Hogan Lovells

Global Media and Communications Quarterly

Communications Law Reform

AUTUMN 2014

Contents

Editorial

This issue of the GMC Quarterly looks at the potential impact of recent and upcoming changes in telecommunications and broadcasting law in various jurisdictions, starting with the major reform taking place in Mexico. On 1 August we combined with a leading Mexican law firm Barrera, Siqueiros y Torres Landa. Federico Hernandez Arroyo leads our newly combined telecoms and media practice in Mexico City and introduces this issue with two in-depth articles on the new telecoms and broadcasting laws in Mexico, which came into force on 13 August this year. The first explores the challenges and opportunities of the new laws, concluding that the new laws should level the playing field in the industry and stimulate greater investment in Mexico. The second article summarises Mexico's introduction of strict regulation of net neutrality. We then look to Russia, where Natalia Gulyeava and Julia Gurieva of our Moscow office discuss the prohibition on advertising on Pay-TV channels (including those that originate outside Russia) that will come into force in Russia at the beginning of next year. Trey Hanbury then explains the possibility of a 'rewrite' of the US Communications Act and the impact the proposed changes to regulation would have on the industry in the United States.

We then have three articles which focus on data privacy/data protection issues in the US, EU and South Africa. Christopher Wolf, of our Washington office, describes Hogan Lovells' leading role in the efforts of the automotive industry to develop a set of self-regulatory privacy principles governing the use of data from "connected cars". Eduardo Ustaran of our London office writes about the wider implications of the Google 'right to be forgotten' case and how each and every local subsidiary of a data controller in the EU may now trigger the applicability of local data protection law. Leishen Pillay, from our new office in Johannesburg, concludes this section of the issue by talking about the introduction of data protection legislation in South Africa.

Finally, Winston Maxwell, together with Marc Bourreau, Professor of Economics at Télécom ParisTech round off this issue of the GMCQ with a detailed article on the regulatory principle of technology neutrality. They explore the meaning of technology neutrality in different contexts, the implications, particularly for regulation of emerging markets and new technologies and how the concept might play into a rewrite of the US telecommunications laws, as discussed in Trey Hanbury's article earlier in the issue. The article was first published in French in the journal of the French regulatory authority, ARCEP.

Follow updates by signing up to our three specialized blogs:

Hogan Lovells Global Media & Communications Watch:
www.hlmediacomms.com

Hogan Lovells Chronicle of Data Protection:
www.hldataprotection.com

Hogan Lovells International Spectrum Review:
www.hlspectrumreview.com

Winston Maxwell
Partner, Paris
T +33 1 5367 4847
winston.maxwell@hoganlovells.com

Trey Hanbury
Partner, Washington, D.C.
T +1 202 637 5534
trey.hanbury@hoganlovells.com

Penny Thornton
Senior Associate, London
T +44 20 7296 5665
penelope.thornton@hoganlovells.com

Mexico: The challenges of the new telecommunications and broadcasting law

The new President of Mexico Peña Nieto started work on 1 December 2012. The following day, the three main political parties executed the so-called "Pact for Mexico", which contained several commitments including the reform of the telecommunications and broadcasting sectors.

On 11 June 2013, an historic constitutional reform in telecommunications and broadcasting was published after a fast-track process of just three months. The main purpose of the reform was to enhance competition in the telecommunications and broadcasting markets and to provide for the publication of a new convergent law on or before 9 December 2013. However, the political negotiations took longer than expected and the new Federal Telecommunications and Broadcasting Law (the "Law") was enacted on 14 July 2014 and came into effect on 13 August 2014.

The Law repealed the Federal Telecommunications Law (1995) and the Federal Law of Radio and Television (1960) and introduced a new regulatory framework based on the principles and guidelines of the constitutional reform. We will highlight some of the most important features of the constitutional reform and the Law in this article.

The Federal Institute of Telecommunications (the "Institute") was created as a constitutional entity with new powers (including in economic competition matters) and institutional design, incorporating specific rules on transparency and contact with the regulated industry.

Telecommunications and broadcasting services are considered as human rights and as public services. In resolving the implementation of the must offer and must carry obligations also introduced by the reform, the Institute envoked the status of such services as human rights.

There is a new authorisation regime (excluding spectrum or orbital resources) called "unique concession" that makes the provision of all services technically feasible. A unique concession can only be granted to Mexican individuals or entities, however there is no limitation with respect to foreign investment for telecommunications services and up to 49% in broadcasting services (subject to reciprocity from the country of the ultimate investor).

Spectrum and orbital concessions are granted through a public bid. The financial amount of the bid is not the sole criterion for success. Concessionaires are allowed to lease frequency bands under certain requirements. As part of the constitutional reform, the Institute is conducting two bidding procedures in order to award: (i) two new open television channels with national coverage, and (ii) the 113.0° West and 116.8° West slots and their associated bands for the provision of fixed satellite services.

Resellers of telecommunications services require an authorisation granted by the Institute. It is expected that this will be used to boost the MVNO market in Mexico.

The Law contains a provision that public telecommunications networks with government ownership will be considered as shared networks for wholesale services only. There are two main projects under this scheme that shall be launched in the near future as public-private partnerships by the Federal Government: (i) extension of the fiber optic backbone network of the Federal Electricity Commission ("CFE"), and (ii) the installation of a wholesale network in the 700 MHz band.

The Law sets forth a new set of rights in favour of telecommunications and broadcasting users (e.g. to consult their mobile credit balance free of charge[1], free election and non-discrimination in the access of Internet services, and distinction between advertising and programming content), including specific rights for disabled users (e.g. service centers, internet pages, and customer lines will have accessibility functions and subtitle services and dubbing of Spanish and Mexican sign language for people with hearing problems).

The Law includes different obligations in security and justice matters, such as the obligation to provide to law enforcement, in real time, a geographic location of mobile devices and to store, register and provide specific information relating to communications made from any line. Such obligations have been subject to criticisms and have been already challenged.

1 According to the Institute, at the end of the 1Q of 2014, 84.7% of mobile users in Mexico are prepaid: http://www.ift.org.mx/iftweb/wp-content/uploads/2014/06/COMUNICADO-ITEL-1T2014.pdf

The Law contains two main provisions that trigger asymmetrical regulation: (i) preponderance, and (ii) dominance. The first is a new concept created by the constitutional reform and it applies to companies that hold a market share of more than 50% in the telecommunications or broadcasting sectors. The second refers to companies with substantial market power in any of the telecommunications and broadcasting markets under the Federal Competition Economic Law. On 6 March 2014, the Institute declared the following agents as "preponderant" and imposed different measures on them: (i) Telcel and Telmex in the telecommunications sector, and (ii) Televisa in the broadcasting sector. In addition, according to the Law, the Institute initiated on 11 September 2014 a process to determine the existence of dominance in both sectors, including the pay television market.

The Law contains a new set of rules to limit the cross ownership of telecommunications and broadcasting licensees and other restrictions in the acquisition of spectrum for broadcasting services, in the event that in certain market or coverage areas there is no access or limited access to diverse information.

Finally, the administrative decisions of the Institute can now be appealed only through a constitutional trial (*amparo indirecto*) and there is no injunction. Such trials will be held before the new specialised judges and courts in broadcasting, telecommunications and economic competition matters, that were incorporated as part of the constitutional reform and are expected to bring more certainty in these highly litigated areas.

Some of the changes introduced by the constitutional reform and the Law follow the recommendations of the OECD. One major step is for the Institute to act independently and according to the Law in order to give certainty to the market and to start producing effects that benefit consumers. In general terms, the Institute has achieved the aims set out in the constitutional reform and some of them have produced some important results, such as América Móvil's intention to sell part of its business in order to cease being a preponderant operator and therefore no longer subject to regulation.[2] Another example is that must offer and must carry are a reality in Mexico. However, additional rules shall be issued by the Institute to properly implement the constitutional reform and the Law.

The foregoing context will level the playing field and stimulate greater investment. European and North American investment groups have already shown interest in the Mexican market.[3]

On the other hand, the specialised judges and courts will also play an important role in duly resolving disputes in accordance with the new regulatory framework and they need to prove that they have the expertise and knowledge in doing so.

The Federal Government also needs to carry out several actions to implement large projects such as the deployment of the CFE Telecom fiber network, the 700 MHz wholesale network, a universal coverage program and the transition to Digital Terrestrial Television before the end of 2015.

The application of the constitutional reform and the Law is in its early stages and we need to wait and see the performance of all actors involved in the industry (private and public). Only time will tell if Mexico finally improves its rankings within the OECD countries, but it is in a much better position than it was before the reform. ■

With thanks to Mónica Sarralde.

Federico Hernandez Arroyo
Partner, Mexico City
T +52 55 5091 0000
federico.hernandez@hoganlovells.com

2 America Móvil press release of July 8, 2014: http://www.americamovil.com/amx/en/cm/news/2014/08072014.pdf

3 *Telecommunications Reform in Mexico: Regulation, Market Structure and Social Coverage*, p. 21, Casanueva and Bacilio, Universidad Iberoamericana, Mexico City.


BAJA
HOTEL

Mexico adopts one of the strictest net neutrality frameworks in the world

The Mexican constitutional reform in telecommunications published last year acknowledged Internet access as a human right. The recent Federal Telecommunications and Broadcasting Law (the "Law") has introduced many new concepts, such as net neutrality, which was previously unregulated in Mexico. For more information about the constitutional reform and the Law, please refer to the previous article in this issue.

Despite its existence and application years before, net neutrality regulation has recently become a hot topic worldwide and international regulators have adopted different positions. For example, the European Parliament recently tabled proposals to: (i) differentiate specialised services from Internet access services and ISPs would be able to offer the former only if network capacity is sufficient to provide the latter; (ii) narrow the concept of network management; and (iii) prohibit ISPs from blocking, slowing down, degrading or otherwise discriminating against specific content, except for network management.[1] In the United States, the Federal Communications Commission ("FCC") submitted the highly debated Open Internet Notice of Proposed Rulemaking for comments. One of the most disputed proposals of the FCC is that ISPs may undertake individualised bargaining with upstream content and service providers in some cases.[2]

The concept of net neutrality regulated by the Law applies not only to licensed operators of public telecommunications services in Mexico, but also to authorised entities that commercialise telecommunications services (both considered as "ISPs"). The law provides that ISPs shall provide Internet access services in accordance with the capacity, speed and quality contracted by users, independent of the content, origin, destiny, equipment or application used, as well as of the services provided through the Internet.

The Federal Institute of Telecommunications (the "Institute") shall issue general guidelines to further regulate net neutrality (the "Guidelines"), which must be consistent with the following principles: (i) free election; (ii) non-discrimination; (iii) privacy; (iv) transparency; (v) traffic management; (vi) quality; and (vii) sustained infrastructure development.

Free election means that Internet users should be able to access any content, application or service offered by an ISP without being limited, degraded, restricted or discriminated on its access and with the possibility of using any kind of instruments, equipment or devices able to connect to the network ("technological neutrality").

Under the non-discrimination principle, ISPs are prohibited from obstructing, interfering, inspecting, filtering or discriminating vis-à-vis any kind of content, application or service over their networks.

In addition, ISPs will have to comply with the following obligations: (i) protect privacy of users and security of the network; and (ii) publish on its websites information concerning the characteristics of the service provided, including the policies applicable to traffic management, network management authorized by the Institute, speed, quality and warranty of the services ("transparency").

The ISPs may take measures or actions necessary for "traffic management" and "network management" under the policies approved by the Institute, in order to ensure the speed or quality of the service contracted by the user, provided that the foregoing does not constitute a practice contrary to efficient competition.

Also, the ISPs should maintain the minimum "quality" standards established for that purpose in the Guidelines. Likewise, the Guidelines shall promote the sustained growth of the telecommunications infrastructure.

Failure of an ISP to comply with the Mexican net neutrality obligations against blocking, interfering, discriminating, delaying or unfairly restricting access rights of any user, will result in a fine of between 1% and up to 3% of the ISP's revenues.

Although a more detailed regulation of net neutrality will be included in the Guidelines, the Law envisages a fairly clear purpose to promote net neutrality without

1 See *European Parliament votes to strengthen net neutrality* in the Spring edition of this GMC Quarterly.

2 See *Open Internet NPRM*.

restrictions such as those discussed in other countries. Moreover, Internet access is considered as a human right and therefore net neutrality will be likely to be protected similarly. On their face, the Mexican rules on net neutrality are among the strictest in the world. They may inspire other countries or regions that are considering net neutrality legislation, including the European Union as it considers net neutrality rules under the "Connected Continent" package.

However, Mexico has not faced the problems and litigation that, for example, the United States has experienced in the past years regarding net neutrality, since it is a new concept in the regulatory framework. At some point in time, such a concept and the Guidelines may be subject to interpretation and litigation, especially as technology evolves. ■

With thanks to Rodrigo Méndez.

Federico Hernandez Arroyo
Partner, Mexico City
T +52 55 5091 0000
federico.hernandez@hoganlovells.com

Russia: Pay-TV businesses affected by changes in Russian advertising laws

On 1 January 2015 amendments to the Russian Federal law "On advertising" No 38 of 13 March 2006 will come into force. The main change is prohibition of advertisement on Pay-TV channels and/or channels that use technical decoding devices. The law does not apply to Free-TV channels.

The amendments affect all Pay-TV channels notwithstanding the country of origin. The Russian national Pay-TV channels (including those owned by the state) are equally affected.

This impending prohibition is bad news for the Russian Pay-TV sector, which does not usually make large profits even including income earned from advertising. The historically low subscription fees offered by the Russian Pay-TV sector do not quite help to set-off the forthcoming loss of advertising income.

Consequently, distributors of Pay-TV channels are forced to search for alternative solutions. Discussed solutions include more effective use of advertising time on multiplex channels (which do not fall within the restriction) and using the time between switching channels to show adverts. However these are business decisions and it is hard to predict how the market and the regulators will react.

The amendments have been widely discussed by the Russian media community. It is evident from the discussion that the amendments are not of a purely political but also of a commercial nature. With the Pay-TV sector growing and offering attractive and entertaining content, the Russian state (Free-TV) channels are unavoidably losing audiences and advertisement-based profits. The goal of the advertising prohibition is to help the state channels be competitive.

One of the effects of the prohibition may be to close the market for newer Pay-TV channels as the distributors would simply not be interested in taking channels without an established audience, particularly if they cannot sell local advertising time on those channels.

Internet TV, however, was not affected by the amendments and, therefore, may become a safe harbour for some of affected channels.

In the meantime, the Pay-TV sector is preparing for more scrutiny by the Russian regulators such as the Federal Anti-Monopoly Service (the Russian competition authority) and Roskomnadzor (the Russian state service in charge of media licensing). The potential penalties for non-compliance with the new prohibition are approximately EUR 2,000-11,000. Persistent non-compliance by a Pay-TV channel will most likely result in revocation of its licence.

There is some hope that the new prohibition may be revised in the future. For example the 2012 ban on TV advertising of beer is now being reviewed and may be amended. However, any such "come back" will require time and lobbying efforts. ■

Julia Gurieva
Associate, Moscow
T +7 (495) 9333000
julia.gurieva@hoganlovells.com

Natalia Gulyaeva
Partner, Moscow
T +7 (495) 9333000
natalia.gulyaeva@hoganlovells.com

USA: Rewriting the U.S. Communications Act for the 21st century

The primary law in the United States governing the telecommunications industry is the Communications Act of 1934 (the "Act").[1] Congress adopted the Act during the Great Depression, at a time when the latest consumer technology was broadcast radio, and last updated the law nearly twenty years ago, when most people accessed the Internet using dial-up and "smartphones" were still science fiction.[2]

The Communications Act has strained to keep up with the incredible changes in the telecommunications landscape in the last eighty years, and rumors of a "rewrite" of the Act swirl regularly in Washington D.C. Recent efforts by several House Republicans suggest that broad reform of the telecommunications law could be possible in the relatively near future. The result could be a significant restructuring of the way radio, television, mobile communications, and the Internet are regulated in the U.S.

Congress drafted the original Communications Act to consolidate already existing laws that governed telephone, radio, and telegraph communications into a single statute. This way of conceptualizing the telecommunications marketplace still defines the Act, which is divided into sections, or "Titles," that roughly correspond to specific industry silos such as broadcast, cable, or telephony.[3] One problem often mentioned by advocates for reform is that the nature of what constitutes "radio" or "common carrier" services is no longer clear-cut, and can give rise to disparate regulatory treatment of otherwise closely related new industries and services.

Against this backdrop, the Republican-led House of Representatives Energy and Commerce Committee (the "Committee") launched a review process of the Communications Act in 2013 with the ultimate goal of rewriting that statute.[4] Since January 2014 the Committee has released five "white papers" seeking public comment on issues central to telecommunications law and policy in the United States. The Committee launched its inquiry by seeking broad comment on how best to "moderniz[e] the Communications Act," including ways to change the basic structure of the Act to remove its emphasis on industry sectors that can quickly become outdated with technological shifts.[5] Since then, the questions posed by the Committee's white papers have become more targeted. The second white paper focused on spectrum policy, and asked for public comment on, among other issues, what Congress could do to maximize the efficiency of spectrum use and how it should regulate unlicensed spectrum.[6] The third white paper, released in May 2014, raised thorny issues of how the FCC should define "competition" in the modern communications marketplace, taking into account the growth in intermodal competition that some critics allege has strained the "siloed" construction of the current Act.[7] A subsequent Committee white paper asked pointed questions about the existing interconnection regime, including the challenges the IP transition poses to existing regulations.[8] The Committee's most recent white paper solicited input on the Universal Service Fund ("USF"), which collects more than $8 billion per year in fees from wireless and wireline carriers and uses it to subsidize telephone and broadband services in high-cost areas, for low-income consumers, in schools and libraries, and for rural healthcare providers, and has long been a lightning rod for reformers on both sides of the aisle.[9]

Although previous efforts to reform the Communications Act have failed, the current Committee's efforts have a better chance of progress than those of its predecessors. The Republicans already control the House of Representatives, and

1 See 47 U.S.C. § 151 et seq.

2 The Telecommunications Act of 1996 is integrated into the Communications Act. See Telecommunications Act of 1996, P.L. 104-104 (1996).

3 The Communications Act is divided into seven Titles: General Authority (Title I); Common Carriers (Title II); Special Provisions Relating to Radio (Title III); Procedural and Administrative Provisions (Title IV); Penal Provisions and Forfeitures (Title V); Cable Communications (Title VI); and Miscellaneous Provisions (Title VII).

4 "Upton and Walden Announce Plans to Update the Communications Act," Energy & Commerce Committee (Dec. 3, 2013), available at http://energycommerce.house.gov/press-release/upton-and-walden-announce-plans-update-communications-act (last visited Sept. 10, 2014).

5 White Paper: Modernizing the Communications Act (rel. Jan. 8, 2014), available at http://1.usa.gov/1tJvebC.

6 White Paper: Modernizing U.S. Spectrum Policy (rel. Apr. 1, 2014), available at http://1.usa.gov/1m1eTQM.

7 White Paper: Competition Policy and the Role of the Federal Communications Commission (rel. May 19, 2014, available at http://1.usa.gov/1uLUBuj.

8 White Paper: Network Interconnection (rel. Jul. 15, 2014), available at http://1.usa.gov/1sDKd8Q.

9 White Paper: Universal Service Policy and the Role of the Federal Communications Commission (rel. Aug. 22, 2014), available at http://1.usa.gov/1D1x3XO.

recent polls show the party is likely to gain control of the Senate this November. With a majority in both houses of Congress, the Committee's efforts to rewrite the Communications Act would not face the partisan divide that has stymied past efforts.

At stake in a rewrite of the Communications Act is the regulatory treatment of a huge driver of the U.S. economy. The telecommunications industry is one of the fastest growing in the U.S., valued at $511.3 billion in 2010, and projected to grow to $774.7 billion by 2020.[10] The wireless marketplace in particular has "large and persistent positive spillovers" to the entire U.S. economy.[11]

Although the Committee has not yet signaled how it might restructure the Act, some of the key areas for reform are already topics of spirited public debate. Efforts to limit discrimination in broadband providers' handling of Internet traffic have attracted the most attention of any issue in 2014. Beyond the headlines about paid "fast lanes" for certain types of Internet traffic, the "open internet" rubric has come to include a raft of related issues and obligations including interconnection, peering, reasonable network management, congestion pricing, and permissible service offerings – any one of which has the potential to alter longstanding commercial relationships among carriers in the industry.

The Committee has also signaled its interest in reform of billions of dollars of subsidies for communications services. Congress created the USF to ensure that all consumers have access to telecommunications and advanced services such as broadband at affordable rates. Funding for all USF programs comes from fees paid by mobile and fixed telecommunications carriers, as well as certain other providers. One of the key debates about USF is what services and providers should have to contribute to the Fund. Some carriers argue that the contribution base should be expanded to include broadband providers. Others, especially in the technology sector, argue for a narrower base of contributing parties in the interest of promoting technological innovation. Because providers can and typically do pass along their USF contribution fees to consumers on their telephone bills, any change in the contribution structure would be likely to have a direct and immediate effect on the bills consumers see every month.

Simplifying the laws that currently govern infrastructure deployment is another Committee goal. The Communications Act includes a complicated series of provisions regarding the rights of telecommunications and cable providers to attach equipment to existing utility poles, and the ability of state and local governments to control the permitting process for the construction of new telecommunications infrastructure. The latter issue, in particular, has set up a key battle, as states and local governments attempt to maintain control over their permitting processes, while wireless providers argue in favor of expedited, federally-controlled processes.

Other important issues that Congress is poised to consider are more arcane, but may have more immediate consequences for the industry. For example, although few consumers are aware of the existing provision of the Act that requires incumbent carriers to provide non-discriminatory "special" wholesale access to their network to competitors, the current statutory language does not specifically require access in an all-IP environment, which could affect the ability of competitors to obtain access to incumbents' networks following the pending IP transition.

As with any reform driven by Congress, a shift in the political environment could change the direction of Communications Act reform at any time. But if the Republicans take control of both the House and Senate this Autumn, as many (though not all) pollsters predict, Congress seems likely to seek substantial revisions to the laws governing broadband and communications in the United States – a development that promises profound and lasting effects on the U.S. communications sector. ■

10 Richard Henderson, "Industry Employment and Output Projections to 2020," U.S. Bureau of Labor Statistics (rel. Jan. 2012), available at http://www.bls.gov/opub/mlr/2012/01/art4full.pdf (last accessed Sept. 12, 2014).

11 Peter Cramton, Evan Kwerel, Gregory Rosston & Andrzej Skrzypacz, *Using Spectrum Auctions to Enhance Competition in Wireless Services*, 54 J. L. & Econ. S167, S170 (2011). An analysis from 2011 found that the U.S. wireless industry directly or indirectly provides 3.8 million jobs, or 2.6 percent of all U.S. employment, and was valued at $195.5 billion. Roger Entner, *The Wireless Industry: Essential Engine of US Economic Growth*, Recon Analytics 1 (May 2012), available at http://bit.ly/Msb2Le (last accessed Sept. 12, 2014).

Trey Hanbury
Partner, Washington, D.C.
T +1 202 637 5534
trey.hanbury@hoganlovells.com

Deborah Broderson
Associate, Washington, D.C.
T +1 202 637 5873
deborah.broderson@hoganlovells.com

New privacy principles for connected vehicles

Hogan Lovells is leading the efforts of the automotive industry to develop a set of privacy principles governing the use of data from "connected cars." This article describes the policy environment leading to the drafting of privacy principles and the resulting work.

For many, the 2014 Consumer Electronics Show – typically a showcase of in-home entertainment technology – was an event about vehicle technologies and services. Consumers and tech writers praised the announcement of 4G connectivity for vehicles and marveled at the demonstrations of autonomous vehicles.

But the excitement about connected vehicles has been tempered, for some, by privacy concerns. In late 2013, the U.S. Government Accountability Office ("GAO") published a report finding that the privacy practices of some providers of in-car location-based services were "unclear." That report led U.S. Senator Al Franken to call for a location privacy law. The California legislature considered a bill that would have required automobile manufacturers to provide owners with broad access to and control over the information that vehicles record, generate, store, or collect. The Detroit Free Press reported that automotive industry and legal experts thought of auto data privacy as "the industry equivalent of the Wild West." Even Volkswagen Chairman Martin Winterkorn stated that "[T]he car must not become a data monster."

> Excitement about connected vehicles has been tempered by privacy concerns.

By the spring of 2014, automakers were increasingly concerned that California and other states might soon pass hastily-drafted and overly-broad laws regulating the collection, use, and sharing of information collected from vehicles. Some of the bills considered by state legislatures would have substantially impacted manufacturers' business models and design practices. The auto industry recognized that it needed to act swiftly.

So, the Alliance of Automobile Manufacturers, later joined by the Association of Global Automakers, and their members (23 automakers) decided to develop a set of principles for vehicle technologies and services that would directly address privacy concerns and address the calls for hasty legislative action. To assist in the development and release of these privacy principles, the car manufacturers turned to Hogan Lovells.

Throughout the spring and summer, a Hogan Lovells team from the firm's Privacy and Information Management Practice met with the Alliance, Global, and their members and drafted a set of principles that demonstrates a commitment to responsible stewardship of the information collected by connected vehicles. The result of those efforts is the Privacy Principles for Vehicle Technologies and Services ("Principles"), which automakers and other participants in the auto industry can choose to adopt when offering innovative vehicle technologies and services. In drafting the Principles, we turned to the Fair Information Practice Principles, the White House's proposed Consumer Privacy Bill of Rights, and guidance from the U.S. Federal Trade Commission ("FTC"). We also drafted the Principles with an eye to ensuring that they would support the evolution and development of innovative technologies and services.

The resulting Principles contain fundamental commitments to:

Transparency: Companies that adopt the Principles must provide clear, meaningful notices about how they will collect, use, and share covered information. The Principles do not, however, establish rigid requirements for the format, presentation, or timing of notices.

Choice: The Principles establish a commitment to providing vehicle owners with certain choices about the collection, use, and sharing of covered information. But choice is not required where information practices are essential to vehicle operations, safety, compliance, or warranty purposes. Participating companies must obtain affirmative consent prior to 1) using precise location information, biometrics, or information about

driving behavior for marketing; and 2) sharing such information with unaffiliated third parties for their own use.

Respect for Context: Participating companies commit to using and sharing covered information in ways that are consistent with the context in which the information was collected, taking account of the likely impact on owners and registered users of vehicle services. This allows companies to engage in adaptive and innovative uses of data while helping ensure that consumer privacy is taken into account.

Data Security: Participating companies commit to implementing reasonable security measures, and the Principles do not establish inflexible security standards.

Integrity and Access: Participating companies commit to taking reasonable steps to ensure that the personal information they hold is accurate. Owners and registered users of vehicle services are entitled to access their registration information. And companies commit to exploring additional means of access, taking into account privacy and security concerns.

Accountability: Participating companies commit to establishing reasonable policies and procedures to help ensure their own adherence to the Principles. Companies also commit to taking reasonable steps to ensure that service providers receiving covered information adhere to the Principles. The Principles do not contain a built-in enforcement mechanism nor do they prescribe specific accountability measures. However, participating companies that do not live up to their commitments risk facing enforcement actions brought by the FTC or state attorneys general.

The Principles reflect an important self-regulatory structure through which subscribing automakers commit to having policies and practices implementing the commitments contained in the Principles. In that way, the Principles are binding public commitments enforceable through Section 5 of the Federal Trade Commission Act, requiring companies to fulfill their publicly stated commitments such as those in the Principles.

An important part of the roll-out of the Principles was outreach to policymakers and public policy advocates. Meetings were held with academics, privacy advocates, and regulators to brief those parties on the advances contained in the Principles. The response to the self-regulatory principles was very positive, with one FTC Commissioner commenting that they could serve as a model for the Internet of Things community.

> “The Principles could serve as a model for the Internet of Things community.”

The Principles reflect a major step in the protection of personal information collected through in-vehicle technologies and provide guidance on how privacy may be promoted in the Internet of Things ecosystem. We are proud to have had the opportunity to help the auto industry build consensus around the Principles and help the industry demonstrate to consumers, regulators, and policymakers that the industry takes its privacy commitments seriously. And we look forward to taking the Principles on the road. ■

Christopher Wolf
Partner, Washington, D.C.
T +1 202 637 8834
christopher.wolf@hoganlovells.com

EU: The wider effect of the Google 'right to be forgotten' case

Much has been written about the decision of the Court of Justice of the European Union (CJEU) regarding Google Spain and the right to be forgotten. The origins of this case go back to early 2010, when Mr Mario Costeja, a Spanish national, asked Google to remove certain search links to newspaper announcements of 1998 regarding the forced sale of properties arising from social security debts which contained his name. As Google did not act on Mr Costeja's request, the Spanish data protection authority became involved and when it ordered Google to honour the request, Google challenged that order in court. Given the legal complexity of the arguments presented by the parties, the National High Court of Spain referred the matter to the CJEU, which in May 2014 ruled in favour of Mr Costeja and the Spanish authority.

The CJEU took the view that when an individual rightfully objects, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name, links to web pages published by third parties and containing information relating to that person. According to the CJEU, this should be the case even where that name or information is not erased beforehand or simultaneously from those web pages, and when its publication on those pages is lawful. The CJEU went on to say that the data protection rights of the individual override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name.

The controversy of this case has focused on the impact of the judgment on freedom of expression and the right of access to information, as well as the potentially devastating effect of a large amount of deletion requests. This is understandable as with the prospect of an even more demanding EU data protection framework looming over the horizon, the right to be forgotten decision is a potential game changer for the whole Internet industry. But the CJEU's decision is not only relevant to search engines or Internet companies. The implications of the judgment are much wider.

Applicability of EU data protection law

For starters, this case has radically shaken the basis on which the applicability of EU data protection law has been understood until now. The CJEU established that Spanish data protection law applied to Google on the basis of the rule set out in article 4(1)(a) of the data protection directive, which relies on data processing carried out in the context of the activities of an establishment of a controller located in an EU Member State. In practical terms, the CJEU took the view that under this rule there were two conditions for the local law of a member state to apply. The first one involves having an establishment in a particular country. For these purposes, a local subsidiary or branch – no matter how modest – will certainly qualify as an establishment. The second condition requires showing that the local establishment is involved in some way in the processing activities, even if that establishment is not actually doing the processing.

Aligning itself with the previous positions of the Article 29 Working Party on search engines and of the CJEU's own Advocate General, the CJEU decided that the sales generated by Google's local establishment in Spain were linked to the profit generated through the data processing activities – irrespective of where these actually took place – and that link was sufficient to trigger the applicability of Spanish law. The key point is that even if the local establishment is not making any real data processing decisions – as was acknowledged to be the case in this instance – that local subsidiary may still bring the whole data activity within the scope of application of the law, as long as there is some commercial connection with the data uses.

What is potentially very significant about the CJEU's interpretation of this rule is that each and every local subsidiary in the EU of a non-EU based data controller may be capable of triggering the applicability of the local data protection law. Something that could be affected by this doctrine is the long standing argument and legal position that a controller operating throughout the EU but headquartered in an EU country only needs to comply with the data protection law of that country. Whilst the CJEU did not address this issue, it pointed out that one of the reasons for taking the approach it took was that the data protection directive sought to prevent individuals from being deprived of the protection guaranteed by the directive and that protection from being circumvented. This would suggest that publicly appointing an EU-based entity as a data controller should still allow global businesses to operate across the EU whilst only being subject to the data protection laws of one member state.

Each and every local subsidiary in the EU of a non-EU based data controller may be capable of triggering the applicability of the local data protection law.

The right to be forgotten

The CJEU also ruled that under the existing data protection directive, the so-called 'right to be forgotten' can be exercised through two articles of the directive:

- Article 12(b) – Right of rectification, erasure or blocking of data, where the processing does not comply with the provisions of the directive.
- Article 14(a) – Right to object to the processing on compelling legitimate grounds.

The CJEU mainly focused on Article 12(b) of the directive and stressed that this right should be honoured in the event of any instance of non-compliance, such as:

- Processing data in a way incompatible with specified, explicit and legitimate purposes (Article 6(1)(b)).
- Processing data in an inadequate, irrelevant or excessive manner (Article 6(1)(c)).
- Processing inaccurate data or not keeping it up to date (Article 6(1)(d)).
- Processing data for longer than necessary (Article 6(1)(e)).
- Not meeting any of the criteria for making the processing legitimate (Article 7).

The CJEU found that in this particular situation, the processing by Google was no longer relevant because the original publication was 16 years old and it could not be justified in the public interest or otherwise. An important point made by the CJEU is that whilst the legal basis for a 'right to be forgotten' exists under the directive, its exercise needs to be considered on a case by case basis. However, when considering each case, it must be accepted that as a general rule, Articles 12(b) and 14(a) override a data controller's entitlement to the processing that simply relies on that controller's legitimate interest. This is a major rebalancing act by the CJEU which puts data controllers in a very weak position to deny the exercise of the 'right to be forgotten' under the existing EU data protection law.

In practical terms, an individual could argue that the processing of their data by a data controller is inadequate, irrelevant or excessive; such data is not kept up to date; or the data is being kept for longer than necessary. In that situation, the doctrine of the CJEU on the Google case would be applicable and most data controllers would find themselves in the same position as Google, where they would need to assess and decide whether any of the conditions triggering the right are present.

What next?

The forthcoming EU data protection Regulation may of course change all this, but that is unlikely. Given that the Regulation will apply to the whole of the EU, the applicability of the law issue will only be relevant from the point of view of which data protection authority will be entitled to claim jurisdiction over a data controller that operates across the EU. Although this point is subject to the outcome of the ongoing debate regarding the 'One Stop Shop' (OSS) provisions, at the very least it can be assumed that all data protection authorities will be empowered to deal with queries or complaints by their local data subjects. To what extent a local authority is then able to take any measures against an EU-wide data controller will entirely depend on the final version of the OSS provisions.

As to the right to be forgotten, the draft Regulation puts data controllers in the same situation as under the directive as interpreted by the CJEU, although the ability of an individual to exercise this right under the Regulation is potentially wider given that the Regulation contains more obligations and hence more opportunities for non-compliance than the directive. The draft approved by the European Parliament in March 2014 was marginally less stringent in this respect, as it referred to a right to erasure which is triggered where the data has been "unlawfully processed", but it does not radically change the position. In summary, the outcome of the current legislative reform will determine the scope of this right but it seems fair to assume that the general principle established by the CJEU under the directive in this respect will remain valid and equally far-reaching. ■

This article was first published in *Privacy and Data Protection, Volume 14, Issue 8*

Eduardo Ustaran
Partner, London
T + 44 (0) 207 296 5249
eduardo.ustaran@hoganlovells.com

South Africa: data protection legislation

Data protection in South Africa is regulated under the broad constitutional right to privacy, the common law and a few pieces of legislation that contained interim provisions relating to data protection. Until very recently, South Africa did not have data protection-specific legislation.

With the increase in electronic commerce globally, large industries managing computerised databases of millions of individuals' records and the surveillance potential of computer systems, prompt demands for specific rules governing the collection and handling of personal information arose.[1] Commissioned in 2005 and completed in 2009, the South African Law Commission finalised an investigation into privacy and data protection in South Africa, with a recommendation that privacy and information protection be regulated by general statute.[2]

The South African Law Commission's recommendation resulted in the creation of the Protection of Personal Information Act (the "Act"). Although signed into law in November 2013, April 2014 marked the partial commencement of the Act with only several sections coming into force, including those related to the establishment of the information regulator, the issuance of regulations to the Act and the definitions clause which, in the latter instance, codified concepts crucial to data protection including "processing" and "personal information". The commencement of the former sections is indicative of the processes being put in place by the government of South Africa to ensure that the commencement of the remaining sections is met with the relevant support, in the form of regulations and the establishment of the information regulator. Outside these sections, the remainder and indeed the material aspects of the Act are not enforceable and have no foreseeable or determinable effective date.

Recognising that a failure to have sufficient data protection is a barrier to international trade, and that the specific obligations in article 25 and 26 of the European Data Protection Directive stipulate that personal data should only flow outside the boundaries of the European Union to countries that can guarantee an "adequate level of protection", the Act draws on data protection principles applied in the European Union, among others, in order to ensure that South Africa can provide "adequate" protection, as gauged from an international perspective.[3]

As a result, the core of the Act consists of eight conditions for the lawful processing of personal information that closely resemble data protection principles utilised in the European Union. These conditions include accountability, process limitations (fair and lawful processing), purpose specification, further processing limitations, information quality, openness, security safeguards and data subject participation.

The Act applies to the "processing" of "personal information", the latter being constructed widely to include information related to the gender, marital status, race, age, health, religion, conscience, belief, language, financial, criminal and employment information, addresses, fingerprints, personal opinions and private or confidential correspondence of a person. The Act covers the processing of personal information by individuals, private and public entities, all of whom are considered "responsible parties" in terms of the Act. The Act also encapsulates the operations of subcontractors of responsible parties, who process personal information for or on behalf of the responsible party, as well as responsible parties not domiciled in South Africa but who make use of automated and non-automated means of processing, situated in South Africa.

By exception, the Act does not apply to the processing of personal information, solely for personal or household activity, that has been de-identified to the extent that it cannot be the re-identified again, by or for the state and for national security, defence or public safety, for exclusively journalistic purposes by persons subject to a professional code of ethics with its own rules for the protection of personal information and as may be exempted by the information regulator.

The Act contains various enforcement and punitive mechanisms to incentivise compliance. From an enforcement perspective, the Act provides for the establishment of an information regulator whose powers and functions include monitoring and enforcing compliance with the Act, the handling of complaints,

1 The South African Law Reform Commission, Project 124 – Privacy and Data Protection Report 2009 page vi.

2 Id. at viii

3 Id. at vii

the issuance and regulation of codes of conduct, and the facilitation of cross-border cooperation. Obstruction of the information regulator or a failure to comply with a compliance notice issued by the information regulator may lead to an administrative fine or a period of imprisonment of up to 10 years. An administrative fine may not exceed ZAR10 million.

The Act also empowers a data subject to institute a civil action for damages against a responsible party for breach of any of the conditions, whether or not there was intent or negligence on the part of the responsible party (strict liability). The Act limits the number of defences that can be raised by the responsible party in response to such claim including force majeure or that compliance with the condition was not reasonably practicable in the circumstances.

Responsible parties will have 12 months from the commencement of the Act within which compliance must be achieved. ■

Leishen Pillay
Senior Associate, Johannesburg
T +27 11 523 6273
leishen.pillay@hoganlovells.com

Technology neutrality in Internet, telecoms and data protection regulation

Technology neutrality is one of the key principles of the European regulatory framework for electronic communications. The principle was first introduced in 2002, and reinforced in the 2009 with the revised EU telecoms legislation. Since the 2009 revisions, all spectrum licenses in Europe are supposed to be "technology neutral." Since 2011, technology neutrality has also been recognized as a key principle for Internet policy (OECD, 2011). The concept now appears in the proposed EU Data Protection Regulation,[1] and the proposed EU Directive on Network and Information Security[2] (the so-called NIS Directive), both of which will likely be adopted in 2015. Technology neutrality sounds like a good idea, but its meaning is not immediately clear. The purpose of this paper is to unpack the concept of technology neutrality, and examine its meaning (and utility) in different contexts.

Depending on the context, technology neutrality can have three different meanings:

- Meaning 1: technology neutrality means that technical standards designed to limit negative externalities (eg. radio interference, pollution, safety) should describe the result to be achieved, but should leave companies free to adopt whatever technology is most appropriate to achieve the result.
- Meaning 2: technology neutrality means that the same regulatory principles should apply regardless of the technology used. Regulations should not be drafted in technological silos.
- Meaning 3: technology neutrality means that regulators should refrain from using regulations as a means to push the market toward a particular structure that the regulators consider optimal. In a highly dynamic market, regulators should not try to pick technological winners.

In practice, Meaning 1 and Meaning 3 can overlap. A regulator may impose a given technological solution both as a means to limit harmful externalities, such as radio interferences (Meaning 1), and as a means of structuring the market in a certain way (Meaning 3). We examine each of these meanings in more detail below.

Meaning 1: Technology neutrality is used in standards intended to limit undesirable effects. Technology neutrality can be used in connection with standards designed to limit negative externalities. The standards may be designed to protect the environment, to enhance automobile safety, or limit radio interference. In this context, technology neutrality is synonymous with the term "performance standards", which are standards that describe the output expected (e.g., the amount of radio interference), but do not impose a given technology (e.g., GSM or UMTS). The concept of performance standards was developed in the United States in the 1980s in the context of the "better regulation" movement. Performance standards are deemed to be more efficient than so-called "design standards" because performance standards give freedom to regulated entities to choose the technology best suited to achieve the outcome specified in the standard (Breyer, 1982). By contrast, design standards incorporate technological choices made by the regulator which can become quickly outdated and inefficient. Moreover, design standards can harm competition because they will lock in certain technologies at the expense of other competing solutions. The choice of technology by the regulator may also be subject to regulatory capture by strong industry players who have the resources to lobby for a particular technological solution. President Obama's 2011 executive order on good regulatory principles reaffirms that the U.S. government should use performance standards whenever feasible (Obama, 2011).

Performance standards can be more difficult to understand and apply, particularly for small companies (Hemenway, 1980). If a standard requires the installation of a certain component, companies will have no difficulty understanding the standard and applying it. By contrast, in the case of the performance standard companies may be left guessing what kind of technology would result in the output specified in the standard. In order to address this problem, particularly for small companies, some technologically neutral regulations give examples of technologies that will satisfy the output described in standard, while leaving the door open to other kinds

1 Commission Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012)11 final, 25 January 2012.

2 Commission Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final, 7 February 2013.

of technologies. Technological choices can also be made in the context of self-regulatory or co-regulatory initiatives. This approach is envisaged in the proposed European Data Protection Regulation, in connection with implementation of "privacy by design."[3]

The use of a performance standard can increase the costs of verification and enforcement for the regulator. Performance standards may therefore be inappropriate where verification of compliance is difficult, and the risk associated with the negative externality is high, for example in the context of safety standards for nuclear power plants (Hemenway, 1980). On balance, however, performance standards (technology neutrality under Meaning 1) generally promote innovation and efficiency (Besanko, 1987, Coglianese *et al.*, 2002).

Meaning 2: Technology neutrality defines the scope of regulation. The second context in which technology neutrality is used is to define the scope of regulation. In the field of electronic communications, the European Framework Directive of 2002[4] makes "technology neutrality" one of the guiding principles for regulation of the telecommunications sector in Europe. Wherever possible, regulators are to ensure that their rules are "technology neutral." When used in the 2002 Framework Directive, the concept of technology is designed above all to reflect the phenomenon of convergence between electronic communications networks and services (Kannecke and Körber, 2008). The idea is that regulators would apply the same principles of market analysis and remedies to all kinds of electronic communications networks and services. At the time, this unified approach to regulation was revolutionary because previously each kind of network (public switch telephone network, cable network, mobile network) was subject to separate sets of rules. Under the "technologically neutral" European approach, all networks and services are subject to the same competition-law based test under which regulators identify relevant markets and dominant actors on the market, and apply appropriate remedies to address enduring competition problems. This market analysis process often leads to market definitions and remedies that are not technology neutral. For example, retail mobile services are generally not considered substitutes for fixed-line services, leading to the conclusion that they belong to different relevant markets. This in turn leads to different conclusions relating to market dominance, and to remedies. As a result, mobile operators in Europe are generally free from economic regulation at the retail level, whereas in the fixed-line market, the incumbent operator is generally subject to significant regulatory burdens. Remedies are also not technologically neutral. Access obligations such as wholesale bitstream access or unbundling of the local loop may be imposed on copper networks, but not on other kinds of networks.

In 2009, the concept of technological neutrality was pushed to a new level in Europe. Under the 2009 Better Regulation Directive[5], European lawmakers imposed the principle that spectrum licenses should be technologically neutral except in limited cases. This means that regulators could no longer impose a particular technology on mobile operators. In theory, mobile operators holding spectrum under an old 2G GSM license should be able to deploy 4G LTE technology over that spectrum. The 2009 Directive led to a wave of "spectrum refarming" in Europe. Operators are not allowed to convert to new technology unilaterally, but must ask permission from the regulator. The regulator then evaluates whether the change in technology would disrupt competition on the relevant retail market, and if necessary will rebalance the spectrum assignments so as to level the playing field. In the context of spectrum licenses, technology neutrality is more akin to "performance standards," ie. Meaning 1 of our definitions.

For spectrum licenses, the 2009 Better Regulation Directive even went further, recommending the principle of "service neutrality." This principle means that the holder of the spectrum license should not be restricted in the kinds of services offered. In theory, the services could be mobile interpersonal communications, fixed communications or even broadcasting services. In practice, the idea of service neutrality is not easily applied to spectrum licenses because of the way the spectrum is divided into blocks. The organization of the spectrum channels will predetermine the kind of service that can usefully be offered. For example, the assignment of a duplex channel including a return path *de facto* means that

3 Article 30.

4 Directive 2002/21/EC.

5 Directive 2009/140/EC.

the service will likely be two-way communication, as opposed to broadcasting. This principle also holds true to some extent for technology neutrality. The way the spectrum assignments are organized, including the size of guard bands and interference rules, will to a large extent predetermine the kind of technology that can be deployed by an operator. The engineers who decide how the spectrum should be divided up and assigned to operators will do so with one or more technologies in mind.

In the context of Meaning 2, technology neutrality brings considerable benefits to regulators, because it permits regulators to adapt to new technologies without having to be concerned with jurisdictional boundaries. Section 5 of the FTC Act, prohibiting unfair and deceptive practices, is an example of a technologically neutral rule. The FTC can apply the rule to new forms of technology and business models without fear of overstepping the FTC's jurisdictional boundaries. The future EU Data Protection Regulation would also be technologically neutral in this sense.[6]

The flexibility given to regulators by technology neutrality can help them put pressure on regulated entities to find self-regulatory solutions (Halftech, 2008). The regulators can use the threat of future regulation as an incentive to push the market toward self-regulatory or co-regulatory solutions, which may be more effective than command and control regulations. As noted above, co-regulatory solutions of this kind are envisaged in the proposed EU Data Protection Regulation in the context of "privacy by design."

Regulations that are technologically neutral give regulators flexibility, but this flexibility could encourage regulators to extend their authority to new markets and technologies prematurely, before there is evidence of an enduring market failure that needs to be corrected. In this sense, technology neutrality could encourage over-regulation of new emerging markets. Conscious of this risk, lawmakers in Europe included in the electronic communications Framework Directive a statement that competitive or emerging markets should not be subject to *ex ante* regulation.[7] Technology neutrality therefore needs to be accompanied by a healthy dose of regulatory restraint.

Along the same vein, where technology neutrality creates uncertainty regarding the scope of regulation as applied to new technologies, companies may react to this uncertainty by deferring investments. A number of incumbent operators in Europe have complained that uncertainty regarding the application of access remedies to new fiber networks in Europe inhibits investment decisions. This in turn triggered debate in Europe about whether certain new network technologies should be granted a "regulatory holiday." Similar arguments are raised in the US regarding whether mobile operators should be subject to net neutrality rules.

Meaning 3: Technology neutrality (or the absence thereof) can be used to nudge the market in a certain direction that is considered desirable by policymakers. For example, regulators might have a particular vision regarding the build-out of fiber networks. In order to implement that vision, the regulator may adopt rules that are not technology neutral. In some cases, the only way the regulator's vision can be implemented is through a non-technologically neutral regulation. An example of this approach is the choice of the GSM standard for mobile telephony in the 1990s. The imposition of the GSM standard was considered critical in permitting the development of a European market for handsets and interoperable mobile services. Whether the imposition of the GSM standard ended up working better than market-driven voluntary standards is a question beyond the scope of this paper. The point is that the objective of the regulator is not just to limit harmful interference (Meaning 1), but to structure the market a certain way (Meaning 3). Whether non-technologically neutral regulations are useful in this context depends a great deal on the risk of error in the policymaker's vision. In a fast moving market with rapid technological change, the risk of regulatory error is high, making non-technologically neutral regulation risky.

A parallel can be drawn here with the debate surrounding government imposed standards, such as UMTS, versus voluntary standards such as Blu-ray. The question is in what cases are government imposed standards preferable to market-led standards.

6 Recital 13.

7 Recital 27.

In a recent article, Llanes and Poblete (2014) show that market standards are preferable where there is a high level of uncertainty surrounding the benefits of the technology. A similar conclusion could be made for technology neutrality: the higher the level of uncertainty surrounding technological evolution, the more it becomes important to make standards technologically neutral. When used in the context of the OECD Recommendation on Internet Policymaking (OECD, 2011), technology neutrality is meant to address this point.

Technology neutrality vs. platform neutrality

Technology neutrality should not be confused with platform neutrality. Some European policymakers believe that the principles of net neutrality should not be limited to Internet access providers, but should also extend to large Internet platforms including search engines, app stores and social media. The idea is to extend some form non-discrimination obligation, or "duty of loyalty," to these platforms, even if doing so would not be justified under competition law. The idea of making net neutrality rules "technologically neutral" has some superficial appeal. However, imposing neutrality obligations on Internet platforms could have significant adverse effects. The first adverse effect is the potential impact on innovation. Shelansky (2013) and Manne and Wright (2011) have shown that in antitrust remedies, the risk of regulatory error is high when dealing with new Internet-based business models. Regulators have a systematic bias toward seeing anticompetitive conduct in new business models. More important, the cost of error is much higher in the case of a so-called "Type I" error – i.e. when a regulator mistakenly imposes a remedy – than for a "Type II" error – i.e. when a regulator mistakenly fails to impose a remedy. This leads to the conclusion that where there is a significant uncertainty due to rapid technological and market changes, regulators should have a bias in favor of doing nothing rather than imposing a remedy. In fast-moving markets, the perceived harms are often addressed by the market, making regulatory remedies unnecessary.

The second adverse effect relates to freedom of expression. Imposing "platform neutrality" would create restrictions to freedom of expression and to freedom to conduct a business, both of which are fundamental rights recognized by the European Court of Justice. In Europe, television broadcasting platforms can be subject to "must carry" obligations, but the case for extending must-carry or other public service obligations to Internet platforms has not yet been made. Audiovisual regulations are typically justified due to the scarcity of audiovisual spectrum and the "push" character of scheduled audiovisual programming. Neither of these factors (scarcity or "push" character of content) is present on most Internet content platforms.

Conclusion

As the US looks at rewriting its telecommunications laws, technology neutrality in the sense of Meaning 2 will be a prime consideration. The US law is built around technology silos that should probably be eliminated in any rewrite. Data protection law is already technology neutral (Meaning 2) in Europe, and that neutrality will be reinforced in the new EU Data Protection Regulation. Section 5 of the US FTC Act is likewise technology neutral in the sense of Meaning 2. For standards developed in the context of cyber-security legislation (such as the proposed EU NIS Directive), and for "privacy by design" (under the EU Data Protection Regulation), technology neutrality in the sense of Meaning 1 will be critical to encourage innovation and efficiency. Self- or co-regulatory instruments may be necessary to help give guidance to companies on technological options. Finally, in Internet policy, cyber-security and telecoms policy, regulators should not attempt to structure the market using technology-based regulation (Meaning 3), because such attempts are likely to create more harm than good in fast-moving markets. ■

A French version of this article appeared in the journal of the French telecommunications regulatory authority: "*Les Cahiers de l'ARCEP*"

References:

Besanko, D. (1987), "Performance versus Design Standards in the REgulation of Pollution", *34 J. of Pub. Econ. 19*.

Breyer, S. (1982), "Regulation and its Reform", *Harvard University Press*.

Coglianese, C., J. Nash et T. Olmstead (2002), "Performance-Based Regulation: Prospects and Limitations in Health, Safety and Environmental Protection", *Harvard Faculty Research Working Paper 02-050, December*.

Halftech, G. (2008), "Legislative Threats", *61 Stanford L. Rev. 629*.

Hemenway, D. (1980), "Performance vs. Design Standards", *National Bureau of Standards, U.S. Department of Commerce*.

Kannecke, U. and T. Körber (2008), "Technological Neutrality in the EC Regulatory Framework for Electronic Communciations: A Good Principle Widely Misunderstood", *[2008] European Common Law Review 330*.

Koops, B.-J. (2006), "Should ICT Regulation be Technology-Neutral?", in Deconstructing Prevalent Policy One-Liners, IT & Law Series, vol. 9, TMC Asser Press, p. 77.

Llanes G. and J. Poblete (2014), "Coalition Formations in Standards Wars"(unpublished manuscript, August 2014).

Manne, G. and Wright, J. (2011), "Google and the Limits of Antitrust: The Case Against the Antitrust Case Against Google," *34 Harvard J. of L. & Pub. Policy 1*.

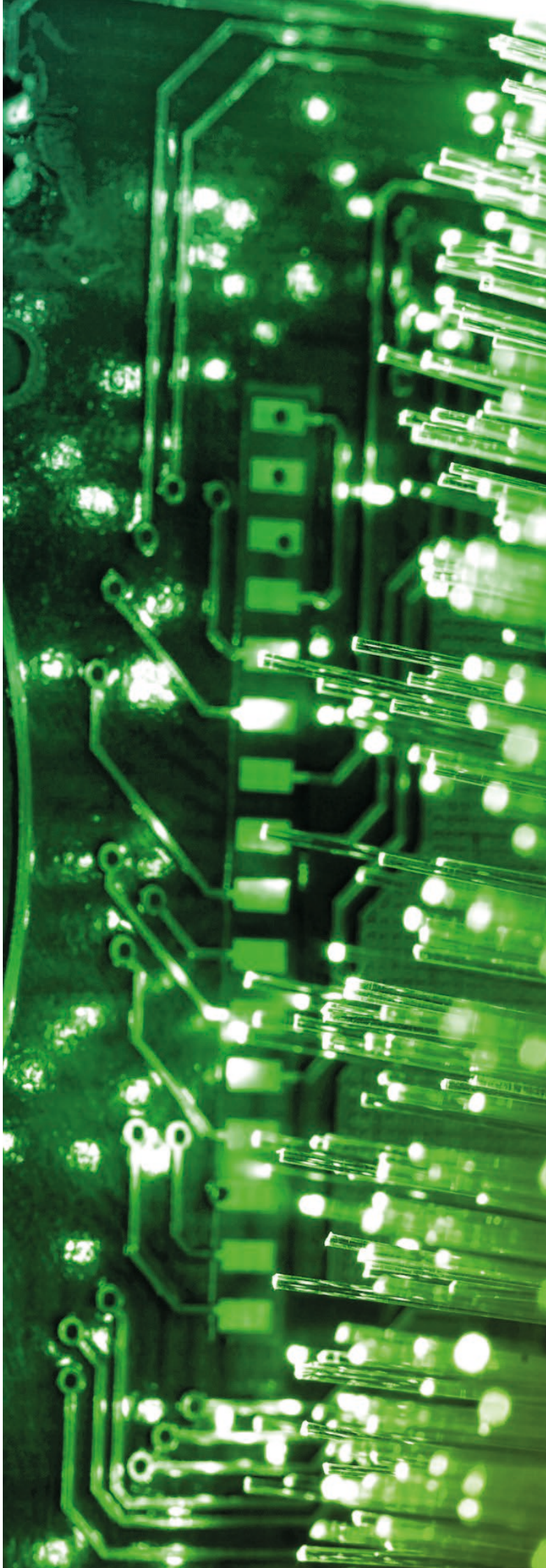
Obama, B. (2011), "Executive Order No. 13563 "Improving Regulation and Regulatory Review", January.

OECD (2011), "OECD Council Recommendation on Principles for Internet Policy Making", 13 December.

Shelanski, H. (2013), "Information, Innovation, and Competition Policy for the Internet", *161 U. Penn L. Rev. 1663*.

Winston Maxwell
Partner, Paris
T +33 (1) 5367 4847
winston.maxwell@hoganlovells.com

Marc Bourreau
Professor of Economics
Télécom ParisTech
marc.bourreau@telecom-paristech.fr



www.hoganlovells.com

Hogan Lovells has offices in:

Alicante
Amsterdam
Baltimore
Beijing
Brussels
Budapest*
Caracas
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Jeddah*
Johannesburg
London
Los Angeles
Luxembourg
Madrid
Mexico City
Miami
Milan
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Philadelphia
Rio de Janeiro
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Silicon Valley
Singapore
Tokyo
Ulaanbaatar
Warsaw
Washington, DC
Zagreb*

* Associated offices