco

Singtel was of the opinion that a fourth telco may potentially harm the existing state of competition in Singapore and the incentives for investment by the existing telcos.

It forecasted direct and indirect costs in subsidising the fourth telco (direct costs in revenue foregone from the spectrum auction, and indirect costs in the form of reduced investments by existing players because of a reduced revenue outlook - the new entrant would likely compete based on lower prices). Further indirect costs to the market cited were where the fourth telco exits the market because of the inability of the market to sustain a new player.

State of the market does not support a fourth telco

Singtel noted that IDA had already publicly stated that the state of competition in the market was satisfactory. It quoted IDA's statistics indicating there was 148% mobile penetration in 2014, showing the advanced development of the mobile market.

It was also of the opinion that there was no factual evidence that four telcos in a market would make the market more competitive – in that regard it cited the European Commission as stating that there is no 'magic number' of mobile network operators. In the absence of a clear market failure, it was of the opinion that IDA should not intervene in market forces, per IDA's regulatory principle in the Telecom Competition Code 2012 that 'to the extent that markets or market segments are competitive, IDA [would] place primary reliance on private negotiation and industry self-regulation, subject to minimum requirements designed to protect consumers and prevent anti-competitive conduct'.[1]

That the market could not support a fourth telco was reflected by the fact that no bidders came forward in the 2013 auction, where IDA had also reserved spectrum for the new bidder. According to Singtel, no bidders came forward because their expectations were that they would not be able to earn a normal return on investments at prices after entering the market.

Allocating scarce spectrum resources to a fourth telco may deprive existing telcos of valuable spectrum

Singtel was of the opinion that the spectrum set aside for the new player was too large in quantity, and there would be a risk of the fourth telco not using the spectrum efficiently. The spectrum set-aside package could risk 'tying scarce resources to inefficient usage for a prolonged period to public detriment'[2] and effectively create an 'artificial spectrum shortage for existing operators'.[3] This may lead to reduced innovation, economies of scale and investment by the existing three MNOs.

Singtel also cautioned that there was no evidence how the fourth telco would provide service offerings which were different from those currently provided.

StarHub took a similar position as Singtel and was doubtful that a fourth telco in Singapore would generate significant benefits for Singapore customers.

IDA's responses to the incumbents' concerns

IDA was generally positive about the introduction of a fourth telco, and considered that the new MNO would bring about further investment, innovation and competition in the market.

It noted that consumers were relying more on mobile broadband services, and technology trends such as the 'Internet of Things' and machine-to-machine communications could potentially offer the new MNO viable business opportunities and a share of the market. It was also of the view that the new MNO would incentivise the incumbents to engage in mobile network investment so as to maintain their competitive advantage.

Certain respondents cited the growing trend of consolidations in the European Union moving away from a four-MNO market. IDA expressed their view that while mergers are happening in the European market, the European Commission had actually implemented conditions which would still encourage a four-MNO market structure, such as for the merged entity to divest or make available spectrum to a new MNO, and/or strengthening regulations to facilitate the entry of Mobile Virtual Network Operators ('MVNOs').

Addressing comments that the spectrum set aside for the new MNO was excessive, and that the prices were too deeply discounted, IDA was of the opinion that it would not be appropriate to directly compare IDA's facilitation framework for a new MNO with other countries as the conditions and circumstances for the spectrum set-asides were different. Indeed, IDA also decided to lower the reserve price further from S$40m to S$35m, on the basis that the package was meant to lower the barriers of entry for the new MNO.

There were various other regulatory measures the IDA stated it would impose on the new MNO so as to address the respondents' concerns. These include:

- spectrum caps to allow efficient use of spectrum resources and prevent monopolisation of the same - so that the MNOs may reasonably obtain sufficient spectrum to deliver viable mobile services;
- relevant regulatory requirements to be imposed on the new MNO in phases - the new MNO will be required to roll out nationwide outdoor service coverage and after a specified period, roll out coverage to other areas, for example, underground MRT stations or lines;
- no spectrum trading unless IDA's prior written approval is obtained – the objective is for bidders to use the spectrum bands to deploy their networks in accordance with the deployment requirements. The new MNO will also be prohibited from providing wholesale services to any of the incumbent MNOs unless it has obtained prior written approval from IDA. And,
- maintaining its two-pronged approach of requiring spectrum right holders to negotiate in good faith with MVNOs and publishing negotiation principles to facilitate the entry of MVNOs - such negotiation principles include the principle that wholesale prices should be no higher than the host MNO's retail prices (including any promotional rates).

Competition regulation trends in the EU

IDA and the respondents made frequent reference to competition trends in the EU. The regulator's priority appears to be increasing competition in the telecommunication sector.

In her speech of 2 October 2015 at the 42nd Annual Conference on International Antitrust Law and Policy, Margrethe Vestager, the European Commissioner for Competition, commented on the proposed joint venture between the Danish operations of two Scandinavian telecom operators, the Swedish-Finnish TeliaSonera and the Norwegian Telenor.

While the deal eventually fell through in the end, the Commission was of the opinion that even if the transaction went through, the Commission would move to prohibit the merger. The Commission's fear was that the merger would create the largest mobile network operator in Denmark and result in a highly concentrated market structure. The Commission had conducted a balancing exercise and found that the benefits for consumers may not outweigh the expected price increases induced by the loss of competition, even if the promised investments by the merger parties materialised.

The Commission would have accepted a remedy which would lead to the entry of 'a strong and independent fourth mobile provider in Denmark that could address serious competition concerns'.[4]

The Commission stressed the importance of a competitive market, where companies have 'strong incentives to invest and innovate to offer superior products and win business from their competitors'. According to research, while a 'four-to-three' reduction in telcos in the EU could lead to higher prices for consumers, the research did not suggest that a merger would lead to more investment per subscriber. In any event, the investment

spoken of by the telcos may not be the type of investment which benefits the consumer (the Commissioner was of the view that investments affecting quality and price would be the type leading to consumer benefit).

Others have argued against the Commissioner's views. At least one writer has commented that the Commissioner's approach 'fails to acknowledge that consolidation could lead to more convergence, which is beneficial to both the consumer and innovation'.[5] In the context of the European Union, more consolidation may 'foster the integration of national markets and the emergence of big players across the whole of the EU'.[6]

The same may not be said of Singapore, where integration of national markets is not at issue. Nevertheless, convergence does have its benefits and can be seen in the incumbents' offerings – for example, StarHub's 'StarHub Go' service offering, which allows a customer to watch cable television programmes on his mobile device without data streaming charges.

A fourth telco in Singapore?

This year, there are two potential new candidates for the spot of fourth telco – MyRepublic Limited ('MyRepublic') and OMGTel Pte Ltd (an entity owned by wireless network solutions provider Consistel) ('OMGTel').

MyRepublic has announced its proposed mobile plans to the public on a website especially created for its bid to be a fourth telco. These include a budget mobile data plan and an unlimited data offering.

Consistel has indicated that its focus will be on technology, innovative network design for improved coverage with higher speeds and consumer-oriented solutions to differentiate itself in the market.

It is clear that in spite of incumbents' responses to IDA's public consultation, IDA is intent on facilitating greater competition in the Singapore market, and likely takes the view that competition is the best way to benefit consumers. It remains to be seen whether either of the above entities, when assuming the mantle of the fourth telco, will bring new market dynamics to the Singapore telco market.

Notes

1 Telecom Competition Code 2012 at Section 1.5.1.

2 SingTel Mobile Singapore Pte Ltd, *Response to IDA Consultation Paper: Second Consultation on Proposed Framework for the Reallocation of Spectrum for Fourth Generation (4g) Telecommunication Systems and Services*, available at https://www.ida.gov.sg/~/media/Files/PCDG/Consultations/20150707_SecondPublicConsultation/Singtel%20Mobile%20Singapore%20Pte%20Ltd.pdf, para 4.24.

3 *Ibid* at para 5.35.

4 Margrethe Vestager, *Speech on 2 October 2015: Competition in telecom markets*, available at: https://ec.europa.eu/commission/2014-2019/vestager/announcements/competition-telecom-markets_en.

5 Laure Roux and Alberta Laschena, *The EU's dilemma on telecom consolidation*, Europe's World, available at: http://europesworld.org/2016/02/19/eus-dilemma-telecom-consolidation/#.VwILFtLUjX4

6 *Ibid.*

Indonesia: a new transport apps regime

Retno Muljosantoso
Soemadipradja & Taher, Jakarta
r_muljosantoso@soemath.com

Robert Reid
Soemadipradja & Taher, Jakarta
robert_reid@soemath.com

Transport apps continue to impact an ever-increasing number of consumers. By providing a direct link between consumers and service-providers, these and other apps have fundamentally changed the shopping, travel and accommodation markets.

The rapidly increasing number of smart phone users, the overwhelming public demand for easy access to transport (particularly during peak periods) and the ever-increasing population of the greater Jakarta conurbation of Jabodetabek (over 28 million people), have together driven an enormous and quick increase in the demand for transport apps.

The first Indonesian-owned centralised motorbike transport services company, from which drivers were hired over the phone (but not through an app), was established in 2011.

Due to increased demand, the company released an Android app in 2015, which benefited both consumers and drivers. The company's services continued to expand, so that consumers can now purchase items ranging from groceries to cinema tickets, and order from other service providers, including cleaners, beauticians and masseuses.

Inevitably, foreign investors soon became interested. Several big international players have indeed already entered the market. Their apps connect users and drivers (who are considered partners, of sorts, in the business).

The success of transport app-providers (domestic and foreign) has prompted conventional taxi and other public transport operators and providers to engage in large public demonstrations (particularly in March 2016).

The protesters considered that the app-providers were unfairly advantaged for a number of reasons, including that they have not had to obtain proper licences to provide transport services, and were using unqualified drivers and unlicensed cars.

In response to these demonstrations, the Indonesian Minister of Transport (MoT) issued a regulation in early April, which specifically addressed transport apps. The new regulation provides that all transport app-providers (as that term is defined) must:

- establish an Indonesian legal entity;
- enter into a cooperation agreement with a licensed public transport provider; and
- not provide a general public transport service (ie, they must not determine tariffs, collect payments, hire drivers or determine the amount of a driver's income).

The new regulation provides, however, that if a transport app-provider does wish to provide a general public transport service, it must:

- itself obtain a public transport licence;
- own at least five vehicles;
- establish a car pool;
- provide a car maintenance facility (ie, garage); and
- hire licensed drivers only.

Compliance with the new regulation will be monitored by MoT investigators and police officers, who have sweeping investigative powers, including to the power to conduct traffic spot-checks.

Failure to obtain a public transport licence (if required) could result in the app-provider being restricted from expanding its business for two years.

This MoT regulation shocked industry players. Prior to it being issued, transport app-providers operated on the assumption that they were permitted to directly deal with drivers.

Such dealings would include requiring drivers to pay a certain percentage of their app-derived income to the app-provider. These dealings are not permitted under the new regulation, unless the app-provider complies with the requirements applicable to public transport service providers, including having to obtain a public transport licence.

What's next?

The new MoT regulation will come into force six months after its enactment on 1 April 2016. Therefore, transport app-providers, which are already active in Indonesia, have up to 30 September 2016 to comply with the new MoT regulation. (Alternatively, they may use this time to campaign for desired amendments to the new MoT regulation.)

Lessons learned

The new MoT regulation may indicate that other non-transport app-providers, which lack a formal Indonesian presence, will face equivalent restrictions in the future. These may include having to obtain a suitable operating licence.

Ernesto Apa
Portolano Cavallo,
Rome and Milan, Italy
eapa@portolano.it

New communication systems and taxi services: lessons from the Italian Uber case

In Italy, as in many other European and non-European countries, it has been debated for a long time whether the driving services provided by Uber may compete with traditional taxi services and whether the relevant legal framework may accordingly apply to the same. Several implications from the regulatory and competition law perspective may arise depending on whether the services of Uber are found to meet the characteristics of the services supplied by taxi drivers holding State licences or the chauffeur-driven car hire services ('CDCH'). The fact that the services being provided by Uber are operated by means of digital technologies lays bare how new communication systems challenge traditional and well-established legal categories and makes the rules governing these phenomena outdated.

Uberpop and the courts

The Uberpop service provided by Uber - consisting of an application that allows consumers to enter into contact with private car owners (who do not hold any licence and are not subject to any regulatory provision) – has raised fiercely debated legal issues, in Italy and elsewhere. The most recent developments include, among others, the decision of the French Conseil Constitutionnel, which found that criminal provisions affecting chauffeured vehicles for hire contained in the Loi Thévenoud were constitutional. The preliminary reference before the Court of Justice of the European Union raised by the Juzgado Mercantil of Barcelona on 16 July 2015, on the other hand, aims, in a nutshell, at exploring whether UberPop should be regulated as a taxi provider or as an app.

In Italy, the most important case was delivered on 25 May 2015 through an interim injunction by the Court of Milan, which ordered the blocking of the UberPop service in the Italian territory. According to the Court of Milan, the performance of UberPop services did constitute acts of unfair competition. In the view of the judges, the legislative framework in force pursues two different objectives: on one hand, the right to 'mobility', and on the other, the protection of passengers' security by the establishment of specific requirements for service providers. The Court also found that the existence of an assessment, as required by the relevant legal framework, does not undermine freedom to conduct business.

The Court has also considered the interference that the service provided by UberPop does actually pose in respect of the cab service offered by licensed taxi drivers. In the view of the Court of Milan, this interference is material because of different aspects. First, the service is provided according to the same etiquette as those operated by ordinary taxi drivers. Second, the Court has pointed out that the service is provided upon payment: in particular, the 'surge' pricing system, which consists of the application of higher fares depending on the availability of cars, considered as a scarce resource, unveils how compensation is not limited to the refunding of the expenses incurred by the driver.

The Court has also specified that the service provided by UberPop does not fall within car sharing services, as the driver's aim is to make money by carrying the customer to the destination chosen by the customer.

In addition to the above, the Court has excluded any claim that Uber meets the definition of 'intermediary' pursuant to relevant Italian legislation. In fact, Uber provides consumers with an app which permits them to enjoy services and, thus, is subject to articles 1678 and 1681 of the Italian Civil Code. It should be noted that the legal notion of 'intermediary', as intended by the Italian Civil Code, is also affected by the growing evolution of new communication systems.

Against this background, Uber obtains additional benefits compared to taxi drivers as it may apply higher fares, and so violate the provisions concerning the provision of public services.

The order of May 2015 has been challenged before the appellate body of the Court of Milan. The panel, however, upheld the Court order of 2 July 2015, first confirming that UberPop drivers are equivalent to taxi drivers holding public licences. As such, they are 'comparable' and competing on the same market.

Further, the Court upheld the finding of the first instance court whereby it excluded the service provided by UberPop from the scope of sharing mobility, particularly of car sharing services. It is specifically the application of fares varying depending upon market conditions and, in particular, supply and demand, that differentiates Uber services from car sharing ones.

Finally, the Court has noted that the violation of the relevant public law provisions by Uber results in greater profitability due to lower costs. This feature specifically creates a prejudice in respect of taxi drivers.

The views of the Italian Transport Regulation Authority

The Italian Transport Regulation Authority outlined its position on the matter in June 2015 in a report to the Parliament and the Government on 'Non-scheduled road transport passenger services: taxi, chauffeur driven car hire and technology mobility services'.

In the view of the Authority, 'it would be appropriate to regulate the technology platforms that mediate between supply and demand ('technology mobility services') and remove some of the constraints associated with the provision of taxi and car and driver hire services.'

While taxi and CDCH services meet a part of the mobility demand that is left unsatisfied by scheduled public transport, there are also systems based on the flexibility and sharing of resources (sharing economy). These include both key enablers (such as 'technology mobility services') and other innovative mobility systems, including bike sharing, car sharing and carpooling, which have emerged as a consequence of the new digital communication services. The dissemination of highly competitive mobile technologies has fostered the development of specific online and mobile service platforms that interconnect demand and supply of services based on the implementation of geolocalisation techniques.

The Authority has noted that these systems have significant effects on the supply of non-scheduled road transport passenger services since they meet the demand for services which are less expensive than those provided by taxi and CDCH and are delivered in a different way.

According to the Transport Regulation Authority, in addition to 'courtesy services' (operated by platforms promoting shared non-commercial transport services provided by drivers who share a predetermined route), there are platforms acting properly as intermediaries. These platforms offer technology services on demand and for commercial purposes on an intermediary basis. In this case, even though the driver is not a professional driver, the basis on which the service is provided is similar and comparable to other traditional taxi services. In practice, the price of the service not only covers the costs of the route, which is defined at the request of the passenger, but also allows these platforms to obtain a profit margin.

In light of the foregoing, the Authority has pointed out that some requirements may be set out insofar as intermediation services are concerned and that the relevant provisions of Law no. 21 of 15 January 1992 should accordingly be amended. These requirements should not apply, however, to 'courtesy services'.

Firstly, 'intermediaries' could be defined as the operators providing technology mobility services 'which, through the use of a technology platform, connect passengers and drivers so as to provide on request a paid-for transport service in the national

territory.' According to the Authority, these platforms should be registered in the regions where the respective services are provided. The reference and application to the specific area of the services provided by Uber reflects the impact of the digital technologies on the relevant market, where new operators are positioning themselves as agents relying on the use of the internet and mobile media as a means of delivering their services.

In addition, a further requirement should be set out in relation to the drivers. The definition of drivers may be amended in order to include 'holders of a licence to operate a taxi service, holders of an authorisation to operate a CDCH service and private drivers using their own private vehicle.' In the view of the Authority 'in the latter case, the private driver should be a casual worker, required to comply with a maximum annual income and a limited weekly working time not exceeding fifteen hours (while shifts of professional drivers can reach twelve hours daily). All drivers should be enrolled in a special register established on a regional basis.'

The role of the Italian Competition Authority

In September 2015, the Italian Competition Authority ('ICA') issued an opinion on a draft bill aimed at amending some of the provisions of Law no. 21/92.

The ICA has remarked that, in light of the nature of CDCH services (such as UberVan and UberBlack), some provisions of the law currently in force are likely to undermine competition. In particular, the requirement to return vehicles to a garage located in the municipality where the service is provided has been found to discriminate against drivers operating in municipalities other than those where they have been awarded a licence.

When it comes to the provision of services by the use of digital platforms these provisions turn out to be even more inapplicable, in the view of the ICA, as it would be detrimental to the freedom to conduct business (protected by article 41 of the Italian Constitution) to require compliance with an obligation based on the provision of well-established, traditional services; again, exposing the contrast between innovative technical solutions and conservative legal schemes.

With respect to UberPop, the ICA has noted that in the absence of a specific legal framework, these services shall not be considered unlawful or prohibited. Nevertheless, the platform connecting demand and non-professional drivers may equally respect some obligations, including the provisions of the 'Codice della Strada' (Legislative Decree no. 285 of 30 April 1992), regulating the circulation of vehicles. Thus, the requirement and interest in protecting security of passengers may not be undermined for the sake of competition, as noted also by the Court of Milan in the aforementioned orders. In this respect the ICA has called for 'minimum regulation' that should balance the need to foster competition and the interest of security and safety of passengers.

The Council of State

Finally, the Council of State is the institutional body that most recently considered the legal implications arising from the provision of UberPop services. These services, in the view of the highest administrative court, fall within the scope of non-scheduled road transport passenger services. Looking at the rationale behind the requirement to obtain a licence, the Council of State has noted that this is of a very different nature when the activity is not merely performed in the driver's own interest but is carried out for commercial purposes, with a view to making profit. In light of these circumstances, it is reasonable to impose further requirements which are necessary to ensure the safety and security of passengers and, more generally, of vehicles' circulation.

At the beginning of March 2016 a draft bill was proposed with a view to regulate 'sharing economy'. This is now under the consideration of the Italian Parliament. After the judges and regulators, now it is the turn of the legislator: regulation, then, remains a possibility, but with an eye still turned to the Court of Justice.

The devil is in the detail: the current state of Korean cloud computing regulatory reform

Eugene Kim
Kim & Chang, Korea
ekim@kimchang.com

Sangchul Park
Kim & Chang, Korea
scpark@kimchang.com

The Cloud Computing Act

Since the enactment of Korea's Cloud Computing Promotion and User Protection Act ('the Cloud Computing Act') on 27 March 2015 (effective as of 28 September 2015), the Cloud Computing Act has thus far attracted more attention around the world for its potential rather than its actual impact. The Korean legislation is the first of its kind and global IT and technology companies in particular have shared concerns that the legislation may serve as a precedent that could adversely affect any subsequent legislation or law-making in other jurisdictions relating to cloud regulation.

The original legislative intent, however, was to promote cloud computing in Korea, rather than to impose or strengthen regulations around it. In fact, the major portion of the Cloud Computing Act is composed of declaratory and non-binding provisions, covering: (1) a government blueprint for the promotion of cloud computing; (2) public agencies' efforts to introduce cloud computing in the public sector; (3) disclosure of public sector demand and plans regarding cloud computing projects; (5) designation of industrial zones to promote cloud computing; and (5) development and recommendation of government-initiated security guidelines and standard terms of service, etc.

To be sure, other sections of the Cloud Computing Act touch upon cloud computing service providers' legal obligations, such as: (1) security breach notification obligations; (2) obligations to identify the country where data is stored upon user request; (3) basic user protection measures; (4) return/deletion of customer information upon closure of business of the service provider or termination of service contract; and (5) damages liability, etc. However, it should be noted that most of these obligations are already covered by other Korean legislation.

In the context of the Korean government's push to promote cloud computing in Korea, the most meaningful development is seen in article 21 of the Cloud Computing Act. It stipulates that, if a certain law requires a certain level of IT facilities on the part of the business operator as a condition to a licence, permit, registration or designation, the use of cloud computing service by such operator shall be deemed to have satisfied such requirement. In many regulated industries, Korean regulators have in the past tended to reject applications for a business licence if the applicants tried to meet the relevant IT facilities requirement under the relevant legislation by use of third-party cloud computing services. This article is aimed to address such challenges by helping facilitate, in time, the introduction and use of cloud computing services in such regulated industries. However, this article does not apply in the following exceptional circumstances: (1) if the law explicitly prohibits use of cloud computing services; (2) if the law actually restricts use of cloud computing services by requiring physical separation of circuits or facilities; and (3) if the cloud computing service to be used cannot meet the relevant IT facilities requirement under the law.

Hence, notwithstanding article 21 of the Cloud Computing Act, 'the devil is in the detail' when it comes to assessing whether or to what extent the government's push to promote cloud computing in Korea will prove fruitful, especially in the regulated industries in Korea. This is because detailed requirements and conditions embodied in the relevant laws regulating financial industry, public sector or healthcare industry in Korea still serve to essentially block the introduction of the cloud computing service in these regulated industries. Some of the current challenges and difficulties and what measures are being proposed or contemplated to deal with them are considered below.

Financial Industry

To promote the introduction of the cloud computing service in the financial industry, two significant developments have been made recently under the auspices of the Korean government. First, the Financial Services Commission ('FSC') - the primary government enforcement body in the Korean financial industry - lifted prohibition of overseas outsourcing (except in relation to unique identification information) or re-outsourcing of IT facilities of financial services companies, by amending the Regulation on Outsourcing of Data Processing of Financial Companies (the 'IT Outsourcing Regulation') on 22 July 2015. Second, on 18 March 2015, the FSC deleted Article 15(2)(i) of the Electronic Finance Supervision Regulation ('EFSR'), which mandated Common Criteria ('CC') Certification (note that this does not mean a typical CC as an international standard but a local CC) for information protection devices utilised for financial IT systems.

While this is a significant development, some remnant provisions in the EFSR still impede the introduction of the cloud computing service. Some examples of restrictions or prohibitions are as follows: (1) the requirement to locally locate an IT room and a disaster recovery centre; (2) the prohibition of the use of Wi-Fi in an IT room; (3) a network separation requirement (which, in principle, means physical separation, although there are certain exceptions); (4) the requirement to use a private line to connect between a financial institution and outsourcing companies, and (5) the obligation to conduct regular security reviews in relation to outsourcing. For the time being, the possibility of the Korean financial services market being open to cloud computing service providers will largely depend on how or to what extent these specific restrictions or prohibitions remaining in the regulations will be interpreted or otherwise relaxed.

Public Sector

Article 12 of the Cloud Computing Act stipulates that government institutions, local governments and public institutions should endeavour to introduce and implement cloud computing, and should preferentially consider the introduction/implementation of cloud computing when planning budgets necessary to promote national information policies or projects. That said, it would be practically difficult for global players to enter the Korean public sector market, unless and until the current relevant regulations are lifted. These are briefly described below.

In accordance with the e-Government Act and the Enforcement Decree for the Act on Control of Public Records, government agencies (central and provincial) and government-owned corporations must undergo the Security Compatibility Certification by the relevant authorities when implementing IT products including security function, or network products in their operations. As part of such Security Compatibility Certification, a review is undertaken to determine whether certain designated IT products including security function have gone through local CC Certification and/or whether relevant encryption modules have gone through a Cryptographic Module Validation Programme ('CMVP'). These local requirements have been major hurdles frustrating the use of cloud computing services provided by overseas-based providers in the Korean public sector.

Nonetheless, the Korean government is now considering the Information Resource Grading System and the Information Protection Grading System, which aims to classify IT resources and public agencies into various grades and to make available less sensitive IT resources of less sensitive public agencies to cloud computing. If and when this is actually introduced, the advent of cloud computing in government-owned enterprises is likely anticipated. However, the specific details around such systems and how such systems would be implemented and operate to provide for greater use of cloud computing in the public sector remain to be seen.

Healthcare Industry

The Medical Act requires medical institutions in Korea to equip themselves with facilities and devices necessary to securely control and keep electric medical records pertaining to patients, and prohibits sharing of medical records pertaining to patients with external third parties. Based on these statutory requirements, the position of the Ministry of Health & Welfare ('the MHW') has been that the facilities and devices necessary for control and maintenance of electronic medical records must be placed physically within the medical institution. Due to such interpretation, the storage and processing

of such electronic medical records through cloud computing has been prohibited. Hence, despite the passage of the Cloud Computing Act, use of cloud computing services in the Korean healthcare industry is still restricted.

Recently, the MHW has announced that it is considering amending the Enforcement Regulation for the Medical Act. It is possible that such amendment, if passed, may allow medical institutions to place electronic medical records outside of their premises, provided that certain secure control and retention requirements are met. However, it may take some time before any such amendment becomes a reality.

Regulation and key developments of wireless service in Brazil

Ricardo Barretto Ferreira da Silva*
Barretto Ferreira e Brancher (BKBG), São Paulo, Brazil
barretto@bkbg.com.br

Camila Taliberti Ribeiro da Silva**
Barretto Ferreira e Brancher (BKBG), São Paulo, Brazil
taliberti@bkbg.com.br

Overview

The telecommunications sector is regulated by Law 9,472 of 16 July 1997 - the General Telecommunications Law - which sets out that the executive branch is responsible for establishing the telecommunications policy whereas the National Telecommunications Agency (Anatel) is in charge of implementing such policy by regulating and supervising the sector.

The Telecommunications sector's regulations have been quite stable since its inception back in 1997. More recently, Brazilian regulation policies in telecommunications have increasingly turned to the promotion of new technologies involving broadband internet and mobile telephony, which are services provided under a private regime without obligations of continuity and universal coverage. On the other hand, fixed switched telephony services ('FSTS') are the only communication service delivered under a public regime and subject to universalisation goals and continuity of service provision, the reason for which the interest of telecommunications companies in developing this service has been decreasing.

It reveals that the Brazilian Government has been attempting to keep pace with the global trend of conversion of traditional telecommunication services into technology services using internet platforms and creating a regulatory framework on internet platform services.

In November 2015, the Ministry of Communications launched a public consultation to debate on the review of the current telecommunications services framework and process of convergence. Based on the result of that public consultation, in April 2016, the Ministry of Communications enacted an Ordinance aiming at placing the broadband services at the centre of public policies, given the following objectives:

- expansion of transmission in high-capacity optical fibre and radio for more municipalities;
- extension of the coverage to villages and rural areas with mobile broadband;
- increased breadth of access networks based on fibre optics in urban areas; and
- attending to public bodies, with priority to education and health services, with broadband internet access.

Anatel will provide instruments to make possible the migration of the current awarding of FSTS to a system of greater freedom, thus conditioning such migration to broadband access goals.

Wireless regulation

Under Brazilian law, wireless service corresponds to fixed and mobile broadband. Fixed broadband is defined by Anatel as Multimedia Communication Service ('MCS' or Serviço de Comunicação Multimídia), and mobile broadband is provided jointly with mobile telephony, which is defined as Personal Mobile Service ('PMS' or Serviço

Móvel Pessoal). Both services depend on prior authorisation by Anatel and may be associated with the right of use of radio frequency.

The rendering of the MSC does not include the transmission, emission, and reception of information of any nature that could amount to the rendering of switched fixed telephone service (FSTS), broadcasting services, and pay or subscription television ('SeAC'), nor the supply of audio and video signals in an unrestricted and simultaneous manner to subscribers.

Anatel Resolution Number 614/2013 establishes that in order to obtain the authorisation to provide MCS, interested companies must:

- be organised according to Brazilian laws with their head offices and administration in Brazil;
- not be forbidden to bid or to contract with the Public Power; not have been declared incompetent or not have been punished, in the two previous years, with the cancellation of a grant, permission or authorisation to provide telecommunications services, or the cancellation of the right to use radio frequencies;
- have legal and technical qualification to provide the service, as well as economic-financial capacity and tax compliance, and be compliant with the Social Security; and,
- not be, in the same service area, or a part thereof, in charge of providing the same kind of service.

Anatel determines whether these conditions are satisfied and will then render a decision on an application within 90 days from its submission date. The number of authorisations for the exploitation of the MCS is unlimited.

The authorisation of MCS is granted for an indeterminate period of time and requires the payment of a public price in the amount of BRL 9,000 plus annual fees, such as: (1) the Installation Inspection Fee ('TFI'), which is the fee on the inspection of installation of stations; (2) the Operating Inspection Fee ('TFF'), which is the fee due upon inspection of the functioning of stations; and (3) the Contribution for the Development of the Domestic Film Industry ('CONDECINE').

On the other hand, a PMS authorisation makes possible communication between mobile stations and between mobile stations and other stations. According to Anatel's Resolution 321/2001, which provides for the Regulation on the General Plan for PMS Authorisations, the PMS provider must be organised under Brazilian law and have its head offices and administration in Brazil. A provider, its parent, subsidiary, or associated company is prohibited from rendering PMS through more than one authorisation, in the same geographical service provision area, or a part thereof. In addition, a PMS provider is subject to several duties and obligations before Anatel, which are established in the PMS Regulation (Anatel's Resolution 447/2007).

The authorisation for PMS is granted for an indeterminate period of time, but the right of use of the radio frequency associated with PMS is granted for 15 years, renewable once for an equal period. It requires the payment of a public price in the amount of BRL 9,000 plus the annual fees mentioned above.

Wireless key developments

Broadband has been considered by the Government an essential service and necessary for the country's economic and social development. It is also a prerequisite for the entry of new technologies and services that use the internet as a platform (ie, M2M, OTTs and Web TV). In this context, it is essential that broadband access be expanded on a universal basis, especially in rural and remote areas.

Under Decree 7,175, since 2010 the Brazilian Government has been implementing the National Broadband Plan ('PNBL') with the purpose of expanding broadband internet access across the country by using the optical fibre infrastructure owned by electric power transmission concessionaries and public companies (such as Petrobras).

Decree 7,175/2010 also approved the revival of Telebrás, which was the government-owned holding company that controlled the State companies privatised in the 1990s. At present and following a great deal of discussion on the matter, Telebrás intends to provide broadband access to the wholesale market only. The intention of the Brazilian Government is to ensure that a 1-Mbps-speed broadband internet service be available for sale by Telebrás to internet service providers at a maximum price of BRL 35 per month.

In addition, in an effort to promote widespread adoption of telecommunication equipment and investment in the country's communication structure by the private sector, the Decree establishes a reduction in

certain taxes through a plan called 'Special Taxation Regimen' for PNBL. Tax relief has been offered for broadband networks expansion enterprises that use national equipment and construction material, revenue for projects specifically developed for telecommunications, and acquisition of M2M equipment.

Mention should be made of the Cidades Digitais (Digital Cities) Programme, which aims at increasing modernisation of municipal management through construction of fibre optical linking public entities, development of e-government applications, and implementation of free Wi-Fi zones in public spaces of large circulation, such as squares, parks and roads.

Finally, the Ministry of Defence has launched the Amazônia Conectada (Amazon Connected) Programme to install 7.8 km of fibre optic cables through Amazonian rivers and offer opportunities for a series of data network services in the countryside of the State of Amazon, such as internet, telemedicine, distance learning and interconnection between health, public security, traffic and tourism.

Notes

* Senior managing partner

** Associate lawyer