the global voice of the legal profession

Communications Law

Committee Update of the International Bar Association Legal Practice Division

VOLUME 23 ISSUE 1 SEPTEMBER 2017

International Bar Association
Conferences 2017–2018




2017

6–8 SEPTEMBER 2017 ETC.VENUES, LONDON, ENGLAND
IBA Europe-Caucasus-Asia (ECA) Forum

8–9 SEPTEMBER 2017 ST REGIS, FLORENCE, ITALY
21st Annual Competition Conference

WEBINAR 12 SEPTEMBER 2017, 1300 BST
Legal directories – the bane of the lawyers' lives, or the way to the stars?

14 SEPTEMBER 2017 MARINA BAY SANDS, SINGAPORE
The Fundamentals of International Legal Business Practice

14–16 SEPTEMBER 2017 HILTON BRUSSELS GRAND PLACE, BRUSSELS, BELGIUM
6th Construction Projects from Conception to Completion

8–13 OCTOBER 2017 INTERNATIONAL CONVENTION CENTRE, SYDNEY, AUSTRALIA
IBA Annual Conference 2017

IBA 2017 Sydney 8–13 OCTOBER
ANNUAL CONFERENCE OF THE INTERNATIONAL BAR ASSOCIATION

OFFICIAL CORPORATE SUPPORTER
LexisNexis®

2–3 NOVEMBER 2017 MANDARIN ORIENTAL HOTEL, HONG KONG SAR
Asia Pacific Mergers and Acquisitions Conference

4 NOVEMBER 2017 HANOI, VIETNAM
IBA-APAG International Arbitration Training Day: Introduction of the IBA Soft Laws

4–5 NOVEMBER 2017 QUEEN MARY UNIVERSITY OF LONDON, ENGLAND
IBA-ELSA Law Students' Conference

6–7 NOVEMBER 2017 SÃO PAULO, BRAZIL
Latin American Anti-Corruption Enforcement and Compliance

10 NOVEMBER 2017 MOSCOW, RUSSIAN FEDERATION
9th Annual 'Mergers and Acquisitions in Russia and CIS' Conference

13 NOVEMBER 2017 CORINTHIA HOTEL, WHITEHALL PLACE, LONDON, ENGLAND
Once in a Lifetime Opportunity or Cliff-Edge Threat: The Antitrust Implications of Brexit

15 NOVEMBER 2017 LEVEL 39, 1 CANADA SQUARE, CANARY WHARF, LONDON, ENGLAND
European Start Up Conference 2017

15–17 NOVEMBER 2017 THE GRANGE ST PAULS, LONDON, ENGLAND
8th Biennial Global Immigration Conference

15–17 NOVEMBER 2017 LABADI BEACH HOTEL, ACCRA, GHANA
Rising to the Challenge of Africa's Development

16 NOVEMBER 2017 FOUR SEASONS HOTEL LONDON AT PARK LANE, LONDON, ENGLAND
Private Equity Transactions Symposium

17 NOVEMBER 2017 MONDRIAN LONDON, LONDON, ENGLAND
Building the Law Firm of the Future

30 NOVEMBER – 1 DECEMBER 2017 BUENOS AIRES, ARGENTINA
The New Era of Taxation: How to Remain on Top in a World of Constant Evolution

1 DECEMBER 2017 MOSCOW, RUSSIAN FEDERATION
11th Annual Law Firm Management Conference

7–8 DECEMBER 2017 MILLENNIUM BROADWAY HOTEL, NEW YORK, USA
Investing in Asia

7–8 DECEMBER 2017 JUMEIRAH FRANKFURT, FRANKFURT, GERMANY
4th Annual Corporate Governance Conference

2018

18–19 JANUARY 2018 HONG KONG SAR
IBA Law Firm Management Conference: Growth Prospects for Law Firms in Asia

29–30 JANUARY 2018 ETC.VENUES, FENCHURCH STREET, LONDON, ENGLAND
7th Annual IBA Tax Conference

1–2 FEBRUARY 2018 THE WESTIN PARIS – VENDÔME, PARIS, FRANCE
6th IBA European Corporate and Private M&A Conference

14–16 FEBRUARY 2018 PARIS INTERCONTINENTAL, PARIS, FRANCE
IBA/ABA International Cartel Workshop

23–24 FEBRUARY 2018 HOTEL EUROSTART GRAND MARINA, BARCELONA, SPAIN
3rd Mergers and Acquisitions in the Technology Sector Conference

25–26 FEBRUARY 2018 BUENOS AIRES, ARGENTINA
21st Annual IBA Arbitration Day

5–6 MARCH 2018 LONDON, ENGLAND
23rd Annual International Wealth Transfer Practice Law Conference

8–9 MARCH 2018 HONG KONG SAR
3rd IBA Asia-based International Financial Law Conference

9–10 MARCH 2018 THE TAJ MAHAL PALACE, MUMBAI, INDIA
The Changing Landscape of M&A in India – New Opportunities in a Dynamic India

11–13 MARCH 2018 LONDON, ENGLAND
18th Annual International Conference on Private Investment Funds

14–16 MARCH 2018 HYATT REGENCY HOTEL AND INTERCONTINENTAL PRESIDENTE HOTEL, MEXICO CITY, MEXICO
Biennial IBA Latin American Regional Forum Conference

Full and further information on upcoming IBA events for 2017–2018 can be found at: **bit.ly/IBAConferences** @IBAevents

IN THIS ISSUE

Contributions to this update are always welcome and should be sent to the Newsletter Editor, Jana Pattynova, at the address below:

Jana Pattynová
Pierstone, Prague
jana.pattynova@pierstone.com

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 update 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 update 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 of the Communications Law Committee

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

We are writing this issue in the aftermath of our annual IBA Communications and Competition conference in Berlin. It was a great success, with over 100 delegates attending the two-day conference. We had excellent panels about the latest trends within regulatory development and discussed highly important issues reflecting developments in Europe and also globally, such as Brexit.

We are entering a new world and era that is even more digitalised and globally connected than at present. In the past, we have discussed and argued about the regulatory implications of public switched telephone networks and dial-up internet regulation; whereas today, we are having discussions about autonomous driving, connected cars and machine-to-machine interconnection, with industrial sectors moving more and more of their processes to the industrial internet.

Therefore, communication is playing an even bigger role in society than it was in the past and we, as sector-specialised lawyers, have a large role to play in how this development is proceeding in different countries and businesses, and how it reflects the needs of end users.

Even if the world is getting more connected, it is also getting more complex, with various stakeholders affected by the regulatory development. Therefore, it is even more important that we have platforms to review and discuss this development. We are going to have very interesting sessions at the IBA Annual Conference in Sydney, Australia, with topics such as 'data, a new oil', 'firewalls on the internet' and many other sessions.

I am looking forward to seeing many of you attending our sessions and also developing the culture of communications lawyers by sharing the same passion for building a better society and bringing new innovations to the market.

In June 2018 we shall reconvene at the 29th Annual Communications and Competition conference in Milan which, in my belief, will be a great event. I hope to see you all there and share interactive debates over actual topics in the area of competition and communications law.

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

With regards,
Jukka-Pekka Joensuu

Jana Pattynová
Pierstone, Prague
jana.pattynova@
pierstone.com

From the Editor

Dear Communications Law Committee members,

The last year has been extremely interesting for our field of practice, thus, it is my pleasure to present you with an interesting mix of articles on various topics.

Our Co-Chair, Jukka-Pekka Joensuu, opens this year's Committee Update with a review of today's digital world and emphasises the importance of digital infrastructure for global connectivity, which will become increasingly indispensable in the future.

When it comes to Europe, last year we experienced many important and, admittedly to many of us, surprising changes. What comes to mind first is probably the Brexit vote in the United Kingdom. Britain's decision to leave the European Union will inevitably have consequences not only for the UK, but will likely impact affairs in the rest of Europe and the world as a whole (even more so if we consider communications, flow of data and digital sectors in general, which rely on interconnection more than other parts of industry and innovation). I am pleased to draw your attention to two articles on this topic, by Amar Breckenridge and Ian Hathaway of Frontier Economics and by Matt Hunt and Neil Pratt of Alix Partners, which will give you an in-depth insight into how much the British digital sector actually relies on connectivity to Europe and the rest of the world and what the likely impacts of Brexit on the UK telecoms regulation are.

Nonetheless, apart from Brexit, Europe is feverishly preparing for another major event – the General Data Protection Regulation (GDPR). The EU's GDPR will enter into force in May 2018, bringing along significant changes in the area of personal data protection. Those who fail to comply with its new strict requirements will risk heavy fines imposed by the European Commission.

This year, we have three more articles which will shed some light on the current digital situation in the EU. The first article, authored by Blanca Escribano, assesses the impact of new digital technologies on the health sector and drug production. I have contributed a short article on the current EU's struggle with balancing privacy and security when it comes to end-to-end encryption and backdoors to such encryption. In the third article, Zoltán Marosi and Lia Scheuer-Szabó report on a record fine imposed by the Hungarian regulatory body for misleading mobile internet advertisements.

Leaving Europe behind, we will explore the recent regulatory developments in Chile and Australia. As our colleagues from these countries attest in their contributions, both countries are currently facing legislative changes of great importance, in particular in the field of communications. The article, authored by Alfonso Silva and Raúl Mazzarella, describes a new regulatory framework enacted by the Chilean communications authority regulating the minimum technical specifications of mobile devices operating in Chilean mobile networks; the purpose of this regulation is to protect free competition, consumers' rights and sustainable development of technology. The last article, contributed by Angela Flannery, covers legal development in Australia, the host country of the IBA 2017 Annual Conference. Australia is in the process of reviewing and reforming its legislation regulating the spectrum. The new regulation is anticipated to come into force in 2019 and is hoped to provide a more flexible approach to the use of the spectrum.

And finally, Vittorio Noseda and Nana Adjoa Asante look into the global question of digital platforms and provide an insight into the European approach to the digital platform regulation

Some of these topics will also be discussed and covered at the 28th IBA Annual conference in October in Sydney, where I hope to see many of you. I would like to extend my congratulations and thanks to the Co-Chairs and authors of the articles for their outstanding work and enthusiasm. I hope that you will find this year's Committee Update as interesting as I do, and that you will consider contributing next year.

Committee Officers

Co-Chairs

Anne Vallery
WilmerHale, Brussels
anne.vallery@wilmerhale.com

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

Senior Vice Chair

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

Vice Chairs

Alfonso Silva
Carey, Santiago
asilva@carey.cl

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

Secretary

Blanca Escribano
CMS Albinana & Suarez De Lezo, Madrid
blanca.escribano@cms-asl.com

Membership Officer

Sam Feder
Jenner & Block, Washington, DC
sfeder@jenner.com

Conference Coordinator

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

Latin American Regional Forum Liaison Officer

Alfonso Silva
Carey, Santiago
asilva@carey.cl

European Regional Forum Liaison Officer

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

Young Lawyers Liaison Officer

Blanca Escribano
CMS Albinana & Suarez De Lezo, Madrid
blanca.escribano@cms-asl.com

Special Projects Officer

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

Website Officer

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

Newsletter Officer

Jana Pattynova
Pierstone, Prague
jana.pattynova@pierstone.com

North American Forum Liaison Officer

Sam Feder
Jenner & Block, Washington, DC
sfeder@jenner.com

LPD Administrator

Susan Burkert
International Bar Association, London
susan.burkert@int-bar.org

IBA 2017 Sydney
8–13 OCTOBER
ANNUAL CONFERENCE OF THE INTERNATIONAL BAR ASSOCIATION

Communications Law Committee's sessions

Monday 0930 – 1230

Around the tables: breakfast and a taste of hot topics in the Intellectual Property, Technology and Communications Section

Presented by the Intellectual Property, Communications and Technology Section, the Art, Cultural Institutions and Heritage Law Committee, the Communications Law Committee, the Intellectual Property and Entertainment Law Committee, the Media Law Committee, the Space Law Committee and the Technology Law Committee

This always very dynamic and well-attended session enables you to select from a menu of hot topics in the Intellectual Property (IP), communications, media and technology sectors, and participate in roundtable discussions.

The format is interactive networking. Topics are selected to be of current interest and likely to stimulate a lively debate. Moderators on each table introduce the table topic and the participants do the rest. Background knowledge or experience within areas for discussion is not required. You will have the opportunity to discuss four topics: at scheduled turnover times the participants move around the tables to the next topic of their choosing.

Our menu will include hot and 'late breaking' topics in the areas of intellectual property law, internet law and mobile technologies, technology contracting and dispute resolution, arts law and space law.

Discussion is usually around the interface of law, business and technology, with a global focus. Many topics for discussion are often the subject of considerable public and media interest, and this will be the case again. In participating in the table topics, you will gain a greater insight into these areas and be able to add your own comments. In addition, a 'degustation' breakfast buffet will be hosted in the room so that no time is wasted for those who want to boost their energy levels prior to or during the session.

The session will provide you with a great opportunity to meet many other lawyers to discuss topics of mutual interest with them: don't forget your business cards. We welcome new participants in these discussions. We will also be soliciting your views about your areas of interest and other suggestions to enable the Section to programme future activities accordingly.

The following topics will be discussed during the session, with the help of the respective moderators identified for each topic:

Table 1

a) Disavowing authorship: in March 2017, artist Richard Prince returned the money paid by Ivanka Trump for her portrait as a political protest against the Trump administration. Can an artist legally repudiate his authorship of a work of art? Does the collector have any legal recourse against a decision that can potentially destroy the economic value of an artistic asset?

b) Public art ownership and market value: a recent judgment in Italy held that the damage that has occurred to a sculpture owned by a municipal museum while it was being exhibited abroad could not be assessed with reference to market value standards (ie, international auction prices of similar works of the artist) because art owned by a public entity is unsaleable in Italy. How does the law work in countries where deaccessioning is permitted? How does (or should) private versus public ownership affect the liquidation of damages by courts? Should the private versus public nature of the owner of an artwork be taken into account by insurance companies in assessing the risk associated with insurance coverage?

Table 2

a) Recently made and planned domestic space legislation

b) Space 2.0: comparison of startup environments in jurisdictions worldwide

Table 3

Time to take off the gloves: website blocking to stop the misuse of IP rights

Table 4

Sights and sounds and shapes and smells, these are a few of my favourite things: the benefits and challenges associated with non traditional trade marks

Table 5

The UPC: where are we now?

Table 6

To 3D or not to 3D: what does 3D printing mean for intellectual property?

Table 7

Biosimilars: how similar is similar enough? From cures to cancer to

Continued overleaf

alleviating arthritic pain, biologics are at the frontier of new medicine. But as with all next generation technologies, biologics present a number of patent and other IP challenges for both the biologic developers and those wishing to bring similar products to the market.

Table 8

a) Image rights/data privacy claims: data privacy and image rights claims are on the rise around the world (particularly in the EU/UK). We'll discuss various facets of the topic.

b) Libel suits and social media: with the recent Jack Monroe/Katie Hopkins libel judgment in the UK (finding Katie Hopkins liable for politically tinged tweets that, in the US at least, would surely have been deemed non-actionable hyperbole), it seems like a good time to discuss how social media is changing the rules of the road when it comes to the free speech/reputation balance.

Table 9

Blockchain: the chain unravelled

Table 10

Government access to information technology (IT) systems

Table 11

Robotics and artificial intelligence (AI): outsmarted by machines

Table 12

Ownership in data

Table 13

Hacks, leaks and liabilities: from distributed denial-of-service (DDOS) to the internet of things (IoT) and plenty in between, who is liable when data leaks?

Table 14

Smart cities

Table 15

Digital platforms: rise and fall.

Monday 1230 – 1330

Communications Law Committee open business meeting

Presented by the Communications Law Committee

An open meeting of the Communications Law Committee will be held to discuss matters of interest and future activities.

Monday 1430 – 1730

Information: the new oil

Presented by the Intellectual Property, Communications and Technology Section, the Art, Cultural Institutions and Heritage Law Committee, the Communications Law Committee, the Intellectual Property and Entertainment Law Committee, the Media Law Committee, the Space Law Committee and the Technology Law Committee

Information has become the new oil and the fundamental building block in the new digital era. Stakeholders are using, collecting and accumulating data and using it for marketing and other various purposes.

In this session, we will discuss the following interesting related topics:

- When is it okay to do so (eg copyrighted content and public data)?
- Who has lawful access to the data (eg, robots.txt, CAPTCHAs and paywalls)?
- What can be done with the information (eg, redisplay, text and data mining and internal use versus commercial use)?
- Who ultimately owns the data?
- What are contractual issues (eg, enforceable terms and conditions)?

Tuesday 1430 – 1545

Firewalls on the internet

Presented by the Communications Law Committee and the Human Rights Law Committee

We are experiencing the internet moving towards many different layers and away from the open internet. There are also many players from the governmental sector to the private sector who want to have control over the internet and various layers. How can we ensure the future development of internet services, individual rights of citizens and governmental interests together with globalisation?

The session will focus on technical and public policy issues, including privacy and other important viewpoints.

The session will also address to what extent global responses to such challenges would be necessary, discussing the international frameworks that are already available with respect to privacy and data protection, such as the Privacy Shield between the EU and US.

Continued overleaf

Wednesday 0930 – 1230

Development of future megacities, infrastructure and services

Presented by the Communications Law Committee

Cities are beginning to invest in stronger, more resilient and flexible technology infrastructure. Whether the purpose is to improve local authorities' engagement with their communities, from waste collection to social care or even shared economy platforms, the need for connectivity is pervasive. The internet of things plays, and will continue to play, an increasingly important role within our cities as they move to a higher level of sensory equipment being retrofitted into our buildings and the space around us.

Whether projects are undertaken in the Middle East, Europe or Asia, one factor has been key to their successful planning and execution: a highly integrated telecoms and fibre network that is future-proofed to deal with the ever-increasing demands technology and society will place on it. Smart cities enhance quality of life through the integration of information and communications technology (ICT) within the infrastructure framework. Upon successful implementation, smart cities will not only boost commercial and capital investments but will be the best approach for reducing the tremendous strain on present day infrastructure.

The success of large-scale projects – and the delivery of the expected output for citizens – therefore rely on the successful planning of authorities and, where relevant, the adoption of the appropriate regulations likely to foster innovation and development, in particular in relation to the sourcing and roll-out of appropriate ICT services.

Whereas, at a local scale, issues arising out of cities' transformation may be focusing on funding, financing, planning and procurement, more global and regulatory issues arise once clear development policies are devised, in particular in relation to (1) spectrum management and allocation, (2) fostering competition on the market (especially where operators do not all have the same network footprint) and (3) guiding future users, authorities and other city stakeholders in handling the vast amount of data they will necessarily collect and process.

Using the current examples of smart city projects around the world, and building upon the conclusions that may be drawn from those, this session will explore in further detail why communication law concerns have a core impact in successfully developing smart cities and paving the way for businesses to invest in and contribute to the community.

Wednesday 1430 – 1730

International online distribution issues - Part 1

Presented by the Antitrust Committee and the Communications Law Committee

This panel will explore issues arising in the online distribution of goods and digital content around the world. The panel will discuss issues such as territorial restraints (export bans and exclusive distribution with a focus on cross-regional issues, eg, a US website not selling to Australian consumers), geoblocking (including the European Commission's e-commerce enquiry and initiatives in this area) and resale price maintenance (minimum advertised prices, platforms and pricing, sales on app stores).

The panel will begin with a keynote speech by Cecilio Madero Villarejo, Deputy Director-General for Antitrust at the Directorate-General Competition of the European Commission, on the European Commission's recent e-commerce inquiry report.

All information in the programme is correct at the time of print. To find out more about the conference venue, sessions and social programme, and to register, visit **www.ibanet.org/Conferences/Sydney2017.aspx**.

Further information on accommodation and excursions during the conference week can also be found at the above address.

FEATURE ARTICLES

Digital infrastructure: the key to economic development

Jukka-Pekka Joensuu
Co-Chair for the Communication Committee, IBA; Cinia Group, Helsinki
jukka-pekka.joensuu@cinia.fi

The key to the digital future – of manufacturing, logistics, travel, retail and communication – is providing secure, low-latency digital infrastructure. This article looks at how the new industrial revolution will change the way business is done around the globe.

Connectivity drives digital evolution

Taking a look into our history, innovations have built society more than anything else. Johannes Gutenberg enabled the main pillars for modern society and unintentionally created more awareness for what is happening in the world outside one's own village. It is fair to say that, without Gutenberg, Martin Luther would have been just a rebel priest preaching for a small audience. Instead, he created a religious movement with high impact in many societies. Today, communications platforms and connectivity drive digital transformation.

Role of connectivity

Today's society is globally more connected than ever. Digitalisation is becoming a major theme in every seminar and discussion forum. Why is this so important?

In today's society, people are more connected than ever. A recent study about 'global tribes' indicated that millennials have more in common among themselves than within their respective countries and this will have a huge impact in tomorrow's society.

Furthermore, the impact on machine-to-machine interactions will be even higher. It has been said that whatever can be digitalised, will be digitalised. This means that many of the activities we are performing today will be performed by machines tomorrow.

Taking a concrete example, grocery shopping is one of the routines we are doing every day. In tomorrow's world, this whole process will be digitalised so that refrigerators can automatically inform retailers that I am running out of food and that retailers, which I as a consumer have an account with, will restock my grocery order automatically, most likely with robots.

We all know that, without connectivity between people, machines and processes, this evolution cannot take place. Therefore, we are more connected than ever and more dependent on connectivity than ever.

Emerging cities

Urbanisation and emergence of global cities is a major trend that heavily relies on the global economy being run by megacities like London, Singapore, Hong Kong and New York. A recent McKinsey study indicates that over 60 per cent of the world's GDP is being created in 600 cities around the world. By 2025, 136 new cities are expected to enter the top 600, all of them from the developing world and overwhelmingly – 100 new cities – from China.

This will have a huge impact on the whole global economy, and building a smarter society is vital for its success and growth. Amsterdam is a very good example of a smart European city, with extensive digital infrastructure and fibre connectivity; several internet exchange points create good connectivity between companies and people and an impressive number of digital companies, start-ups and data centres form a strong cluster for a smart city concept.

Digital Europe

Europe has made many efforts to become more digitalised and Digital Europe 2020 is envisioned to be created on seven pillars.

One of these is digital security and trust. Building digital trust is a major effort for the whole of society, trade and also for people using digital services.

The Finnish government made a major decision on a single digital market in Europe investing in a C-Lion 1 cable system between Finland and Germany. This new northern digital highway is connecting natural data centre havens in the Nordics with businesses and people in continental Europe with low latency, security and redundancy.

Also, other governments have made major efforts in enhancing digital development. Estonia has introduced the idea of digital citizenship and many countries in Europe are pushing digital agendas to create growth in an otherwise stagnated economy. Also, links between Asia and Europe need to be strengthened to promote the huge growth in Asia.

Germany, with its strong economic performance and experience in creating industrial champions, especially in the automotive industry, will also benefit from the digitalisation and the fourth industrial revolution built on an industrial internet and the 'Internet of Things' (IoT).

The IoT and growth of data

The IoT is really transforming the whole economic structure and changing entire industries. In the financial industry, this rapid development with blockchain and other technologies poses a major threat but also an opportunity to renew the whole industrial approach. This will also have a major impact on other traditional industries. Autonomous driving and steps towards new technologies create a major opportunity, not only regarding how cars are manufactured, but also how processes are run. Ownership and usage of cars and car pooling, as well as mobility as a service, will pose a major change, with new business opportunities in the new economy.

The world needs security and trust but also new innovations. A simple example of mobile phones changing the way we work and interact predicts something about the future, with augmented reality making better drivers or operators of cars, healthcare applications and people being able to be their own doctors.

All of this is heavily dependent on how well systems work, how interoperability is ensured, and how standards and protocols enable us to trust the applications used. These data-intensive machines and factories are run in data centres that are increasingly better connected and business will be more global than ever. Therefore, we have to build more connectivity, and the digital bridge between Asia and Europe will become more essential.

There is a project known as 'Arctic Connect' that aims to build a secure subsea route over the Northeast Passage, which will bring point-to-point connectivity between Asia and Europe and to link the megacities of the world together with direct connections. Infrastructure is the key for overall development and digital infrastructure will be the key to economic development in the future, just as the road and railways have created past industrial successes.

The UK digital sectors after Brexit: free flow of data

Amar Breckenridge
Frontier Economics, London
amar.breckenridge@frontier-economics.com

Ian Hathaway
Frontier Economics, London
contact@frontier-economics.com

In a report commissioned by techUK, Frontier Economics examined the impact of the United Kingdom's exit from the European Union on the 'digital sector' – the groups of industries that produce or intensively use digital goods and services. The analysis focused on the links between the UK's digital sector and suppliers and customers globally and across Europe. Among the major findings, the report demonstrated that the digital sectors account for 16 per cent of output, ten per cent of employment and 24 per cent of exports. In particular, the report detailed the extensive international orientation of the digital sector, including its heavy reliance on global talent and cross-border data flows. In the following, we discuss the economics of cross-border data flows.

The United Kingdom has a digitised, information-driven, services-oriented economy that relies on free flow of data across borders. These cross-border data flows raise productivity and national income. Brexit potentially puts these flows at risk, creating a regulatory fragmentation of information and communication links between the UK and Europe – its largest trading partner for data flows.

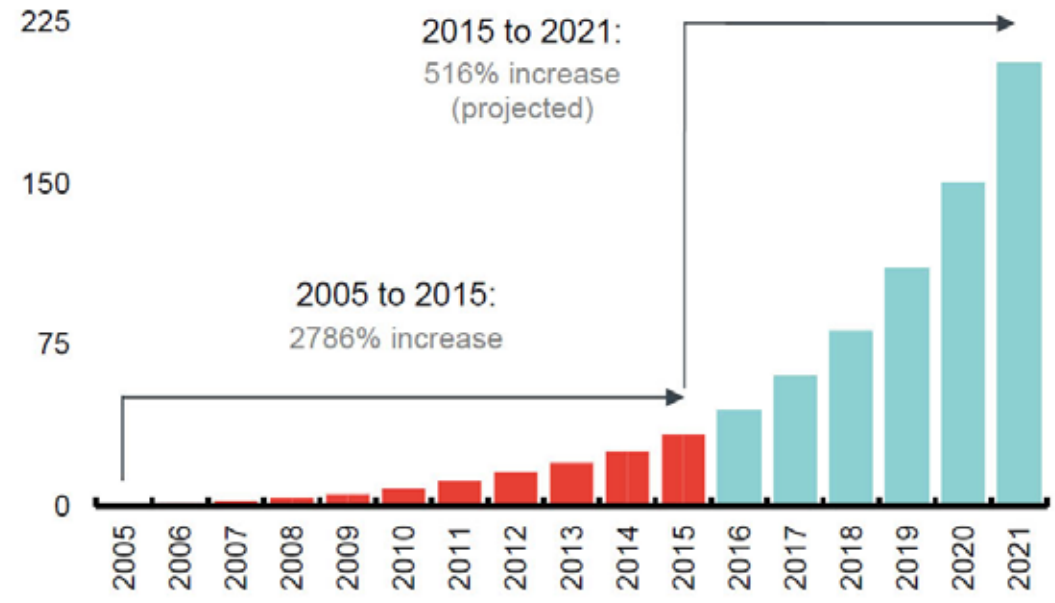
The economic value of cross-border data flows

Like international flows of goods, services, capital and people, the flow of information and data helps power modern economies. Businesses depend on data flows to access markets, facilitate supply chains and enable transactions around the globe.[1] This fact is especially true in an open, services-oriented economy like the UK – service industries account for 79 per cent of output and 43 per cent of trade exports across the country. For the digital sectors, those same figures are 96 per cent and 81 per cent. Economists estimate that about half of all trade in services is 'digitally-enabled' – they have the potential to be delivered remotely via information and communication links.[2]

However, measuring the economic value of cross-border data flows is challenging for a few reasons. The first is the nature of data flows, which are easy to witness but difficult to observe and measure in the statistical sense. Second, is the 'pricing' of many data flows. Some are associated with transactions where money changes hands and a market price is attached – such as digital platform services, online advertising, or data processing and hosting services. Others, such as data shared between or within businesses, or digital services that are transacted with end-users at a zero market price, fall outside of standard measurement mechanisms for market-based economic exchange. Looking at cross-border data flows within affiliated enterprises, one study found that UK firms are among the largest traders globally.[3]

One way to get around these conceptual and measurement challenges is to estimate the indirect impact that data flows have on innovation and efficiency – or how data flows improve productivity. The McKinsey Global Institute recently took this approach, measuring the 'spillover' benefits of cross-border data flows on gross domestic product (GDP) growth for 139 countries.[4] Their analysis estimated these benefits simultaneously with other international flows – of goods, services, people and capital – and controlled for other confounding factors. Their main conclusion was that cross-border data flows accounted for a 3.8 per cent uplift of global GDP in 2014, and the primary channels through which this manifests is productivity improvement and increased capital and labour inputs. As a relatively services-oriented economy and a leading digital adopter (as noted in the same report), this figure likely represents a conservative, lower bound estimate for the impact of cross-border data flows on the UK economy.

Figure 25. UK International Bandwidth in Terabytes per Second



Source: Frontier analysis of Telegeography, Cisco and McKinsey data
Note: Figures are capacity, not actual flows; figures from 2016 to 2021 are forecasts

These estimates are aligned with a United States government study that calculated a 3.4 to 4.8 per cent increase in GDP from 'digital trade', in addition to an increase in wages of 4.5 to 5 per cent, and the creation of 2.4 million jobs.[5]

UK cross-border data flows

The UK is a leader in cross-border connectivity, accounting for 11.5 per cent of global cross-border data flows in 2015. By comparison, the UK accounted for 3.9 per cent of global GDP and 0.9 per cent of global population.[6]

Figure 25 (above) of the frontier analysis of Telegeography Data and World Bank Open Data shows the growth in cross-border data flows for the UK from 2005 to 2015, with forecasted figures through 2021. Cross-border data flows between the UK and partner countries have achieved explosive growth in the last decade, and are now 28 times what they were in 2005. We forecast flows will continue to increase over the next decade and will be a factor of six times in 2021 compared with what they were last year.

As Figure 26 (see overleaf) of the frontier analysis of Telegeography Data and World Bank Open Data shows, 75 per cent of UK cross-border data flows are with European Union partner countries. These flows are generally for information, communications, search, audio and video, transactions, inter- and intra-company traffic, and machine-to-machine links (smart connected devices and logistics), and are due to strong links between UK–EU households and consumers, but also businesses. It is not possible to disaggregate data flows among these groups with the information we have available. As stated before, 43 per cent of total UK exports are services-related, more than one-third of these trade flows are with European partners, and the majority of trade in services is underpinned by cross-border data flows.

By comparison, 84 per cent of cross-border data flows for a European mainland country – Germany – are with EU partners. Much of this difference is made up through stronger links between the UK and North America (primarily the US).

Data flows and Brexit

So clearly, cross-border data flows are increasing rapidly for the UK, are heavily linked with European countries, and are important in driving economic activity – particularly for an open, services-driven

economy like the UK. But, what does that mean with regard to Brexit? A few points are worth making briefly.

The biggest challenge is the upcoming implementation of the EU's General Data Protection Regulation (GDPR), which is a new personal privacy law that comes into effect in May 2018. The GDPR expands and unifies the protection of personal data on individuals within the EU, and restricts the flow of that data outside the EU. It has wide-reaching effects on individuals and businesses.[7]

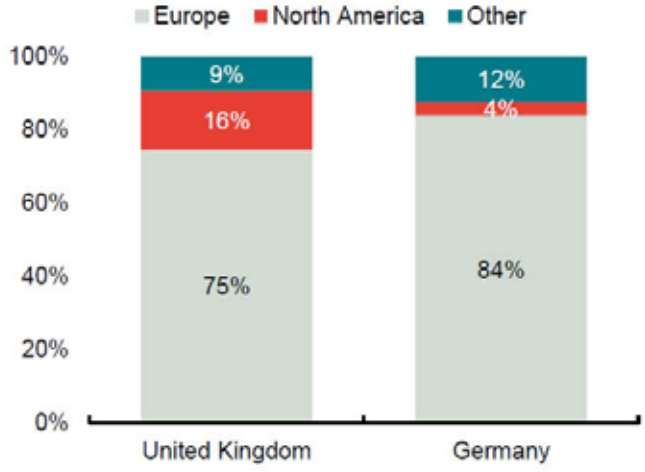
Notably, the GDPR will require full implementation in the UK ahead of exiting the EU, as the Regulation will apply in May 2018, almost certainly prior to the completion of Article 50 negotiations and the UK's formal exit from the EU. Even if the UK were to maintain data protection regulations identical to GDPR – for purposes of continuity, EU market access or other reasons – risks remain. Adoption still leaves open the question of the secure legal basis on which companies can transfer data in and out of the EU. GDPR adoption does not ensure 'adequacy', which can apply to third countries and is decided by the European Commission.[8]

An 'adequacy' decision determines that a third country offers an equivalent level of protection compared to provisions laid out in EU law, satisfies recent EU case law and matches the expectations of the Article 29 Working Party's templates for adequacy decisions. Any UK adequacy decision would be based on the Commission's full review of the UK's domestic data regime to determine how the UK's data protection landscape matches the requirements of EU law.

An assessment of such issues is outside the scope of this analysis, but ensuring adequacy will be something the UK government will need to consider ahead of upcoming negotiations.

Failure to secure adequacy may force the 'localisation' or redirection of data flows on EU citizens (that requires storage and/or processing outside the UK), risking fragmented communications links and data flows between the UK and European partners. In addition, many UK businesses will need to implement costly alternative legal mechanisms, many of which are subject to ongoing legal challenge and uncertainty. Continued uncertainty over EU–UK data flows could also see companies restrict the amount and type of data processed in the UK. Such an outcome could impact data infrastructure and, in particular, data centres in the UK, which are among the region's and the world's most active.[9]

Figure 26. Distribution of International Bandwidth by Country and Partner Region (2015-16)



Source: *Frontier analysis of Telegeography data*

Note: *Figures are International Bandwidth, which measure capacity for—not actual—data flows*

Data localisation may also have impacts on the UK economy; acting as a barrier to trade in data services that increases costs and reduces investment, competition and innovation. According to one study, the economic impacts of data localisation on the EU as a whole would be a reduction in GDP of 0.4–1.1 per cent, in private investment of 3.9–5.1 per cent, and in services exports of one per cent.[10]

Data flows and emerging digital technologies

One risk to impeded data flows is reduced innovation. Emerging digital technologies – cloud computing, advanced analytics, the Internet of Things (IoT) and artificial intelligence (AI) – hold significant economic potential. They also require vast quantities of data – along with seamless links of distributed computing, high-speed communications, and mobile and autonomous digital equipment.

Frontier partnered with Accenture to estimate the impact of the IoT and AI (separately) on economic performance for a number of advanced and emerging countries, including the UK.[11] Our models project that the IoT could raise GDP by as much as two per cent in the UK by 2030, and AI could raise annual GDP growth by as much as 50 per cent by 2035.

Our models adjust for the ability of countries to fully absorb the benefits of these technologies – accounting for stark differences between potential and realised economic benefits. Issues like free-flowing data can accelerate, or deter, this technology-driven growth. Similarly, future trade agreements must recognise the digitisation of many goods, which are becoming services, as smart, connected devices begin to blur the line between what is a 'good' and what is a 'service'.

Key takeaways

Data flows underpin a modern, services-oriented economy. It is estimated that about half of all trade-in services are enabled by digital technologies and the related data flows. The quantification of the economic impact of cross-border data flows is in its nascence, though a recent McKinsey study estimates that cross-border data flows account for 3.8 per cent of global GDP. As a relatively services-oriented economy and leading digital adopter, this likely represents a conservative estimate for the UK.

The UK is a leader in cross-border connectivity, accounting for 11.5 per cent of global cross-border data flows in 2015. By comparison, the UK accounted for 3.9 per cent of global GDP and 0.9 per cent of global population. Cross-border data flows for the UK increased 28 times between 2005 and 2015, and are expected to grow another five times through 2021. A full 75 per cent of the UK's cross-border data flows are with EU countries.

Brexit poses major risks in potentially disrupting the benefits of cross-border data flows, due primarily to new EU data protection regulations and the need for third countries to demonstrate 'adequate' compliance with those laws. The determination of third-country 'adequacy' is less than clear, and would be the purview of the European Commission to make such a decision.

Notes

1 Nicholson and McHenry, *Measuring the Value of Cross-Border Data Flows*, (US Department of Commerce, 2016); Nicholson, *ICT-Enabled Services Trade in the European Union* (US Economics and Statistics Administration, 2016).

2 See United Nations Conference on Trade and Development (UNCTAD), *Information Economy*, (2009); Lee-Makiyama, *Digital Trade in the US and Global Economies* (European Centre for International Political Economy (ECIPE), 2014); and Nicholson (2016) (see n 1 above).

3 van der Marel, *Disentangling the Flows of Data: Inside or Outside the Multinational Company?* (ECIPE Occasional Paper, 2015).

4 Manyika, Bughin, Lund, Nottebohm, Poulter, Jauch, and Ramaswamy, *Global flows in a digital age: How trade, finance, people, and data connect the world economy* (McKinsey Global Institute, 2014).

5 United States International Trade Commission (USITC), *Digital Trade in the US and Global Economies*, Part 2 (2014).

6 Frontier analysis of Telegeography Data and World Bank Open Data at http://data.worldbank.org accessed 8 August 2017.

7 For a summary, see *The EU General Data Protection Regulation* (Allen & Overy, 2016).

8 *Shaping up for adequacy – powering the UK data-driven growth post-Brexit* (techUK, 2017).

9 *European Data Centres Marketview*, Q2 2016 (CBRE, 2016); and *Silver Linings: The implications of BREXIT for the UK Data Centre Sector* (techUK, 2016b).

10 USITC (2014), see n 5 above; Bauer, Lee-Makiyama, van der Marel, and Verschelde, *The Costs of Data Localisation* (ECIP, 2014).

11 Purdy and Davarzani (2015); Purdy and Daugherty (2016).

UK telecoms regulation after Brexit: some potential new directions?

Matt Hunt
AlixPartners UK, London
mhunt@alixpartners.com

Neil Pratt
AlixPartners UK, London
npratt@alixpartners.com

Depending on the model that is adopted for future relations between the European Union and the United Kingdom, Brexit may allow telecommunications regulation in the UK to diverge from that in the EU. Assuming Ofcom can determine its own policies independent of the EU and can influence the UK government on the shape of the telecommunications regulatory framework in the UK, we believe that it is nonetheless likely to prefer a gradualist approach to change. This is partly as Ofcom has played an influential role in shaping the current EU regime, but also given its recognition of the importance of regulatory stability and certainty to encouraging investment. However, over a longer period, there is potential for a progressive divergence in key areas of regulation as the UK adapts regulatory decisions to its particular circumstances and policy goals. Based on Ofcom's stated views, the areas where it is more likely to take a different policy approach from the EU include: a more flexible approach to market reviews; regulation of non-collusive oligopolies; structural separation powers; fewer exemptions from access regulation; and a more flexible interpretation of net neutrality.

On 29 March 2017, the United Kingdom government started the formal process for terminating the UK's membership of the EU. This article considers some of the potential implications of Brexit for the future development of telecommunications regulation in the UK. We highlight the potential for regulation in the UK to diverge from the EU in the key areas of network access regulation and net neutrality.[1]

The impact of Brexit will depend to a significant extent on the model that is adopted for future relations between the EU and the UK. The UK government has stated that it does not seek membership of the single market, but aims to negotiate a new trade agreement with the EU before the UK is expected to leave the EU in March 2019 (potentially with a phased implementation). For the purpose of this article, we therefore assume that, after Brexit, the UK will be outside the single market, and that some form of free trade agreement will be in place with the EU.

Access regulation post-Brexit

Brexit is not likely to result in immediate major changes in access regulation. In part, this is because the set of Directives that comprise the EU Regulatory Framework for Electronic Communications ('the Framework') are generally already transposed into UK law and will therefore continue to apply. There are also a number of important EU regulations and recommendations that are directly applicable to the telecoms sector. These include the roaming regulation,[2] the net neutrality regulation[3] and the recommendation on non-discrimination and costing methodologies for network access.[4] The UK government has stated that it intends to safeguard such measures in UK law after Brexit to ensure that they continue to apply after Brexit.[5]

The UK Parliament could modify the UK regulatory regime after Brexit through national legislation (for example, to give Ofcom further powers or additional duties). However, it should be noted that this is likely to be subject to the nature and content of any free trade agreement that is negotiated with the EU that includes the communications sector, in particular any requirements on the UK to keep its laws harmonised with EU law.

A further important factor to consider is that the Commission is currently consulting on its proposal for a new European Electronic Communications Code (EECC) that will replace the existing Directives of the Framework.[6] The proposed EECC contains a number of important changes to network

access regulation that are intended to ensure that the Framework is fit for purpose and provides support for the large-scale fibre investment that is called for in the Commission's Digital Single Market strategy. The EECC is expected to be enacted in EU law in early 2018. It is unclear whether the UK Parliament will seek to transpose this into UK law, either prior to Brexit or through the Repeal Bill process.

From the perspective of regulatory policy, Ofcom is likely to err on the side of caution and prefer a gradualist approach to regulatory change. In part, this is because Ofcom has played an influential role in helping to shape the access regulation regime in the EU in line with its own approach and hence is unlikely to want to carry out wholesale reforms to the existing regime, not least because it is seen to have performed reasonably well in terms of outcomes. In addition, Ofcom is well aware of the importance of regulatory stability and certainty to encourage investment in fibre networks, which is one of the key objectives in Ofcom's recent Digital Communications Review.[7]

There is, however, the potential for a progressive divergence between access regulation in the UK and EU after Brexit if Ofcom is no longer required to follow the harmonised approach that it prescribed in the Framework after Brexit. This would enable Ofcom to take decisions in future market reviews that are adapted to suit the particular circumstances and policy goals of the UK, should it choose. For the remainder of this article, we assume that Ofcom does have the freedom to do this after Brexit and highlight a number of areas that may be affected.

While it is not possible to predict exactly how UK regulation will develop after Brexit, Ofcom's published documents (most notably relating to the Digital Communication Review, and Ofcom's consultation response to the European Commission's review of the Framework) suggest a number of areas where Ofcom may wish to diverge from the EU Framework.[8]

A more flexible approach to market reviews?

The EU Framework requires national regulatory authorities (NRAs) to review each of the five wholesale markets that appear on the Commission's list of recommended markets every three years. In its response to the Commission's consultation for the Framework Review, Ofcom called for NRAs to be given greater flexibility in determining the frequency of market reviews, depending on the characteristics of the relevant market.[9] The Commission has proposed to increase the minimum review period to five years in the EECC, but has otherwise retained the existing approach.

After Brexit, Ofcom may have the freedom to adopt a more flexible approach to market reviews. For example, it could choose to move to a system whereby formal market reviews are triggered by a material change in competitive conditions or where market participants petition for a change, rather than by a fixed timetable.[10] In principle, this would potentially avoid the need to carry out unnecessary reviews in circumstances where market conditions are fundamentally unchanged since the previous review, and hence the existing regulatory remedies (if any), remain appropriate. In practice, however, the pace of technological change in many communications markets may be such that Ofcom wishes to carry out a market review at least every five years. Moreover, Ofcom's current approach to charge controls is based on a control period of known duration (currently three years), and it is unclear how this would work if the length of the control period is uncertain.

Ofcom may also have greater flexibility to determine which markets to review after Brexit. In particular, Ofcom may no longer be required to carry out a market review for each of the Commission's recommended markets, and could also look at other markets without having to satisfy the '3 criteria test' set out in the Framework. This could, for example, potentially allow Ofcom to focus its market analysis on a broad infrastructure market that comprises services that support both broadband and leased lines, with remedies that allow communications providers to exploit economies of scale and scope across the full range of business and residential markets.

Finally, the Commission has proposed in the EECC to remove NRAs' *ex ante* powers to regulate retail markets.[11] This is unlikely to be welcomed by Ofcom, who are likely as a matter of principle to want to have the flexibility to deal with situations where wholesale regulation is insufficient to ensure effective retail competition. Indeed, this situation has arisen recently in the UK, where

Ofcom has proposed to regulate significant market power (SMP) in the standalone fixed voice services markets in the light of concerns about weak retail competition.

Ofcom may seek enhanced powers to regulate oligopoly markets

Ofcom has called for regulators to be given additional powers to deal with market power concerns in concentrated 'oligopoly' markets where there is no single firm dominance.[12] Ofcom's concern is that oligopoly markets with two or three large players are likely to become more common in future in both fixed and mobile markets, and it considers that the Framework does not give NRAs the tools to deal effectively with competition problems that might arise in this type of market structure.

The Body of European Regulators for Electronic Communications (BEREC) shares this concern, and has proposed that the EECC should give NRAs new powers to impose access remedies in markets where two or more firms have unilateral market power (UMP) – so called 'non-collusive' oligopolies.[13] The concept of UMP is that two or more firms in an oligopoly each have a degree of market power that it can profitably exploit unilaterally (eg, by raising access prices), without any tacit coordination with rivals. Ofcom and the BEREC appear to be concerned that the aggregate effect of the exercise of this unilateral market power by each firm may be sufficient to undermine effective competition. As the exercise of UMP does not rely on tacit collusion, it is unclear whether NRAs can use a finding of joint SMP as a basis for imposing *ex ante* regulation.

The BEREC has proposed two alternative options that are designed to ensure that NRAs have clear powers to deal with non-competitive oligopolies in future. The first suggestion is to broaden the scope of the SMP concept to explicitly include two or more holders of UMP. The second suggestion is to introduce UMP as an additional concept alongside SMP that could also allow NRAs to impose *ex ante* regulation.

The Commission will need to take these suggestions into account in finalising the EECC. However, there are concerns that powers to regulate oligopoly markets would represent a significant departure from the competition law framework that underpins the Framework, and also that it could result in perpetual regulation, given the tendency of fixed markets to evolve towards a duopoly structure. At this stage, it is therefore not at all certain that the EECC will give NRAs enhanced powers to regulate oligopolies.

Ofcom will be able to seek changes to the UK regulatory regime that would allow it to regulate non-collusive oligopoly markets after Brexit. This would, however, require a change in the UK Communications Act by the UK Parliament. Ofcom would therefore need to persuade the government that this is a priority area for legislation. In addition, there are likely to be concerns about how such a change would fit into the overall competition law framework in the UK, given that the UK Enterprise Act already provides broad powers for the Competition and Markets Authority to investigate competition problems in oligopoly markets, by means of so-called market investigations, under the Enterprise Act 2002.

Finally, as noted above, there are likely to be concerns that enhanced powers to regulate oligopolies could potentially result in an inappropriate extension of regulation that might chill competition and investment. These concerns have particular force since economics does not give any clear guidelines for where to draw the line between competitive and non-competitive oligopoly markets. Without this, there is a risk of a lack of regulatory predictability, and also the potential for regulatory overreach – both of which are likely to undermine investment in fibre networks.

Strengthened structural separation powers?

Ofcom identified a number of concerns in its Digital Communications Review relating to the independence of BT's access division, Openreach, which were undermining the effectiveness of non-discrimination regulation in various ways. After a lengthy period of negotiation, BT agreed to make a number of voluntary organisational and process changes to enhance the effectiveness of the functional separation regime that was established in the UK in 2002. Ofcom has indicated that it will monitor the effectiveness of these changes, and stated that it may consider requiring the full structural separation of Openreach from BT in future, should concerns about discrimination continue.[14]

In this regard, Ofcom has stated that it can use Article 8(3) of the Access Directive to impose structural separation on BT if other SMP remedies are insufficient (subject

to the Commission's approval).[15] This power has been transposed into the UK Communications Act 2003, and hence Ofcom will continue to be able to pursue this course of action after Brexit if it wishes, presumably without needing to seek the Commission's approval.

It will remain the case, however, that any attempt by Ofcom to rely on Article 8(3) powers would need to survive appeal to the Competition Appeal Tribunal. This would likely be a hotly contested and controversial issue given the significance of mandatory structural separation to BT, and the lack of relevant precedent relating to the use of Article 8(3) by NRAs to impose structural separation. Ofcom may therefore seek legislative change to clarify, or possibly strengthen, its powers to impose structural separation under UK law.

Ofcom is unlikely to adopt some of the restrictions in the EECC

The proposed EECC includes a number of modifications to the Framework that will constrain the application of access regulation by NRAs in future. This includes provisions that limit NRAs' powers to regulate wholesale only undertakings; prevent NRAs from imposing SMP remedies where co-investment offers meet certain criteria; and narrow existing NRA powers to impose symmetric access.[16]

The BEREC has expressed its concerns that these provisions in the EECC require the removal of, or forbearance from, access regulation based on rigid assumptions defined in the code rather than robust economic analysis based on national market circumstances.[17] It is unclear whether or how the Commission will reflect these concerns in the final EECC. In any event, we would not expect Ofcom to follow this type of prescriptive approach. Indeed, Ofcom stressed the need for NRAs to have a broad regulatory toolkit that can be used flexibly in response to market circumstances in its response to the Framework Review consultation.[18] Given this philosophy, Ofcom will be averse to giving any kind of unconditional regulatory forbearance to wholesale only undertakings or co-investments. It is much more likely to consider each case on the merits, based on the market circumstances and policy considerations in the UK.

Net neutrality regulation after Brexit

As explained above, the application of the net neutrality regulation in the UK after Brexit will depend on whether it is transposed into UK law in the Repeal Bill, and also on the extent to which any free trade agreement requires harmonisation between UK and EU laws. This is a matter of uncertainty at present, and it is possible that Ofcom will have greater flexibility than other NRAs in the way in which it seeks to enforce the principle of net neutrality, and this could have important implications for consumers, internet service providers and content providers in the UK.

This could arise, for example, if Ofcom has the scope to depart from a strict application of the BEREC's net neutrality guidelines without infringing EU law. Among other things, these guidelines impose a number of specific requirements that NRAs must consider when assessing the compatibility of paid prioritisation deals and zero-rating offers with net neutrality.[19] It is possible that Ofcom may be able to take a more permissive approach to such commercial offers after Brexit than would otherwise be the case.

This could be an important consideration in the context of incentivising the development of 5G services in the UK. 5G is likely to require very substantial network investment. It will, therefore, be important that the regulatory regime provides operators with enough commercial freedom to recover the investment cost and earn a rate of return commensurate with the risks involved in deploying new networks, while also sharing risks with other players in the value chain that are better placed to bear them.[20]

Conclusion

Depending on the model that is adopted for future relations between the EU and the UK, Brexit may allow telecommunications regulation in the UK to diverge from that in the EU. Assuming Ofcom can determine its own policies independent of the EU and can influence the UK government on the shape of the telecommunications regulatory framework in the UK, we believe that it is nonetheless likely to prefer a gradualist approach to change. This is partly as Ofcom has played an influential role in shaping the current EU regime, but also given its recognition of the importance of regulatory stability and certainty to encouraging investment. However, over a longer period,

there is potential for a progressive divergence in key areas of regulation as the UK adapts regulatory decisions to its particular circumstances and policy goals. Based on Ofcom's stated views, the areas where it is more likely to take a different policy approach from the EU include: a more flexible approach to market reviews; regulation of non-collusive oligopolies; structural separation powers; fewer exemptions from access regulation; and a more flexible interpretation of net neutrality.

Notes

1 The authors would like to thank Richard Eccles of Bird & Bird for helpful input regarding the legal implications of Brexit.
2 Regulation EU 531/2012.
3 Regulation EU 2120/2015.
4 Regulation EU 2013/466.
5 Whether EU Regulations will enter onto the UK statute books will depend on the Repeal Bill which the UK government has committed to in the Queen's Speech of 21 June 2017. The Repeal Bill will remove the European Communities Act 1972 from UK law while passing large parts of EU law into UK law to keep them in force following the UK's exit from the EU. Directives that are in force at the date of a UK exit but which have not been transposed into UK law, because the deadline for doing so has not been reached, would cease to apply after Brexit, unless included in the planned Repeal Bill.
6 Com/2016/0590.
7 Ofcom (July 2016): *Initial conclusions from the Strategic Review of Digital Communications.*
8 Ofcom (2015): *Response to Commission public consultation on the review of the regulatory framework.*
9 *Ibid*, p 3.
10 Such provisions exist in other countries. For example, in Singapore, licensed operators, which are classified as dominant or non-dominant, can petition the regulator for re-classification of the status of themselves or of other licensed operators.
11 The Commission is proposing to delete Article 17 of the Universal Service Directive in the EECC. This will remove NRAs' powers to impose regulatory obligations on undertakings with SMP on a retail market.
12 See p 2 of Ofcom's response to the Framework Review consultation.
13 BEREC (May 2017): *Berec views on non-competitive oligopolies in the Electronic Communications 2017.*
14 Ofcom (2017). Delivering a more independent Openreach.
15 This is set out in Sharon White's letter of 28 November 2016 informing the Commission of Ofcom's intention to impose an exceptional remedy on BT to require the legal separation of Openreach using Article 8(3) of the Access Directive.
16 See Articles 77, 74 and 59 of the EECC.
17 These concerns are set out in a number of papers published by BEREC in May 2017 in which it provides its views on the proposed EECC.
18 See page 2 of Ofcom's response to the Framework Review consultation.
19 BEREC guidelines on the implementation by National Regulators of European Net Neutrality Regulations. BoR (16) 94.
20 For example, it is frequently stated that autonomous cars may be a key service that will rely on 5G. Whether or not this is accurate, it provides a useful illustration of this point. If auto manufacturers are best placed to assess the latent demand for autonomous cars, and the value of these to consumers, they may wish to pay mobile operators for guaranteed access to 5G networks. Such payments might enable the widespread roll out of 5G networks, however, they appear likely to be banned under BEREC's guidelines for implementing the EC's net neutrality regulation.

Blanca Escribano
IBA Communications Law Committee Secretary; CMS Spain, Madrid
blanca.escribano@cms-asl.com

Digital health: legal challenges in the European Union

Digitalisation and the fourth industrial revolution is especially impacting the health ecosystem. Technologies like the Internet of Things (sensors), virtual reality, 3D printing, robots, machine learning algorithms, mobile communications, web portals, social media, big data analytics and patient engagement platforms are shaping a new reality called digital health, e-health or m-health, depending on the level of technology support. Tech companies are entering the health ecosystem and in the very near future, most drugs will have both a chemical and digital component. That is why the industry is identifying data as 'the new drug'.

Legal challenges like access, ownership, portability and free movement of data are being tackled at European Union level and addressed here.

Market and trends

We are currently seeing the tip of the digitalisation process iceberg, starting what some people call 'the fourth industrial revolution'. The digitalisation of the economy means that industrial sectors are not only implementing new technologies in their processes but transforming the entire value chain. Traditional industries like the automotive, pharmaceutical and utilities sectors are being accessed by tech giants that are becoming new players and challenging the status quo. Digital innovations (especially information and communication technologies and data analytics) are converging with the elements and decision-making structures of traditional value chains.

However, the digitalisation process in which every industry is currently immersed is especially affecting the health ecosystem. Healthcare providers are seeing these technological changes as an opportunity to reduce costs and achieve better patient outcomes. Payers (as national health systems) or insurers are obviously interested in implementing these new technologies to reduce some of the fixed infrastructure costs that are necessary to provide onsite attention and increase the effectiveness of drugs by monitoring how they are consumed and their outcomes on the different groups of patients. In addition to the improvements that it may have in developed markets, where this can have a disruptive effect, is in undeveloped countries where not everyone has access to medicine. Digital health could mean the extension of the scope of reach of medicine and access to medicine to groups of people that were excluded from health services or had them available, but in very precarious conditions.

Web portals and telemedicine[1] are enabling direct channels of communication between manufacturers and patients to help understand usage habits, support the exchange of results in medical trials, save costs, increase revenues and, mostly, improve relationships with doctors and enable remote diagnosis (e-health).

With the proliferation of smart handsets, apps that help patients in achieving the best use of pharmaceutical products and treatments are improving outcomes (m-health).[2]

Nevertheless, it will be the industrial Internet of Things (IoT) that will take healthcare to the next level. The use of wearables, body sensors and the most disruptive development, the so-called 'chip in a pill',[3] will make this industry a truly 4.0 one, boosting the full digital health value chain.

The most important way technology is improving and will improve the healthcare industry by making it more predictive is by using more and more precise and sophisticated data. The gathering of – even inside body – data and the use of complex big data analytics (ie, the IBM Watson Health platform) is putting the health industry at a different level. Machine learning backend

means the more data that is fed into the system, the better our understanding will be of which therapies are effective on, for instance, mutations of cancer.

It is being said that, really, what can conquer cancer is data .[4] However, for data-driven medicine and before algorithms, machine learning and big data can be leveraged, it is necessary to connect and pool data in, at least (if not single), interoperable systems, as well as the sharing of information and free flow of data. The idea of collective and non-proprietary clouds, or at least interoperable and interconnected databases for the exchange of (anonymised) health data, is something that could boost research and treatment therapies.

In the very near future, most drugs will have both a chemical and digital component, as every pill will have an accompanying mobile app that collects patient-specific data. We are entering an era in which data will be as important as the drug itself in the therapeutic management of the patient. Unlike traditional passive therapies, the data will enable therapeutic recommendations that are tailored to the individual and actionable. Hence, data is the new drug, as widely acclaimed in this sector.

New business models are being developed to 'beyond the pill'[5] models. Companies are evolving from the sole sale of drugs to the provision of services: pharma as a service in order to embrace a more personalised approach that incorporates acquiring mobile data, medical devices, health IT, big data and the Internet of Everything.

Under this new reality, healthcare companies are facing new competitors from the tech industry. Tech giants such as Google, Apple, Qualcomm and Microsoft are investing heavily in HealthTech. For instance, and as an interesting example of what tech can do for healthcare, in 2015, Google filed a patent application with the World Intellectual Property Organization (WIPO) for a wrist-worn device that could destroy cancer cells in the blood. The patent application, which has the name 'Nanoparticle Phoresis', describes a wearable device that 'can automatically modify or destroy one or more targets in the blood that have an adverse effect on health'. As result of this evolution, partnerships between life sciences companies and tech giants are increasing, combining expertise to bring innovative therapies to the market.

Finally, and from a patient point of view, it is not just physicians making judgments, but patients who are empowered with their own data and who control, own and manage it to make their health decisions. Patient empowerment is boosted by tools like data portability.

Legal challenges and the European Union approach

The European Commission is determined to achieve a Digital Single Market that will replicate the physical single market in the digital ecosystem. The final purpose is 'to achieve an inclusive digital society which benefits from the digital single market: building smarter cities, improving access to e-government, e-health services and digital skills will enable a truly digital European society'.

Starting from the eHealth action plans, the first launched back in 2004 and the second in 2011,[6] European regulators have tackled the legal issues that arise from the provision of health services by digital channels.

Having set the scene, now for a few words on the regulatory and legal challenges. The healthcare sector is highly regulated, regardless of whether operating in the physical field or using digital channels. European regulators have been tackling the legal challenges since the aforementioned eHealth plans were published. To name a few instruments, the Art29WP Opinion on the processing of personal data relating to health in electronic health records (2007),[7] the mHealth Green Paper (2014)[8] and the Staff Working Document on the existing EU legal framework applicable to lifestyle and well-being apps,[9] the EDPS Opinion on mHealth (2015)[10] and the Code of conduct for mHealth apps (2016).[11]

In addition, there are some other non-sector specific opinions and regulations that apply because of the use of digital means, for instance, the Art29WP Opinions on apps on smart devices (2013)[12] and on the IoT (2014),[13] and the ePrivacy Directive, which is currently under review in the form of a Regulation.[14]

Some of the main legal issues that must be considered when dealing with digital health products or services are: (i) whether the app or the software qualifies as a medical device and therefore is subject to the sector-specific strict obligations;[15] (ii) whether it is a lifestyle and wellness or purely a health product or service;[16] (iii) security; (iv) liability across the complex value chain[17] for any damages

resulting from a (software, connectivity, machine) fault in a connecting device;[18] and (v) interoperability and standards.

However, as described above, what is disrupting the health sector is what technology is doing to provide access to patients' data (machine-generated or not) and how treatments interact with them.

When data relates to identifiable individuals and has not been made fully anonymous, it is personal data. In the EU, personal data is regulated by the General Data Protection Regulation (GDPR),[19] a horizontal legislation that applies to all sectors, and the ePrivacy Directive that concerns the confidentiality of electronic (including Over the Top) services (*lex specialis*) and which aims to ensure a high level of protection in full coherence with the GDPR. Health data[20] is treated by the GDPR as a 'special category' of personal data which is considered to be sensitive by nature. Processing is prohibited unless exceptions apply, such as the provision of the individual's explicit consent; it is necessary for achieving purposes in the public interest, for scientific or historical research purposes or statistical purposes; or where Member States have inserted further conditions or limitations. Both the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including pseudonymisation and the encryption of personal data. In summary, health data must comply with higher protection and security standards.

When data is non-personal (or has been anonymised), GDPR and ePrivacy do not apply. The European Commission, with the purpose of achieving a true single digital market, has published the 'Building a European Data Economy Communication'[21] which intends to tackle restrictions on the free movement of data for reasons other than protecting personal data and in order to enable the market players to extract value from all kinds of data by creating a variety of applications, including remote healthcare.[22]

The issue of access to machine-generated data is under consideration in several sectors including healthcare. In some circumstances, producers of raw machine-generated data are protected by the Data Base Directive,[23] also under review at present, and the Trade Secrets Protection Directive.[24] Data ownership across the value chain and voluntary data sharing is something that the different parties involved should regulate in their commercial agreements to fill the gaps in the regulatory framework.

Data portability is a key issue in the data economy, whether it is personal or not. It means that consumers and businesses can easily take their data from one system to another to reduce the switching costs and entry barriers. In the digital health sector, the common use of this right is widely expected. While GDPR introduces the right to personal data portability for data subjects and service providers, there is no legal obligation to port non-personal data (ie, by cloud hosting providers). Consequently, the European Commission is considering developing standard contract terms requiring service providers to implement portability and extending those rights to non-personal data, in particular to cover business to business contexts.

Data portability is closely related to interoperability and technical standards. The EU Commission is also considering launching sector-specific experiments on standards involving industry, technical community and public authorities.

Finally, security in the healthcare industry is critical and, as such, there are different mandatory security obligations in a diverse legal framework. Not only do the GDPR security obligations apply, but also the critical infrastructures[25] and security of network and information systems regulations.[26] Ransomware attacks to hospitals, both in Los Angeles in February 2016 and more recently in the UK in May 2017, evidence the risks that this sector is facing.

To conclude, it would not be an overstatement to say that the application of next generation technology and the entry of tech players into the health market will mean a change of paradigm comparable to that which penicillin entailed a century ago. No doubt, healthtech will benefit the full ecosystem, patients and also stakeholders as the market will significantly grow and there will be more services demanded across the value chain. Blockchain technologies for granting better security and control of data needs may play an important role as the market evolves, but this is another story for another time.

Notes

1 Telemedicine services: interaction between doctors and patients through electronic media.

2 According to the European Commission, mHealth is a sub-segment of eHealth and covers medical and public health practice supported by mobile devices. It especially includes the use of mobile communication devices for health and well-being services and information purposes, as well as mobile health applications.

3 Consumption captures health status, including drug effects on key organs, and sends to a wearable device. The data is then sent as a report over the cloud for diagnosis.
4 Peter Piot, *Wired Health* 2017.
5 Michelle Longmire MD, a Stanford-trained physician-entrepreneur and Chief Executive Officer of Medable.
6 One of the instruments on which the Commission is relying on is the eHealth second action plan 2012–2020 (Brussels, 6.12.2012 COM(2012) 736 final Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions eHealth action plan 2012–2020 – innovative healthcare for the 21st Century), and the Accompanying document Commission Staff Working document on the applicability of the existing EU legal framework to telemedicine services (Brussels, 6.12.2012 SWD(2012) 414 final).
7 'Article 29 Data Protection Working Party', Working Document on the processing of personal data relating to health in electronic health records (HER).
8 Green Paper on mobile Health ('mHealth') SWD (2014) 135 final (Brussels 10.04.2014 Com(2014) 219 final).
9 Commission Staff Working Document on the existing EU legal framework applicable to lifestyle and wellbeing apps – Accompanying the document Green Paper on Mobile Health ('mHealth') COM(2014) 219 final (Brussels, 10.4.2014 – SWD(2014) 135 final).
10 European Data Protection Supervisor Opinion 1/2015 Mobile Health 'Reconciling technological innovation with data protection', 21 May 2015.
11 The Code of Conduct on privacy for mobile health apps was formally submitted for comments to the Article 29 Data Protection Working Party in June 2016. Once approved by this independent EU advisory group, the Code will be applied in practice: app developers will be able to voluntarily commit to follow its rules, which are based on EU data protection legislation.
12 Article 29 Data Protection Working Party Opinion 02/2013 on apps on smart devices, adopted on 27 February 2013 (00461/13/EN – WP 202).
13 Article 29 Data Protection Working Party Opinion 8/2014 on the on Recent Developments on the Internet of Things, adopted on 16 September 2014 (14/EN - WP 223).
14 Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (Brussels, 10.1.2017 COM (2017) 10 final 2017/0003 (COD)).
15 Guidelines on the qualification and classification of standalone software used in healthcare within the regulatory framework of medical devices. Ref Ares (2016) 3473012 – 15/07/2016. Qualification criteria as a medical device are the following: is it a standalone software or an accessory to the medical device?; does the software perform an action on data?; is it designed to monitor individual patient's data?; and is it designed to be used as a health product?
16 This distinction is not always easy but is important because the Consumer Directive applies to lifestyle and wellness products but not to health ones, which are excluded from the scope thereof and regulated by sector specific rules.
17 Complex interdependencies between different layers as, for instance and at least, the connectivity provider and the internet service provider, the healthcare practitioner, device manufacturer and distributor, app distributor, app developer, the patient/user.
18 The EU Commission has launched a broad evaluation of the Products Liability Directive to assess its overall functioning and whether its rules need to be adapted to emerging technologies such as the IoT and autonomous connected systems. Intermediary liability rules (app store and marketplace as hosting service providers?) must also be considered.
19 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).
20 'Data concerning health' is defined for the first time under EU Data protection law as 'personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about his or her health status'.
21 'Building a European Data Economy' (Brussels 10.1.2017 COM (2017) 9 final). Commission Staff Working Document on the free flow of data and emerging issues of the European data economy – Accompanying document Communication 'Building a European Data Economy' (Brussels, 10.1.2017 – SWD(2017) 2 final).
22 By the end of 2017, the Commission will present an initiative to abolish unnecessary barriers on where data is located.
23 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.
24 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, to be transposed into national law by June 2018.
25 Council 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; Commission Staff Working Document on the review of the European Programme for Critical Infrastructure Protection (EPCIP) (Brussels, 22.6.2012 - SWD(2012) 190 final); Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection 'Making European Critical Infrastructures more secure' (Brussels, 28.8.2013 – SWD(2013) 318 final).
26 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Jana Pattynova
IBA Communications Law Committee Newsletter Officer; Pierstone, Prague
jana.pattynova@pierstone.com

Regulatory approaches to encryption in Europe: To encrypt or not to encrypt (and what about backdoors)?

This article provides a short overview of the current European Union's struggle with balancing privacy and security when it comes to end-to-end encryption and backdoors to such encryption.

The European Union is considering banning the so-called 'backdoors' that allow the reading of encrypted messaging in communication platforms using the end-to-end encryption (E2EE) such as Signal or WhatsApp. End-to-end encryption prevents unauthorised access but also lawful interception of private messages by, for instance, law enforcement authorities.

The EU draft proposal for a new regulation on Privacy and Electronic Communications (the 'E-Privacy Regulation') released on 9 June 2017 by the European Parliament's Committee on Civil Liberties, Justice, and Home Affairs recommends end-to-end encryption and categorically rules out any backdoors.

The key provision strongly recommending end-to-end encryption and banning backdoors is contained in Article 17, para 1(a) of the draft proposal newly added by the Parliament's Committee to the Commission's original draft released in January 2017:

> 'The providers of electronic communications services shall ensure that there is sufficient protection in place against unauthorised access or alterations to the electronic communications data, and that the confidentiality and safety of the transmission are also guaranteed by the nature of the means of transmission used or by state-of-the-art end-to-end encryption of the electronic communications data. Furthermore, when encryption of electronic communications data is used, decryption, reverse engineering or monitoring of such communications shall be prohibited. Member States shall not impose any obligations on electronic communications service providers that would result in the weakening of the security and encryption of their networks and services.'

This builds on Article 7 of the EU's Charter of Fundamental Rights which provides that EU citizens have a right to personal privacy, as well as privacy in their family life and at home.

When releasing the proposal for the E-Privacy Regulation, the European Parliament's Committee on Civil Liberties, Justice, and Home Affairs stressed that: 'the principle of confidentiality should apply to current and future means of communication, including calls, internet access, instant messaging applications, email, internet phone calls and messaging provided through social media'.

The European Commission aims to have the proposed ePrivacy Regulation come into force on the same date as the General Data Protection Regulation (GDPR), which is 25 May 2018. However, the proposal must first be reviewed and debated by the European Parliament and the Council.

The United Kingdom, on the other hand, advocates for a completely opposite approach, namely imposing mandatory backdoors for lawful interception on any end-to-end encrypted communication, arguing an overriding public safety and security interest. This is much closer to the United States' approach to balancing privacy and security.

The opponents of this approach argue that designing exceptional access into today's information services and applications will give rise to a range of critical security risks. According to these

views, major efforts that the industry is making to improve security will be undermined and reversed. Providing access over any period of time to thousands of law enforcement agencies will increase the risk that intruders will hijack the exceptional access mechanisms.

Unless the EU or the UK reconsider their current approach, mainland Europe and the UK may take very different paths in reconciling privacy and security after Brexit. This would probably not contribute to the overall security of the continent.

Record fine imposed by the Hungarian Competition Authority due to misleading mobile internet advertisements

Zoltán Marosi
Oppenheim Legal, Budapest
zoltan.marosi@oppenheimlegal.com

Lia Scheuer-Szabó
Oppenheim Legal, Budapest
lia.szabo@oppenheimlegal.com

In January 2017, the Hungarian Competition Authority imposed the highest ever fine for misleading advertisements in its practice. The case, Vj-104/2015 (Magyar Telekom)*, concerned the advertisement of Magyar Telekom promoting its 4G mobile network as 'the largest 4G network' in Hungary. The GVH found that: (i) the statement failed to comply with the requirement of verifiability (as the maps showing the network coverage of the Hungarian market players were not capable of serving as a precise basis for verification); and that (ii) the statement cannot, by its very nature, comply with the requirement of objectiveness as, due to the dynamic development of 4G networks, such status cannot be guaranteed for the entire (one- or two-year) consumer contract period.*

In January 2017, the Hungarian Competition Authority (GVH) imposed the highest ever fine in its case law for misleading advertisements on the Hungarian subsidiary of Deutsche Telekom (Magyar Telekom). The case concerned comparative advertisements by Magyar Telekom regarding its 4G mobile internet network, published between October 2014 and June 2015. In the advertisements, Telekom promoted its 4G mobile network as 'the largest 4G network' in Hungary.

The GVH found that the above campaign failed to comply with the requirement of verifiability as required by European Union and Hungarian rules applicable to comparative advertising, as the maps published by Magyar Telekom, which showed the network coverage of the Hungarian market players (Magyar Telekom, Vodafone and Telenor), were not capable of serving as a precise basis for the verification of Telekom's statement in the eyes of consumers.

Further, the GVH concluded that the statement of Magyar Telekom's 4G mobile network being the 'largest' among the market players cannot, by its very nature, comply with the requirement of objectiveness as, due to the dynamic and rapid development of 4G mobile networks, such status cannot be upheld for the entire contract period. Specifically, contracts for 4G mobile internet services in Hungary are usually concluded for a period of one or two years: the GVH argued that, within this time period, network coverage (and the relative position of

market players) may change significantly. In the GVH's assessment, the lack of this information resulted in an information asymmetry, which may have distorted consumers' decision when they made their choice about their 4G mobile internet provider.

The GVH regarded the complexity and novelty of the service as well as the duration of the campaign as aggravating circumstances (the service was still unknown to consumers and the advertisements were published almost over a one-year period). The fact that the relative coverage maps in the ads were generally verifiable/correct at the time of their publication by Magyar Telekom (fully in the case of one provider and partly in the case of another) was considered as a mitigating circumstance.

According to its statements made to the press, Telekom has challenged the GVH's decision in front of the competent administrative court. A final and binding judgment may be expected in 2018/2019.

Alfonso Silva
Vice-Chair, IBA Communication Committee; Carey y Cia, Santiago
asilva@carey.cl

Raúl Mazzarella
Carey y Cia, Santiago
mazzarella@carey.cl

Analysis of the new Chilean Telecoms Regulation on multiband homologation and certification of mobile devices

As mobile devices have become an essential part of our lives, this article offers a brief explanation of the new Chilean Telecoms Regulation about the multiband homologation and certification of such devices. This new Regulation sets forth broad provisions mainly aimed to: (i) protect the consumers in the Chilean mobile device market; (ii) promote the free competition between distributors, sellers and mobile services concessionaires; and (iii) promote a sustainable technology development. Although its full impact is still unknown, this Regulation is an interesting case to be analysed and debated in order to improve the mobile device market conditions.

Introduction

Nowadays, mobile devices have become an essential part of our lives, as they interact with the world according to a new paradigm: an interconnected society. In this regard, mobile phones are the new wrist watches, the new cameras, the new agendas, the new calculators, the new mobile computers, radios and televisions and the new game consoles, all in one single device. For this reason, currently, there are more mobile devices than people worldwide and the growth of these devices is only expected to increase.[1]

Due to the importance of these devices, several regulations (or at least promotions of some sort) have been developed around the world. These regulations or promotions are generally related to device unlocking,[2] interoperability[3] and other related topics such as international roaming.[4] Other countries have been more aggressive and have created a mobile devices registration system in order to have complete control over the mobile devices of such countries.[5]

The Chilean approach

Until the year 2016, the Chilean mobile devices' business was subject to a light touch regulation; the importation, distribution and general operation of these kinds of devices were performed freely by mobile service concessionaires and local importers, distributors and sellers, complying only with

minimum regulatory requirements, mostly related to portability, maximum frequency emissions and regulatory requirements for short-range frequency devices.

However, the regulatory needs in the Chilean telecoms connectivity's structure and the entrance of new competitors in the provision of mobile connectivity services required the need to establish a regulatory framework aimed to protect free competition, consumers and sustainable technology development. In this regard, on 16 June 2016, the Chilean Undersecretary of Telecommunications ('Subtel') enacted the Exempt Resolution No 1463-2016 (the 'Technical Requirements Regulation' or TRR), which regulates the minimum technical specifications that mobile devices shall comply with, in order to be available to operate in Chilean mobile networks. This Regulation, jointly with Subtel's Exempt Resolution No 3261-2012 that regulates the Emergency Alert System (the 'EAS Regulation'), and the subsequent amendments to both Regulations, provided a new regulatory framework for mobile devices distributed and commercialised in Chile destined to the public mobile telephony and data transmission services ('devices').

The provisions of this new regulatory framework can be summarised below.

Devices' technical requirements

Any device that is going to be distributed or commercialised in Chile, either by the public mobile services concessionaires (the 'concessionaires'), manufacturers or importers, shall support at least the total frequency bands that operate over one technology, whether in 2G (850-900-1900 MHz bands), 3G (850-900-1700-1900-2100 MHz bands), 4G (700-1700-2100-2600 MHz bands) or any other implemented technology in the future. Therefore, any devices that do not comply with these minimum requirements would not be able to be distributed or commercialised in Chile. As an example, a device would be approved to be distributed or commercialised in Chile if it operates in all of the bands of 3G technology, even though it only operates in one band of the rest of the technologies.

Additionally, in order to be advertised in the country as compatible devices with any of the available technologies, devices must support the total operative bands assigned to at least one such technology. As an example, if a device is compatible with all the bands of the 3G technology, but only compatible with one single frequency band over the 4G technology, such device would not be authorised to be advertised as compatible with 4G technology.

Homologation and certification of devices

In order to assure the effectiveness of the aforementioned rule, the TRR provides that devices, in order to be distributed or commercialised in the Chilean market, must receive the approval of a certification company registered before Subtel that shall homologate the first model, granting the relevant certificate to the applicant (importer, distributor or single individual). In this regard, a successful homologation process ends with the certification of the device. Additionally, after granting such certificate, the certification company must validate each of the devices that enter into the Chilean market, in accordance with the first approved device model (if they have the same technical characteristics). In spite of this, the TRR excludes from the certification process certain types of mobile devices (eg, M2M, POS, GPS, tablets and equipment used by people affected by certain disabilities).

Sticker

Furthermore, the TRR requires that the devices, after their corresponding homologation, certification or validation, in order to be commercially distributed in the Chilean market, must bear a distinctive sticker, located in a visible spot on the front of its box, wrapping or packaging, that should identify the capabilities of such devices to operate over any of the technologies, as well as the ability of the phone to support the Emergency Alert System (EAS) according to the EAS Regulation.

Enabling of mobile networks

The TRR provides that concessionaires must only enable in their operating networks those devices that have complied with the homologation and validation procedure, except for those that are temporarily in the country (eg, devices that are operating in international roaming mode). However, the same Regulation provides that single individuals, who introduce devices into Chile for their personal use, may obtain the

approval and/or validation of such devices free of charge by a certification company, notwithstanding their personal responsibility to verify before the purchase of such device if its specifications are compatible with Chilean mobile networks.

Database

Additionally, a single and centralised database was created by the TRR. This database is aimed at having a registry of all the devices commercialised in Chile, in order to assure the compliance with the TRR. This database must register the IMEI number of every device that has been homologated and validated according to the TRR. In this regard, the database must always be checked by the concessionaires before enabling any device in their networks in order to verify if such device fully complies with the TRR.

Search system for users

The TRR sets out that concessionaires shall maintain a search engine in their website by which the users of a specific device can verify – by entering the IMEI number of such device – which are the frequency bands that support the same.

Sanctions

The TRR punishes: advertising of equipment that does not comply with the TRR; commercialisation of devices that do not comply with the TRR; non-compliance by the certification companies regarding the homologation and validation processes; misleading advertising in violation of the TRR; and the performance of conducts or measures aiming to confuse the consumers that are purchasing devices, by promoting a false perception of the device that they are buying.

Conclusion

Although it is a new Regulation, of which the ultimate effects in the telecoms market cannot be foreseen at this stage, we believe that the Chilean regulations related to multiband homologation and validation of mobile devices are already accomplishing the goal of improving the free competition, consumer rights, and sustainable technology development by means of assuring the consumer's freedom to choose the concessionaries and networks with whom they want to operate, notwithstanding the kind of device that they currently own and use. In this regard, the stickers that the devices have to bear, and the single and centralised central database that is being created according to the TRR, are a huge improvement in allowing users the free choice in the market. For this reason, in our view, this Regulation could be analysed and also applied in other countries, with similar positive results as the those obtained to date in Chile.

Notes

1 'There are officially more mobile devices than people in the world' (*Independent*, Press Release, 7 October 2014) available at www.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html accessed 8 August 2017.
2 'Cell phone unlocking' (Federal Communications Commission (FCC) promotion) available at www.fcc.gov/general/cell-phone-unlocking accessed 8 August 2017.
3 '700 MHz Interoperability' (FCC promotion) available at www.fcc.gov/document/700-mhz-interoperability accessed 8 August 2017.
4 Regulation (EU) 2015/2120.
5 Azerbaijan Mobile Devices Registration System available at www.rabita.az/en/c-projects/mdrsen accessed 8 August 2017.

Australian spectrum reform: a more flexible framework for a valuable asset

Angela Flannery
Holding Redlich, Sydney
angela.flannery@holdingredlich.com

The importance of spectrum in the communications sector and for use in the production of a wide range of services is acknowledged in Australia, as in other jurisdictions. Australia first embarked upon a process to review and reform its spectrum regulatory framework in 2014 and is currently undertaking consultation on draft legislation that is proposed to replace the existing Australian Radiocommunications Act 1992. The new regulation is expected to commence in 2019 and will provide a more flexible and streamlined structure that it is hoped will be well-suited to ongoing changing technology and demands for spectrum use.

Background: the importance of spectrum

It is trite to say that radiofrequency spectrum is essential infrastructure. In Australia, as in many other economies, it enables the production of many industrial, commercial, educational and other services (including essential services). The Australian Department of Communications and the Arts, the public sector agency responsible for providing policy advice to the Australian government in relation to spectrum management, has estimated that the economic value of spectrum to the Australian economy is approximately AUS$177bn over 15 years.[1]

The increasing importance and value of spectrum is reflected in the prices that the Australian government is able to obtain for the grant of spectrum licences. This was demonstrated by the 2017 auction of spectrum in the 700 MHz band, used for the delivery of 4G mobile services. Certain spectrum licences in that band remained unsold following a 2013 auction, given a lack of demand for the licences at the reserve price set by the government at the time of that auction. The government determined to auction those remaining licences for a reserve price reflecting the reserve price for the 2013 auction (reduced to allow for the fact that the term of the newly auctioned licences will be shorter). On 12 April 2017, the Australian government announced the results of that auction. TPG, an Australian listed telecommunications company, was the successful purchaser of a licence of 2X10 MHz of the spectrum in the 2017 auction for approximately AUS$1.26bn. That price was equivalent to a stunning AUS$2.75/MHz/pop – more than double the reserve price.

Australia's spectrum review

Use of spectrum in Australia is currently regulated by the communications sector specific regulator, the Australian Communications and Media Authority (ACMA) under the Radiocommunications Act 1992 (Cth) ('the Radcomms Act'). The Radcomms Act has not been substantially overhauled since it was first put in place. Although the current regulatory framework was considered best practice when the Radcomms Act was first enacted in 1992, technology advances and increased demands for spectrum have meant that this framework is no longer fit for purpose.

In May 2014, the then Minister for Communications, and now Australian Prime Minister, Malcolm Turnbull, announced a review of Australia's spectrum policy and management framework. That review, undertaken by the Department of Communications and the Arts and ACMA, concluded that the current framework has substantial deficiencies. The review made three core recommendations, as set out in a May 2015 report, namely:

1. The current legislation should be replaced with a simplified and outcomes-focused legislation, which facilitates timely allocations, greater flexibility in the use of spectrum (including by allowing sharing and facilitating transfers) and improved certainty.
2. The management of broadcasting spectrum, currently largely dealt with in the Broadcasting Services Act 1992 (Cth) (BSA), should be incorporated in the framework. In addition, better integration of public sector agencies should be provided for, including by requiring reporting of their spectrum holdings and allowing those agencies to lease, sell or share that spectrum.
3. Spectrum pricing arrangements should be reviewed to make these both consistent and transparent. This would support efficient use of spectrum and facilitate secondary markets.

The review supported a rewrite of the existing legislation to address these issues and also to streamline regulation, including by the adoption of a single licensing system to replace the three categories of spectrum, apparatus and class licences.

The government announced its agreement to implement the recommendations of the review in August 2015. As a next step, in early March 2016, the government released a Legislative Proposals Consultation Paper on its proposed approach to the rewrite of the legislation (but excluding consideration of pricing issues). Consistent with the review recommendations, that consultation paper noted that the approach of the new draft legislation would be to:

- simplify regulatory structures for planning, licensing and equipment regulation;
- streamline regulatory processes;
- clarify the roles of the government and ACMA, and also spectrum users;
- bring broadcasting spectrum into the general spectrum framework; and
- provide for graduated and proportionate enforcement and compliance tools.

What reforms are being considered?

In May 2017, the government took the next step in the reform process, by releasing a partial exposure draft of the new Radiocommunications Bill, together with consultation papers on broadcasting spectrum, transitional arrangements, spectrum pricing and Commonwealth held spectrum. The draft bill and consultation papers generally remain consistent with the recommendations of the review, with a focus on modernising and simplifying Australia's spectrum management framework. Key points include:

1. As expected, the draft bill provides for a move to a single licensing system. ACMA will design and implement this single licensing system. It is intended that this system will remove existing barriers to replanning spectrum, given current processes to convert and reallocate spectrum between licence types are seen as inefficient and slow. Under the proposed regime, licences can be issued in three ways, in response to written applications, where the Minister provides a direction to issue or in accordance with a licence issue scheme established by ACMA. Class licences will be replaced with a spectrum authorisation mechanism allowing particular transmitters to be used for particular purposes on specified terms.
2. The maximum term of a licence will be extended to 20 years. Licensees will have more certainty in relation to renewal, with licences required to state whether there is a right to renewal (or no right of renewal) or whether renewal is in the discretion of ACMA.
3. The Minister's role will be strategic, with the existing involvement of the Minister in many operational decisions removed. The Minister will set strategic priorities to guide ACMA in its spectrum management regulatory functions, and will have direct oversight of decisions with significant public policy implications.
4. The regime for broadcasting spectrum is currently complex, with regulation split between the Radcomms Act and the BSA. Although it will continue to be the case that the two Acts will govern the rights of broadcasters, there will be some simplification of the existing regime. This will include, for example, removing the special planning provisions that apply to broadcasting spectrum. These changes also link to a decision made by the government in early May 2017 to abolish broadcasting licence fees and to increase the fees that broadcasters pay for the use of spectrum.
5. ACMA will be required to publish an

annual five-year spectrum management work programme, with a high degree of detail included for the first 12 months of each plan. ACMA will need to undertake consultation with both the Minister and the public in respect of each plan. It is hoped this approach will improve transparency, as stakeholders will have visibility of ACMA's priorities and ACMA's proposed spectrum planning and other decision processes.

6. On pricing, the government is currently proposing that, outside the changes that have been announced for broadcasting spectrum licences, ACMA should publish guidelines on its approach to pricing, the government and ACMA should endeavour to charge users of similar spectrum the same rate, and reasons should be published if fees are determined other than by auction or an administered pricing formula.
7. It is currently proposed that a 'hybrid' approach will be adopted to transition, allowing the elements of the new regime to be implemented over a five-year period. Ultimately, ACMA will be responsible for implementing transition.

ACMA will be generally responsible for designing the new spectrum management arrangements that are provided for in the draft bill, should it become law. Therefore, its views on how it will implement the new framework are very important. Together with the draft bill and consultation papers that have been released by the government, ACMA has released additional material setting out certain of its initial views on implementation, including, for example, draft licence conditions for the new single licensing system.

Next steps

The current consultation is only one step in an ongoing process in the development of the new regulatory framework. Following consideration of stakeholder input, the government will issue another exposure draft of the Radiocommunications Bill, together with exposure drafts of associated legislation (including a Transitional and Consequential Bill), for further consultation later in the year.

Current indications are that, if possible, the Australian government will seek to introduce the new legislation during the calendar year 2017. This seems to be an ambitious timetable and it is more likely that the Australian Parliament will consider, and hopefully pass, this legislation in early 2018. There would then be a period of up to 14 months following the passing of the legislation before it takes effect. On that basis, the new regime would not commence until 2019. Allowing for the 'hybrid' approach to transition, the last provisions of the new law may not take effect until 2024.

Concluding comments

The government is fond of stating that the rewrite of the Radcomms Act is the most substantial change to Australia's spectrum management framework in over 25 years. It is a well overdue and necessary change, given the economic importance of spectrum and the need for a more flexible and responsive framework to optimise use of that valuable asset.

In the short term, spectrum is particularly important for the next stage of the evolution in mobile services, which is the roll out of 5G services. 5G is the fifth-generation wireless broadband technology and it is thought that it will provide speeds significantly faster than can be achieved with 4G LTE networks. Given the proposed timeline for the introduction of Australia's new spectrum regulatory framework, it is unfortunate that spectrum allocation for 5G mobile services will be likely to occur under the current regulatory regime.

Note

1 'The economic value of spectrum', Research Report prepared for the Department of Communications by the Centre for International Economics, January 2015.

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

Nana Adjoa Asante
Nctm, Milan
nana.asante@nctm.it

The EU and its bid to regulate digital platforms

The important role of digital platforms necessitates its discussion. As this new phenomenon becomes increasingly sophisticated, the need for laws to govern it becomes more poignant. In consequence, the European Union has taken various actions towards realising this aim of regulating the digital platform horizon. This article focuses on the debate surrounding this bold step of the EU, with particular focus on the arguments of scholars, positions of some EU member states, the position of the EU and its policy plan towards regulation of digital platforms.

Digital platforms play a key role in our day-to-day interaction; be it economic, social or political, they afford patrons the option of much smoother and simpler interaction with the rest of the world. Digital platforms as a technological innovation have injected substantial contributions into the global economy and have generated substantial legal issues resulting from their dynamism.

What is a digital platform?

The definition of digital platforms has not seen much clarity. Indeed, the EU Commission has not come to an agreement on a concise definition of digital platforms.[1] Inasmuch as definitions may be useful, it is important to consider the features attributable to digital platforms to get a fair appreciation of this important technological tool. A digital or online platform is generally considered as a two-sided or multi-sided medium where users are connected by a platform operator in order to facilitate exchange of information or resources. Significant examples are Alibaba, Amazon, eBay, Facebook and Uber.

Current EU regulation of digital platforms and the social landscape of digital platforms

Presently, within the EU, there is not a uniform legal regulatory framework specifically governing digital platforms. In principle, they are presently governed by standard and well-established EU rules relating to data protection, intellectual property, consumer protection, competition and intellectual property, etc.[2]

Within the EU, there is mutual agreement by stakeholders[3] that the advent of digital platforms, despite numerous advantages, poses myriad issues including actual/potential risks associated with unfair pricing, network effects,[4] abuse of market dominance, infringement of privacy and display of illegal content.

The seemingly overwhelming question that arises is: how do we regulate these platforms?

'To regulate or not to regulate?'

There are views that digital markets are more regulated than analogue markets. This is based on the argument that, for instance, physical cash transactions are subject to less stringent measures than online transactions,[5] thus buttressing the position that there is a need for better enforcement of existing rules within the new era of digital platforms. It is further opined[6] that the digital market offers keen competition and, in addition, the financial and reputational incentives of the market are enough to ensure responsible use of data and creation of customer value, making further legislation obsolete.

On the other hand, there is the argument to 'score platforms before regulating them'.[7] Thus, there is a need to gather factual evidence on specific concerns relating to digital platforms, which will inform the type of legislation to be adopted. Furthermore, there are suggestions for the need for specific regulation that targets evidence-based harm. This position is based on the risk of

premature intervention, which may harm the innovative character of digital markets. On the ground that digital markets are consistently birthing new business models that are not regulated, the argument is that there is need for tailored regulation for each business model.

Positions of EU member states

Germany

In March 2017, the German Federal Ministry for Economic Affairs and Energy published a white paper[8] on digital platforms. In the white paper, Germany advocates for a 'made in Europe' approach as opposed to individual regulation by member states. Dissimilar from the EU, Germany advocates for the establishment of an appropriate general regulatory framework,[9] including revision of existing competition laws to accommodate new antirust threats.

Sweden and Italy

In a joint communication,[10] Italy and Sweden express that a targeted assessment and response is more beneficial to the regulation of digital platforms. The position is in support of legislation targeted at specific regulatory lapses or legal uncertainties.

The Netherlands

The Netherlands expresses its position in a non-paper on the EU consultation.[11] The Dutch government is in favour of a tailor-made regulation to address case-by-case scenarios. The Netherlands is in support of government collaboration with platform operators to reduce the risks associated with the use of these platforms. The Netherlands also encourages the need for a clearly outlined purpose for regulations, giving member states the latitude to achieve these identified objectives in diverse ways.

United Kingdom

The UK's position is for a more flexible market that is regulated to accommodate the dynamism of the digital economy.[12] Principally, the UK, through its Competition and Marketing Authority, argues that the significant diversity of digital platforms makes it almost ineffective to have 'broad-brush' legislation or economic regulation to govern this wide spectrum.[13] The country highlights the need for targeted regulation for specific harm as opposed to premature regulation. The primary focus supported is for the enforcement of pre-existing rules governing competition as well as fundamental rights such as privacy, clear standards relating to fair pricing, data protection and consumer protection, improved free trade across borders and possible deregulation to encourage innovation and market penetration by smaller companies.

Brexit and the EU regulation on digital platforms

Digital platforms cannot be discussed without considering the issue of Brexit and its attendant consequences in light of the UK's position on EU regulation of digital platforms. The UK being anti-EU regulation of digital platforms creates a potential challenge for the UK when Brexit finally occurs; a less regulated UK digital platform market risks substantially less access to the EU market.

The EU position

In a bid to assess the role of online platforms, the EU has conducted various stakeholder consultations.[14] The outcome of the assessment gave rise to the EU's issuance of a communication on Online Platforms[15] in May 2016. This Communication, among others, identifies the need to monitor business trading practices, ensure fairness, safeguard innovation and tackle illegal content online. In the Communication, the EU highlights its decision to introduce regulations that are 'future-proof' and flexible, such as principles and guidelines on eID interoperability as well as to admonish EU wide self-regulation and co-regulation, and bolster existing EU regulations. The EU, through the Communication, stated that a targeted assessment will be made on business-to-business practices, made legislative proposals to review the Regulation on Consumer Protection Cooperation and submitted a review of the Unfair Commercial Practices Directive.[16] Additionally, a review of other existing rules such as the EU telecoms rules, ePrivacy Directive and Audio-visual Media Services Directive was forecasted. In the Communication, the EU earmarked spring 2017 as the deadline for commencement of a

majority of these initiatives.

Consequently, on 10 May 2017, the EU, in its midterm review[17] of its Digital Single Market strategy, revealed plans to introduce legislation by the end of 2017 to tackle the problem of unfair trading practices identified through impact assessment and introduce procedural frameworks designed to remove illegal content focusing on principles-based self-regulatory measures.

The EU's aim of principles-based self-regulatory measures is evidenced by recent stakeholder dialogues leading to the birth of the Memorandum of Understanding on the Sale of Counterfeit Goods over the Internet and Code of Conduct on illegal online hate speech.

Nonetheless, the EU posits that it is effectively utilising its enforcement powers regarding existing competition rules to deal with certain threats posed.[18] An example is the EU decision dated 4 May 2017,[19] which adopts commitments from Amazon not to enforce unfair clauses which mandate publishers to offer Amazon similar or better conditions offered to competitors as well as disclose alternative terms offered to Amazon's competitors.

Conclusion

From thorough assessment and stakeholder consultation by the EU, its calculated position is the introduction of new facts-based and targeted regulations combined with the reinforcement of already existing rules. This position is laudable, as it does not belong to any of the extremes of regulation or non-regulation but rather a targeted combination in order to produce effective results.

Notes

1 See www.lexology.com/library/detail.aspx?g=86673885-eb5a-443c-ab04-8a5f31c1e060 accessed 21 August 2017.
2 See www.kwm.com/en/it/knowledge/insights/online-platforms-and-eu-regulation-20160620 accessed 21 August 2017.
3 Reports of various stakeholder consultations by EU, https://ec.europa.eu/digital-single-market/en/consultations accessed 21 August 2017.
4 Situation where a good or service becomes more valuable due to increased usage.
5 See https://ecommerce.blogactiv.eu/2016/01/22/platform-regulation-new-rules-or-strengthened-existing-ones accessed 21 August 2017.
6 Joe Kennedy, 'Why Internet Platforms Don't Need Special Regulation', Information Technology and Innovation Foundation (ITIF) report, 8, available at www2.itif.org/2015-internet-platforms.pdf accessed 21 August 2017.
7 See https://medium.com/@sorianotech/how-to-regulate-internet-giants-348e44648df74.
8 See www.bmwi.de/Redaktion/EN/Publikationen/white-paper.html accessed 21 August 2017.
9 See www.insidetechmedia.com/2017/04/10/german-ministry-for-economy-publishes-a-white-paper-on-digital-platforms accessed 21 August 2017.
10 See www.government.se/opinion-pieces/2016/05/sweden-and-italy-united-for-a-more-competitive-and-digital-europe accessed 21 August 2017.
11 See https://zoek.officielebekendmakingen.nl/blg-661677.pdf accessed 21 August 2017.
12 See https://engage.number10.gov.uk/digital-single-market accessed 21 August 2017.
13 See www.gov.uk/government/speeches/alex-chisholm-speaks-about-online-platform-regulation accessed 21 August 2017.
14 See https://ec.europa.eu/digital-single-market/en/consultations accessed 21 August 2017.
15 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Online Platforms and the Digital Single Market Opportunities and Challenges for Europe (COM (2016)288).
16 *Ibid.*
17 Commission Staff Working Document Accompanying the Document Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions on The Mid-Term Review on The Implementation of The Digital Single Market Strategy a Connected Digital Single Market for All (SWD/2017/0155 final).
18 See www.europa.eu/rapid/press-release_MEMO-17-1233_en.htm accessed 21 August 2017.
19 See http://europa.eu/rapid/press-release_IP-17-1223_en.htm accessed 21 August 2017.

IBA App – additional functionality now added

– available from the App Store and the Google Play Store

The IBA App has been updated to become even more user friendly, providing you with the latest legal news, updates and content while on the move.

All new functionality is now available for the App in both the Apple Store and for the Android version in the Google Play Store.

New functionality:

- Access to IBA Digital Content – with new articles, stories and items of interest available and updated daily
- The ability to download PDFs and podcasts from the IBA Digital Content library to your mobile device

How do I access the App?

- Simply download the App (search for International Bar Association and download the IBA Members' Directory) via the Apple App Store or Google Play Store
- Login with your IBA membership user ID and password
- Search the full IBA Member Directory or update your My IBA profile

Download on the App Store

ANDROID APP ON Google play

INTERNATIONAL BAR ASSOCIATION

the global voice of the legal profession

Don't let valuable contacts pass you by, update your profile today!

INTERNATIONAL BAR ASSOCIATION

KING'S College LONDON

For more information and how to apply:

Visit www.kcl.ac.uk/executivellm

Email executivellm@kcl.ac.uk

Tel +44 (0)20 7848 5926

A unique opportunity to learn with, and from, the best

King's College London and the International Bar Association (IBA) have collaborated to offer an elite world-class professional LLM. Designed to bring together wide-ranging legal perspectives and expertise from around the world, the Executive LLM aims to confront some of today's most challenging global legal issues.

This two-year, part-time advanced Master of Laws course is for ambitious commercial, in-house or regulatory lawyers, keen to build on their achievements and develop their careers.

The Executive LLM offers a range of unique course content designed to equip you with advanced legal, commercial, and policy knowledge as well as sectoral expertise. You will also develop complementary skills that will make you a more rounded, more accomplished and more successful lawyer.