Hogan Lovells

Global Media and Communications Quarterly

Featuring Highlights from the Winnik International Telecoms and Internet Forum 2013

OCTOBER 2013

Contents

Editor's Note

Broadband has changed everything and wireless broadband is changing everything all over again. With the estimated number of mobile connections worldwide in excess of 6 billion, mobile broadband has become the foundation for the next stage of Internet services, commerce, and innovation. The sheer volume of wireless data traffic is already astounding: global mobile data traffic in 2012 (885 petabytes per month) was nearly twelve times greater than the total global Internet traffic in 2000 (75 petabytes per month), according to Cisco's recent Global Mobile Data Traffic Forecast Update.

Winnik Forum

Against this backdrop, this issue of the Hogan Lovells *Global Media and Communications Quarterly* examines the wireless broadband market and its implications for global business. We begin this issue by collecting perspectives on international telecommunications issues from the firm's 2013 Winnik International Telecoms & Internet Forum, which was held in our Washington, D.C. office. The telecommunications professionals participating in the forum offered international perspectives on a wide range of topics that could either impede or accelerate the mobile broadband revolution. For example, the process of installing the base station and backhaul facilities essential to mobile broadband continue to pose challenges for operators around the globe; panelists at the Winnik Forum explained how these challenges might be met. At the same time, non-practicing entities (or "patent trolls") target the technology necessary to support the operating systems needed to run end-user devices and network-management products. Our panel discussed strategies companies can use to combat lawsuits by patent trolls, which have proven especially significant for the U.S. telecommunications industry, where median damage awards in patent suits remain many times higher than that of any other industry.

The Winnik Forum section of this issue also highlights opportunities for purchasing the spectrum resources needed to support wireless broadband data growth; the process and prospects of broadband companies acquiring the scale needed to provide cost-effective services; the challenges posed to traditional intellectual property regimes from new technological developments, and the feasibility of the United States and the European Union entering into new, transnational agreements that can promote services between some of the world's most developed economies. You can find links to the full discussion in the video archives available at our website, www.hoganlovells.com.

Cross-Border Data Flows

This issue of the *Global Media and Communications Quarterly* also offers an in-depth analysis of the legal implications of cross-border data flows. In *Delusions* of Adequacy: *A Critical Assessment of Cross-Border E.U. – U.S. Data Transfers,* Christopher Wolf explores the need for stronger transatlantic cooperation on privacy. The need to move data across borders is one of the drivers behind the growing demand for wireless spectrum, and an article by Coleman Bazelon and Giulia McHenry, *The Economics of Spectrum Sharing*, takes a close look at the economic tradeoffs associated with various spectrum sharing arrangements between commercial, federal, and local public safety users. Meanwhile, Suyong Kim and Matthew Levitt discuss the limits of attorney-client privilege for U.S. attorneys who provide advice to multinational corporations with a presence in Europe in *Can U.S. Attorneys Provide Privileged Advice in Europe?* New to this issue is a survey of innovative or unusual regulatory developments relevant to broadband services from around the world. In a series of articles covering Singapore, France, and Germany, we explore regulatory and legal developments that may have global resonance for the broadband marketplace.

Satellite Payload Procurement

Finally, in *Hosted Satellite Payload Procurement: A Brief "How-To" Guide*, Steven Kaufman and Randy Segal discuss the innovation of hosted payloads on board satellites. These "piggie back" loads have become an increasingly common way of reducing the cost of putting communications satellites in orbit, but managing the complex web of liabilities and risk by contract continues to pose a challenge for all parties.

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

Winnik Forum: Infrastructure Solutions to the Wireless Data Crunch

Infrastructure development, along with more spectrum and more efficient spectrum use, are all parts of the solution to the looming data crunch.

Keynote Address
Jonathan Adelstein, President and CEO, PCIA – The Wireless Infrastructure Association

Panel Moderators
Ari Fitzgerald, Partner, Hogan Lovells, Washington D.C.
Conor Ward, Partner, Hogan Lovells, London

Panelists
Richard Cimerman, Vice President, National Cable & Telecommunications Association
Michael McKenzie, Partner, Chief Strategy Officer, Grain Management
Stagg Newman, McKinsey & Company
Michel Rogy, ICT Policy Advisor, The World Bank

Infrastructure will play a critical role in meeting the challenges of the looming "wireless data crunch," said Jonathan Adelstein, President and CEO of PCIA – The Wireless Infrastructure Association, during his keynote address at the 2013 Winnik International Telecoms & Internet Forum. Mr. Adelstein explained that while more spectrum and more efficient use of spectrum are components of the solution, these approaches will not be sufficient to prevent service degradation or rationing of wireless data through pricing structures. What is needed in the U.S. are infrastructure solutions that allow for denser networks, cell splitting, and spectrum re-use, he said. These solutions are complex and take time, requiring the deployment of tens of thousands of small cells, including distributed antenna systems (DAS), heterogeneous networks (HetNets), picocells, and Wi-Fi. While Mr. Adelstein praised the efforts of U.S. policymakers to streamline the deployment of small cells, citing the President's Executive Order making it easier to build broadband infrastructure on federal lands, congress' wireless siting legislation limiting the ability of local governments to hinder antenna collocations on existing towers, and the Federal Communications Commission's tower siting shot clock and pole attachment rules, he maintained that more work is needed to ensure that small cells are a viable solution.

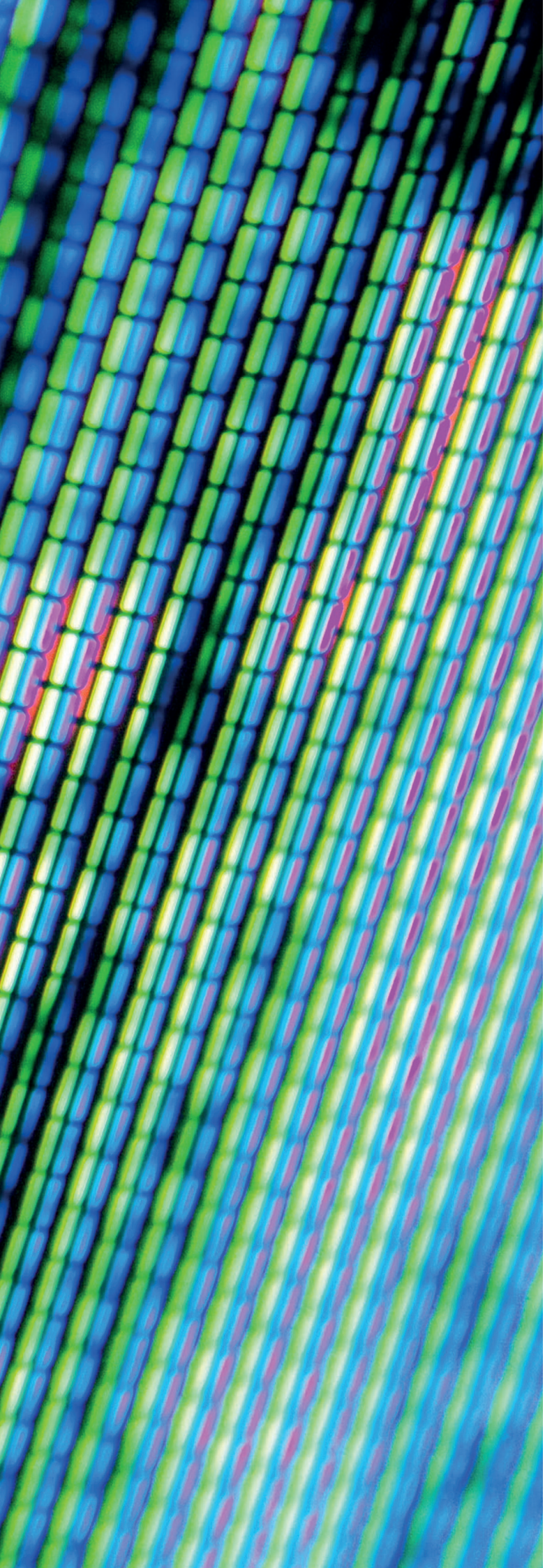
The infrastructure challenges abroad are equally thorny, and include access to tall infrastructure, deployment of neutral host infrastructure, development of backhaul solutions, and the expanded use of small cells.

Mr. Adelstein concluded by emphasizing that these issues are not simply about towers and antennas; they are about what wireless communications enable: economic opportunities, health care, education, public safety, and more.

> "The need for speed paces infrastructure deployment and outpaces policy."

Numerous panelists expanded upon the themes of Mr. Adelstein's keynote address. Discussing the challenges of the data wireless crunch, Stagg Newman of McKinsey & Company put it simply: the need for speed paces infrastructure deployment and outpaces policy. The policy issues consist of "poles and holes" and "sites and rights" problems that policymakers worldwide must resolve. In the U.S. 90% of homes are passed by hybrid fiber-coaxial networks capable of supporting 100 Mbps, which could suffice for the next 10 years or so, but would eventually become inadequate. The problem in other countries is more pressing. Most homes in Australia, for example, are passed by long copper loops, which could strand residents at 50 Mbps over the same 10-year period. Still other countries face even more fundamental problems related to access generally, regardless of speed. While the world's infrastructure challenges are daunting, Mr. Newman believes that industry will rise to meet them, even if policymakers do not.

Focusing on the U.S., Rick Cimerman, Vice President of the National Cable & Telecommunications Association, lauded the cable industry's ability to push fiber out, noting that since 1996 Internet connection speeds have increased 900% while prices have gone down. Mr. Cimerman explained that cable is rising to meet future challenges by deploying the largest Wi-Fi network in the country, with over 127,000 active hotspots already in use and tens of thousands more in the offing. While most communities recognize and embrace the benefits of Wi-Fi, certain unregulated entities see an opportunity



to exploit their monopoly resources and stifle this broadband infrastructure solution. Mr. Cimerman called for action to prevent these abuses, particularly against cooperative utilities that stifle broadband in rural communities where it is needed most.

Michael McKenzie, Chief Strategy Officer at Grain Management, agreed with Mr. Adelstein's observation that the mobile Internet is generating exponential growth in data consumption and corresponding network capacity challenges. Mr. McKenzie also agreed that the solution to these challenges must involve massive infrastructure investment. In emerging markets in particular, the solution must focus on the expansion of the neutral host model, or "passive infrastructure sharing," where independent tower and infrastructure companies lease space to competing wireless carriers. Mr. McKenzie observed that a key catalyst for infrastructure sharing is a spectrum auction, explaining that when a regulator sees the benefit of auctioning, it suggests a corresponding market for increased sharing and tenancy on independently owned infrastructure. In the U.S., Mr. McKenzie suggested that industry should continue to engage municipalities in a "win-win" dialogue to encourage them to compete on being broadband friendly.

Concentrating on the benefits of mobile wireless, Michel Rogy, ICT Policy Advisor at The World Bank, elaborated on its potential to alleviate poverty, stimulate development, and empower individuals worldwide, such as by providing market pricing for the day's catch to independent fisherman in Africa. Given these benefits, Mr. Rogy noted that all developing countries are convinced that they need to push their broadband agendas. This involves identifying the mix of technologies to deploy affordable broadband, including submarine cables and broadband links that institutions such as The World Bank can promote through the use of public-private partnerships.

Keynote Address: PCIA – The Wireless Infrastructure Association President and CEO Jonathan Adelstein

http://hlglobal/sites/Tools/SitePages/VideoPlayer.aspx?vidID=202

Winnik Forum: International Spectrum Policy Developments

Regulators around the world are trying various approaches to satisfy global demand for additional spectrum for mobile wireless services.

Panel Moderators
Michele Farquhar, Partner and Director of the Communications Practice Area, Hogan Lovells US LLP, Washington D.C.
Reinhard Wieck, Managing Director – Deutsche Telekom

Panelists
David Jeppsen, Vice President, NTT DoCoMo USA
Dean Brenner, Senior Vice President-Government Affairs, Qualcomm, Inc.
Diane Cornell, Vice President-Government Affairs, Inmarsat plc.
Chris Guttman-McCabe, Executive Vice President, CTIA – The Wireless Association®

The global demand for additional spectrum for mobile wireless services is rapidly increasing. In a panel addressing international spectrum developments, panelists discussed emerging issues and hot topics surrounding this growing need and the policy issues currently shaping the debate around how to meet the demand.

Some countries have recently made more spectrum available, and U.S. wireless carriers are still hoping that the FCC will do the same, stated Chris Guttman-McCabe, now Executive Vice President at CTIA – The Wireless Association®. Guttman-McCabe went on to note that if the U.S. wants to remain ahead of the curve and have manufacturers continue to debut mobile devices in the U.S., policymakers must find a way to meet increased demand and release more spectrum.

> “Japan is currently looking to release 300 MHz of spectrum by 2015 with an additional 1,500 MHz by 2020.”

David Jeppsen, Vice President at NTT DoCoMo USA, also stressed the need for additional spectrum, emphasizing the challenge that operators face when it comes to developing forward-looking spectrum technology that can handle the increase in traffic. Jeppsen pointed to Japan as an example of a country that is considering the release of more spectrum to accommodate a pressing data crunch. Japan is currently looking to release 300 MHz of spectrum by 2015 with an additional 1,500 MHz by 2020.

Another hot topic discussed by the panelists was spectrum-sharing between government users and the private sector. Dean Brenner, Senior Vice President – Government Affairs for Qualcomm, Inc., discussed a technology that Qualcomm is currently working on that would enable bandwidth-sharing and allow users to temporarily access the spectrum of other users when it is not otherwise in use. Brenner also suggested that in order to put spectrum to a more rational use, either the industry or the government should come up with ways to incentivize government agencies to share or clear spectrum. Brenner contended that without these incentives for government agencies, extensive spectrum-sharing will be unlikely. During the discussion Reinhard Wieck, Managing Director – Deutsche Telekom, also noted that spectrum licensed for exclusive use also has some efficiency advantages over shared spectrum.

Moderator Michele Farquhar from Hogan Lovells also asked the panelists whether they think that policymakers understand the importance of spectrum. Although most responded that they felt policymakers appreciated the need to make additional spectrum available, some panelists, such as Jeppsen, noted that policymakers can sometimes rely too much on technology. Diane Cornell, Vice President – Government Affairs for Inmarsat plc. also stated that while policymakers understand the importance of spectrum, they have hit a roadblock and are trying to understand and figure out what the sharing and reallocation incentives should be.

Winnik Forum: Technology, Media and Telecommunications M&A: Global Update

While M&A activity in the U.S. and E.U. stalls, there are growing opportunities in the telecommunications sector in developing markets.

Panel Moderators
Dr. Andreas Gruenwald, Hogan Lovells, Berlin
Stephen Kay, Hogan Lovells, Los Angeles

Panelists
Richard Feasey, Public Policy Advisor, Vodafone Group
Mark Johnson, Partner, Carlyle Group
John Krzywicki, Partner, Analysys Mason

Panelists at the Winnik International Telecoms & Internet Forum expect immense merger and acquisition activity in developing markets around the globe, but predict little near-term M&A activity in the United States, where substantial consolidation has already occurred, or Europe, where logistical and business constraints affect consolidation opportunities.

John Krzywicki, partner at Analysys Mason, explained that there is significant international M&A activity in the telecommunications sector. In the wireless market, there are simply too many operators that cannot achieve enough scale to be sufficiently profitable, with the fourth largest operators globally only averaging 2.2% of their national markets. This abundance of providers, according to Krzywicki, has provided significant opportunities for consolidation in developing markets.

While markets with an abundance of carriers with low market shares appear ripe for M&A opportunities, Richard Feasey, Public Policy Advisor with Vodafone Group, observed that although such dynamics exist in Europe, the likelihood of meaningful M&A activity there is meager. According to Feasey, there are many more wireless carriers in each European market than is ideal, leading to sub-optimal returns for even the most profitable carriers. And with disappointing earnings, carriers are unable to invest in next generation wireless networks.

Feasey pointed out that policymakers in Europe hope to encourage the emergence of continent-wide wireless carriers, similar to the largest carriers in the United States, which can achieve greater scale and increase investment in advanced infrastructure. However, carriers are not lining up to expand across the continent because market fragmentation (e.g., advertising, retail) and supply chain fragmentation (e.g., utilities) reduce the opportunity for service providers to benefit from any economies of scale that acquiring a pan-European network could generate.

Carriers themselves would prefer increased consolidation within the individual national markets, rather than across Europe. National consolidation would allow wireless carriers to achieve greater scale in singular markets and achieve greater profits than would be yielded by expansion across Europe – a result that competition regulators in the individual markets are not likely to permit. The solution to the European conundrum, Feasey explained, is for policymakers and regulators to take the long view – allow for consolidation in the national markets and for the strongest national players to acquire and invest in networks across the continent, which would give carriers the ability to generate profit margins necessary to branch out into Europe and build the next generation wireless networks that the European economy will need. But there is little likelihood that any of this activity occurs.

While significant M&A activity in Europe is doubtful in the short-term, Mark Johnson, partner at the Carlyle Group noted that the rest of the world has plentiful opportunities for M&A in the telecommunications sector. As consumers transition from feature phones to smartphones, mobile devices are now outstripping the ability of wireless networks, and as a result, networks are becoming increasingly dependent on the use of Wi-Fi to offload wireless traffic onto fixed networks. Along with the increasing integration of fixed networks and wireless networks through Wi-Fi comes the opportunity for consolidation between the owners of wireless and wireline infrastructure.

The need for additional scale to invest in next generation networks, the glut of small carriers, and the confluence of wireless and wireline networks point toward consolidation; however, the example of Europe shows that these indicators will not always accurately predict increased M&A activity. According to the panelists, M&A opportunities are most robust in markets where decisions by policymakers on a national level (such as the Federal Communications Commission in the U.S.) provide certainty and stability in the regulatory approval process. Furthermore, investors in emerging markets should understand that while there are significant opportunities for M&A, the political and regulatory approval processes in those countries carry greater unknown risks and more uncertainty than transactions in more established markets.

Winnik Forum: Protecting Intellectual Property in a Time of Technological Change

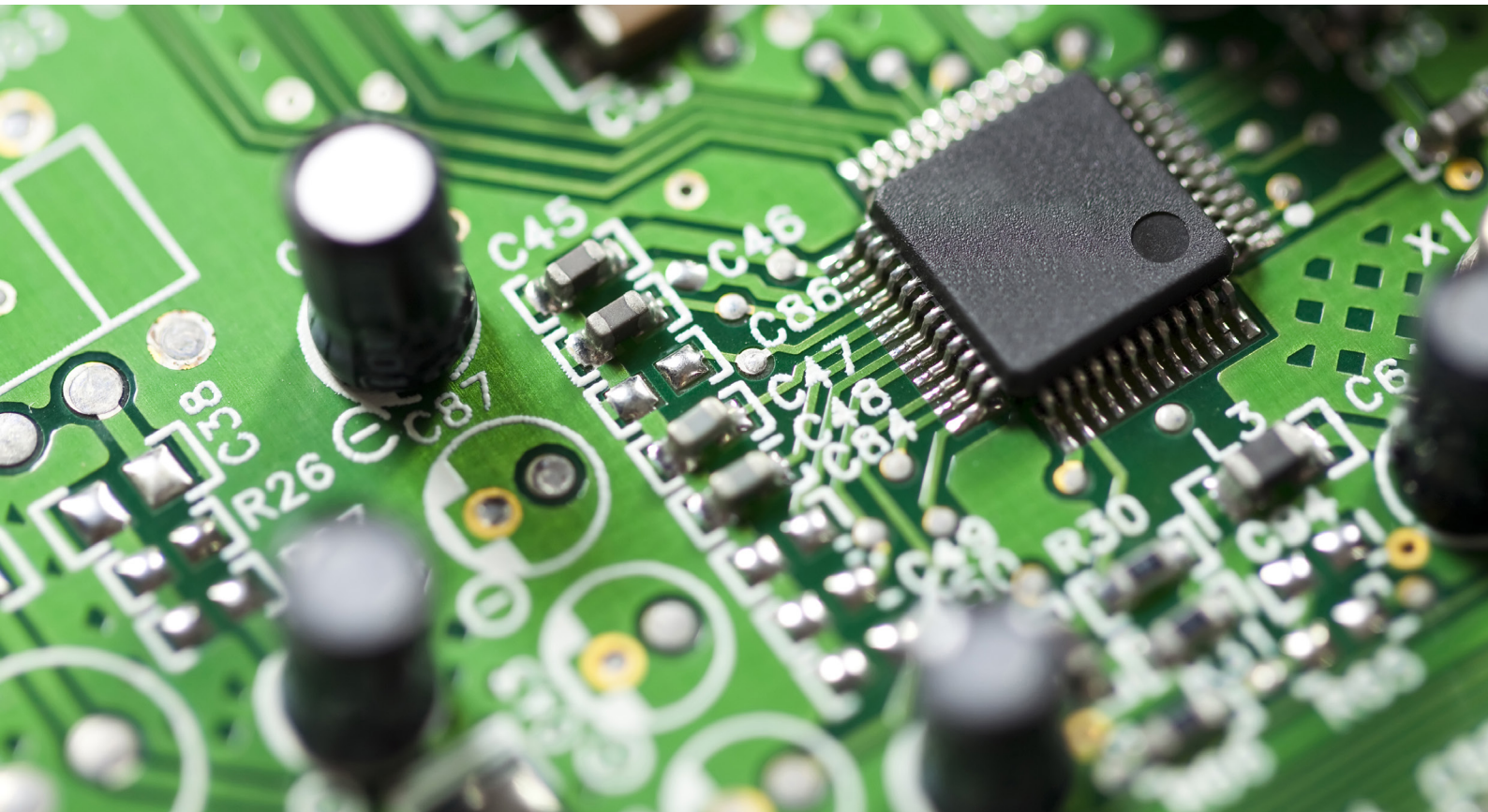
Technological developments continue to challenge traditional intellectual property regimes.

Panel Moderator
Peter Watts, Partner, Hogan Lovells, London

Panelists
Jill Lesser, Executive Director, Center for Copyright Information
Mark MacCarthy, Vice President, Public Policy, Software and Information Industry Association
Gabriela Kennedy, Partner, Hogan Lovells, Hong Kong
Conor Ward, Partner, Hogan Lovells, London
Dr. Andreas Gruenwald, Partner, Hogan Lovells, Berlin

Intellectual property protections have long struggled to keep pace with emerging technologies, and the accelerating evolution of technology today has only made the struggle more challenging. In a panel addressing intellectual property rights in a technically dynamic market, moderator Peter Watts, partner in the Hogan Lovells's London office, noted that it was not until almost 300 years after the invention of Gutenberg's printing press that the first copyright law was implemented. And it was not for another 200 years after that until there was an international agreement protecting copyrighted works. By breaking down physical and social barriers, the current information and technological revolution is spurring change in the content and communications industries in a manner that is seemingly in constant tension with protecting the intellectual property rights of the creative class.

Jill Lesser, Executive Director of the Center for Copyright Information, explained that these innovations have revealed that a new, multistakeholder approach to copyright protection is necessary. The existing legal structures simply were not created with these innovations in content delivery and social networking in mind. Because of these issues, the content community has partnered with Internet Service Providers and formed the Center for Copyright Information. This multistakeholder effort seeks to change norms regarding protecting intellectual property and to help consumers find legal alternatives for enjoying digital content. Through a series of notifications (with each subsequent alert progressing in severity), the Center warns Internet users regarding activity associated with their accounts that potentially violates copyright laws and provides information regarding legal avenues for accessing the content.



Although this alert system is currently only available in the United States, Jill Lesser and Mark MacCarthy, Vice President of Public Policy at the Software and Information Industry Association, explained that this system represented an experiment that, if successful, could be scaled to protect intellectual property throughout the international community. Mark MacCarthy described the approach as one of the most exciting developments in the area in a long time.

As Mark MacCarthy discussed, the Center for Copyright Information system offers a particularly important step in protecting intellectual property: enlisting the intermediary – here, the Internet Service Provider – to protect the content. As little as fifteen years ago, Internet Service Providers were disclaiming any responsibility for pirated content downloaded on their networks; they contended that they were merely operating a conduit into the home and had no control over what information traveled through that pipe. But as the Center for Copyright Information model shows, intermediaries often hold the key to stemming illegal activities, and when they recognize an ethical responsibility to act, big changes can occur.

> “A new, multistakeholder approach to copyright protection is necessary.”

The role of a robust legal system in copyright protection, moreover, cannot be taken for granted, as Hogan Lovells Hong Kong partner Gabriella Kennedy reminded the audience. Voluntary multistakeholder and consumer education efforts can only work if there is a sufficient legal backdrop to penalize wrongdoers, as illustrated in China. Piracy has been a large problem there, in part due to the lack of an effective penalty system for intellectual property violations. Hopefully, as China is undergoing revisions of its copyright law, the government will adopt stronger and more effective penalties to deter would-be violators.

The panelists also discussed the inherent tension between exclusive (i.e., monopoly) intellectual property rights and antitrust law. Conor Ward, partner in Hogan Lovells's London office, illustrated this issue in the context of territorial licensing of satellite broadcasts in the European Union. While there is an effort to promote economic integration throughout the E.U., content owners want to maintain licensing regimes based on territory (i.e., maintain the right to price content differently depending on the country).

This issue came to the fore in the European Court of Justice case, *Football Association Premier League Ltd. v. QC Leisure; and Murphy v. Media Protection Services Ltd.,* Joined Cases C-403/08 and C-429/08, (Oct. 4, 2011). In this case, a United Kingdom pub owner was sued for showing a Premier League football match that she had purchased from a Greek broadcaster. This Greek broadcast was less expensive than that offered by the U.K. broadcaster holding the exclusive U.K. broadcasting rights. In its decision, the European Court of Justice affirmed that territorial licenses are not per se anticompetitive, but it also explained that there is some (unspecified) limit to such differential pricing. And such territorial licensing can be problematic if it is dividing national markets. This decision, however, left many questions unanswered, and panelists agreed that similar problems present themselves in a range of contexts (e.g., variably-priced online streaming rights, transportation of physical goods, such as textbooks, across borders, and others).

Ultimately, panelists recognized that technological developments continue to challenge traditional intellectual property regimes. These trends, when combined with changing government and consumer practices, may make alternative, multi-stakeholder options more attractive – and more important – than ever before.

Winnik Forum: The Challenge of Patent Trolls

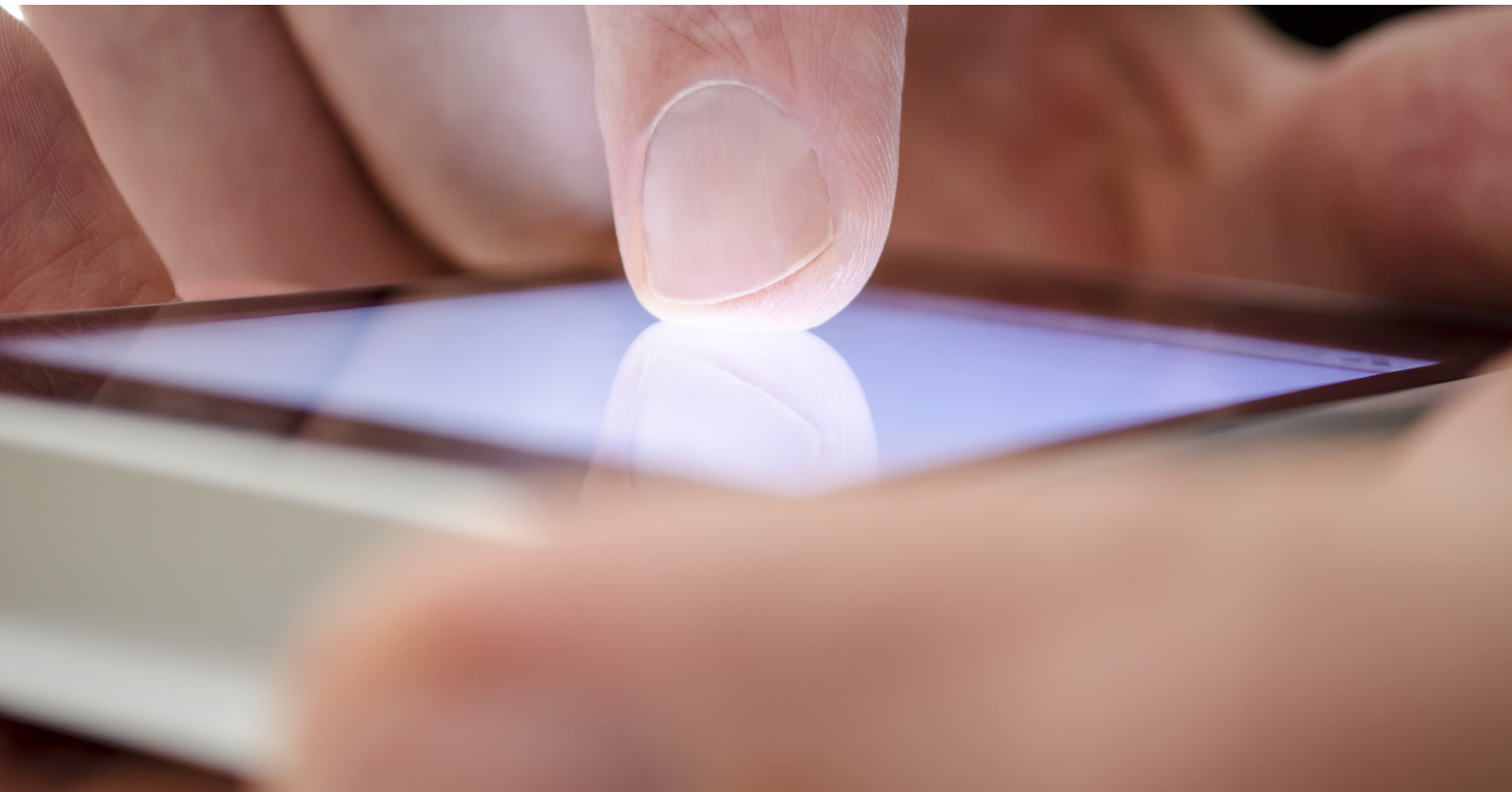
Technology companies increasingly find themselves the target of patent litigation from non-practicing entities.

Panel Moderators
Raymond Kurz, Partner, Hogan Lovells, Washington, D.C.
Trey Hanbury, Partner, Hogan Lovells, Washington, D.C.

Panelists
Jud Cary, Cable Labs
Joshua Lamel, Computer & Communications Industry Association
Dr. Martin Chakraborty, Partner, Hogan Lovells, Dusseldorf

The rise of patent litigation by non-practicing entities ("NPEs"), colloquially known as "patent trolls," has resulted in a "chess game:" companies that rely on patents must employee an interdisciplinary defensive strategy involving litigation, regulatory and legislative fronts, according to Ray Kurz, partner in Hogan Lovells's Washington, D.C. office. As Hogan Lovells partner Trey Hanbury explained, this expensive defensive strategy disproportionately burdens companies in the technology, media, and telecoms industries, as they are the target in three out of every four patent lawsuits.

Joshua Lamel, Vice President of the Computer & Communications Industry Association, noted that all companies, not just technology companies, were vulnerable to patent trolls. Although technology companies have borne the initial brunt of such litigation, the increased implementation of technologies in the operations of non-technological companies has meant that the rest of the commercial world has faced a steadily increasing threat from patent troll litigation. For instance, traditional brick-and-mortar retailers introducing electronic scanning devices to permit customers to check out their own purchases, or retailers implementing online shopping carts to permit online purchases of their products can open up avenues for patent litigation. With respect to technology companies in particular, Lamel points out that the very nature of the products produced by such companies makes them vulnerable. For purposes of comparison, Lamel estimates that a typical smartphone contains components that may be covered by as many as 250,000 patents that could be targeted by a patent troll, while a pharmaceutical product may be covered by only one patent, greatly reducing the opportunity for a patent troll suit.



A surge in patent filings in the 1980s and 1990s combined with an understaffed Patent and Trademark Office ("PTO") that was charged with reviewing applications, created a "perfect storm" for patent litigation, observed Jud Cary, Vice President of Cable Labs. Patent portfolios could then be used as the primary asset for an NPE to launch suits against various companies. Financial decisionmakers encouraged this monetization of patents, which made sense from a financial perspective, but had the unintended consequence of providing more raw materials for NPEs to enter the patent suit business as well as creating a conceptual shift that placed a higher value on the litigation potential of patents rather than a patent's ability to protect innovation.

> "How difficult is it to identify a patent troll pursuing litigation for purely monetary purposes as opposed to a company interested in enforcing its patent to protect its own innovations?"

Hanbury asked whether it was possible to clearly identify the various players as "black hats" and "white hats." In other words, how difficult is it to identify a patent troll pursuing litigation for purely monetary purposes as opposed to a company interested in enforcing its patent to protect its own innovations? Dr. Martin Chakraborty, a partner in Hogan Lovells's Dusseldorf office, noted that in the current environment, no stark "black and white" difference existed. For example, the practice of "privateering," in which an innovating company licenses its patent to an NPE for the purpose of having the NPE enforce its patents on its behalf in exchange for a kickback, blurs that line between black and white. Cary suggested that the line could be drawn between companies protecting their innovations and companies interested in obtaining a financial payout. Lamel agreed that not all privateering is nefarious, but a recent trend of licensing patents to "friendly" companies, while leaving competitors to be sued by the licensor's privateer is troubling, particularly because the defendant company cannot use its own patents to countersue the privateer, which produces no products of its own under the contested patents.

What are the prospects for countering the efforts of patent trolls? The panelists identified a number of initiatives and possibilities:

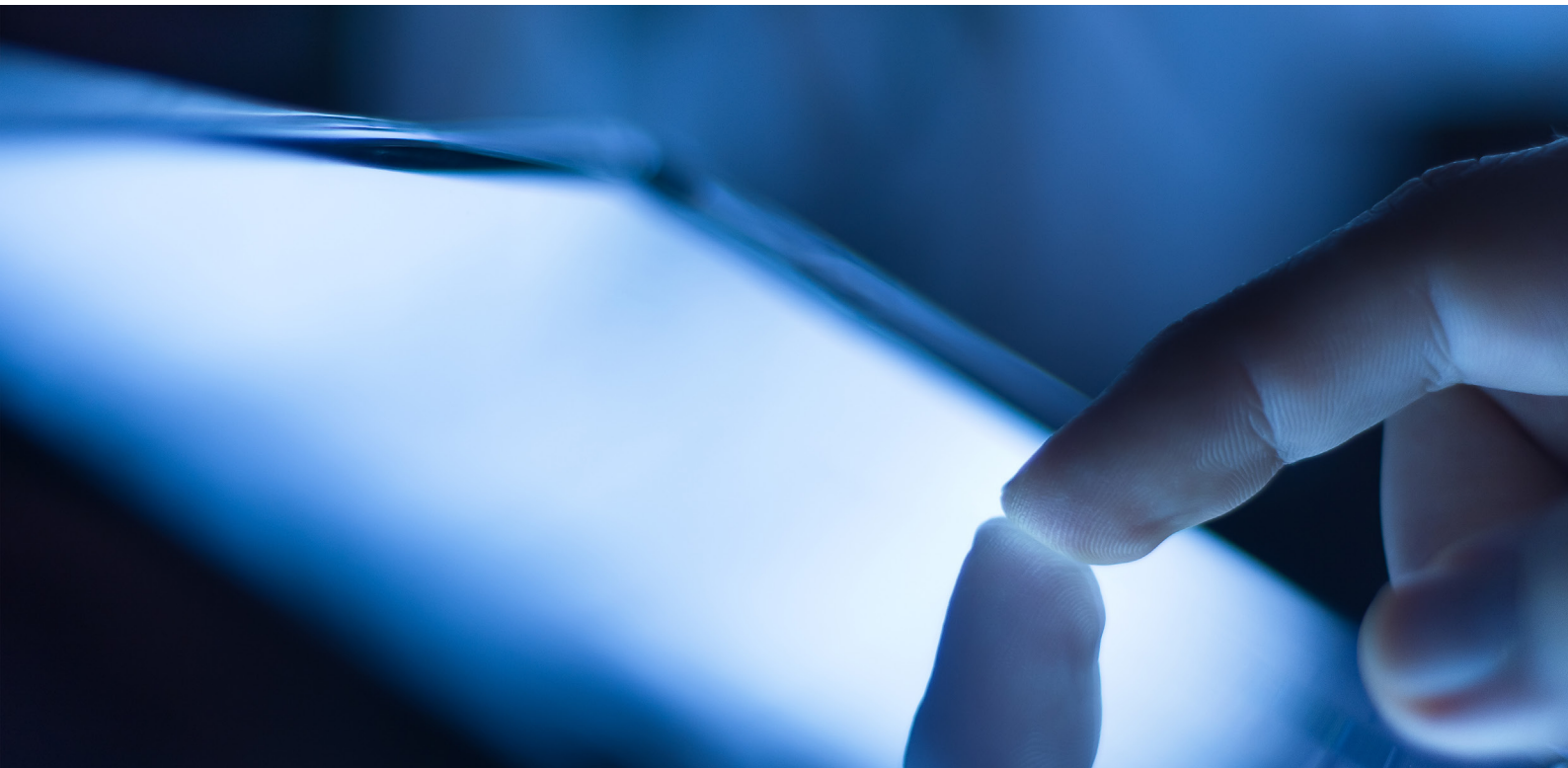
- Cary identified the potential of patent-aggregating coalitions such as Rational Patent Exchange and Allied Security Trust, which acquire patents from distressed companies, to keep patents out of the hands of NPEs. Lamel noted that patent pooling entities have the potential to "deactivate" such loose patents like rogue nuclear weapons, but that there may be antitrust challenges to such activity. Chakraborty countered that there are concerns that such coalitions are too similar to privateer NPEs, however, and also noted that licensing "standard essential patents" under fair/reasonable/nondiscriminatory license terms to participants in standards setting processes may provide additional protections. Nevertheless, Chakraborty also conceded that entities that did not participate in such standards processes would not be affected.
- Hanbury noted that a number of legislative efforts seek to combat patent troll suits. For example, the Saving High Tech Innovators from Egregious Legal Disputes Act of 2013 (the "SHIELD Act"), introduced by Rep. Peter DeFazio (D-OR) and Rep. Jason Chaffetz (R-Utah), would permit a patent litigant to recover the full costs of litigation in the event that the losing party failed to prove that it was the inventor or assignee of the patent, failed to provide documentation that it made a substantial investment in exploiting the patent through the production or sale of a product covered by the patent, or failed to identify itself as an institution of higher learning or an organization created primarily to facilitate the commercialization of technology developed by institutions of higher learning. The aim of the SHIELD Act would be to reduce a major advantage held by patent trolls over operating companies: the lack of disincentive to file patent troll suits due to a

troll's immunity to patent counterclaims coupled with the inherent financial incentives to settle such suits. By way of illustration, there are estimates that the cost to defend a patent suit could range from $1.3-5 million, while the typical settlement amount is in the $200,000 range. An NPE, while still immune from patent counterclaims, would then risk responsibility for the litigation costs in the event of a failed suit.

> The EPO recently undertook an initiative to make the patent registration process more strict.

- Another bill introduced by Sen. Charles Schumer (D-NY) would attempt to reform patent law by expanding the 2011 America Invents Act to permit businesses facing patent suits to request that the (PTO) review patents enforced against them before the lawsuit can proceed in court. The proposed bill expands a current provision in the 2011 act that permits financial services companies to challenge business method patents enforced against such companies via a post-grant review. Sen. Schumer's updated proposal would expand this program to include businesses outside the financial services industry.
- The panelists also identified the need for less ambiguous patents and improved review of patents. Cary noted that while the PTO has been understaffed in the past, the office currently enjoys much improved staff, funding, and expertise to review patent applications. Chakraborty noted that in Europe, the EPO recently undertook an initiative to make the patent registration process more strict, which has increased the quality of patents.

In closing, Kurz suggested that policymakers must go back to basics: national patent regimes should foster progress in science and the arts while working to curtail litigation that frustrates that fundamental purpose.



Winnik Forum: A Trans-Atlantic Dialogue: U.S. – E.U. Free Trade Agreement Negotiations

Successful negotiation of the Transatlantic Trade and Investment Partnership would cover nearly one-third of world trade, and have implications for the future cross-border flow of data.

Panel Moderator
Lewis Leibowitz, Partner, Hogan Lovells, Washington D.C.

Panelists
Jonathan Stoel, Partner, Hogan Lovells, Washington D.C.
Michael Maibach, Senior Fellow, The Aspen Institute
Mark MacCarthy, Vice President for Public Policy, Software & Information Industry Association
Jacquelyn Ruff, Vice President – International, Verizon

In February 2013, the United States and European Union agreed to begin negotiations for a comprehensive trade agreement, the Transatlantic Trade and Investment Partnership (TTIP). Jonathan Stoel, partner in Hogan Lovells's Washington D.C. office, noted that any such agreement would be unprecedented in size and scope. If successful, TTIP would cover nearly one-third of all world trade and account for nearly half of world GDP. A remarkable $2.7 billion of trade flows between the U.S. and the E.U. each day.

> "If successful, TTIP would cover nearly one-third of all world trade and account for nearly half of world GDP."

Jonathan Stoel also discussed the unique, open structure of TTIP. He explained that while TTIP negotiators have set high-level goals, they have until July 2013 to decide the specific issues under discussion and establish a framework for negotiation. In the intervening months, negotiators will reach out to stakeholders for their input on which issues to include and how to structure the negotiations. This presents an exceptional opportunity for industry to shape the debate.

To take advantage of this blank canvas, Michael Maibach, Senior Fellow with the Aspen Institute, proposed a two stage framework, with an "early harvest" of short-term achievable successes to be completed within a year and then a "late harvest" of issues to be concluded thereafter. The "early harvest" issues would be those where the industry in both

the U.S. and the E.U. would exert strong pressure to achieve success on their respective governments. As such, the "early harvest" industries must truly represent a "win-win" situation to prove successful.

However, Michael Maibach warned that even in such "win-win" situations, reaching agreement will prove challenging. He noted that both the E.U. and U.S. have developed bureaucracies and that accepting a proposed agreement will require significant internal coordination by the E.U. Moreover, the parties must work through difficult regulatory harmonization issues or develop a mutual recognition framework that does not allow regulatory forum-shopping.

> "A complete ban on the flow of information is not required to protect privacy."

Focusing on mutual recognition in the privacy context, Mark MacCarthy, the Vice President for Public Policy of the Software & Information Industry Association, noted a recent trend for countries to restrict cross-border data flows because of privacy concerns. Countries are increasingly requiring data be stored within the country's boundaries and prohibiting it from flowing across borders. To counteract this trend, Mark MacCarthy advocated that TTIP establish the principle that a complete ban on the flow of information is not required to protect privacy. Though TTIP should not develop a specific privacy regime, it could agree that where there is a privacy regime with enforceable codes of conduct, there should be a mechanism to allow the free movement of data among nations.

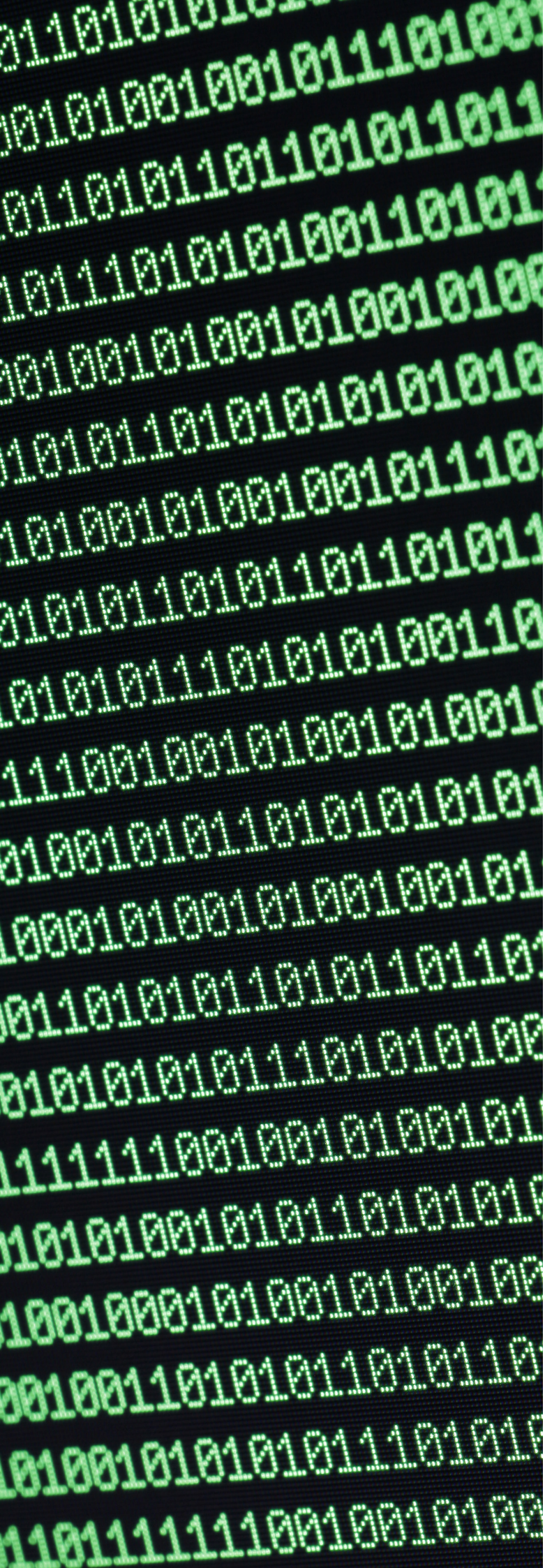
Jacquelyn Ruff, Vice President – International at Verizon, also discussed the need to resolve cross-border privacy concerns in TTIP and suggested an interoperability standard because she viewed complete harmonisation of privacy standards as unlikely. Jacquelyn Ruff also emphasized the need to approach the sector as a true Information and Communications Technology (ICT) sector instead of as distinct regulatory regimes for telecommunications and Internet services to adequately reflect the increasing convergence of the formerly distinct sectors. Jacquelyn Ruff also argued against using rigid classification systems in TTIP, as they quickly become outdated.

The panelists also discussed the importance of TTIP for the global trade regime more broadly. Moderator Lewis Leibowitz, partner in Hogan Lovells's Washington D.C. office, noted that multi-lateral and bi-lateral agreements such as TTIP were becoming more common since the Doha global trade round has stalled. Michael Maibach suggested that a successful TTIP could serve as a model for global trade agreements, potentially even to the extent of using language directly from TTIP in later agreements. Jonathan Stoel echoed these sentiments, noting that if successful, the TTIP process may be expanded to reach new areas.

The panelists concluded by observing that TTIP was likely only the beginning of the process for the ICT sector. Both Jacquelyn Ruff and Mark MacCarthy noted that, if successful, TTIP will likely expand in scope in the face of the industry's rapid change and will require continuous revision and adjustment.

Roundtable #1: Trans-Atlantic Dialogue/U.S.-EU Free Trade Agreement Negotiations

http://hlglobal/sites/Tools/SitePages/VideoPlayer.aspx?vidID=194



International Data Privacy – Delusions of Adequacy: A Critical Assessment of Cross-border E.U. – U.S. Data Transfers*

The key to achieving long-term interoperable E.U. and U.S. privacy standards is a more flexible approach to cross-border data transfers.

This Paper explores the E.U. adequacy mechanism for assessing cross-border data flows and highlights where U.S. law aligns with and differs from the E.U. approach to privacy. Following an Introduction, Part I explains how the E.U. adequacy mechanism works and how it has been applied in practice. Parts II and III then review the case for and against U.S. privacy law being deemed adequate under the E.U. privacy framework. The Paper concludes with some thoughts on how crossborder data flows can be managed as both the U.S. and E.U. contemplate new privacy laws and a new transatlantic trade agreement.

Introduction

The United States and the European Union clearly share a commitment to promoting the rights of individuals to have their personal data protected and to facilitating interoperability of our commercial data privacy regimes.

The European Union and the United States are global leaders in protecting individual freedoms, including privacy, while at the same time fostering innovation and trade that are so critical to the world economy, notably in the present times. Stronger transatlantic cooperation in the field of data protection will enhance consumer trust and promote the continued growth of the global Internet economy and the evolving digital transatlantic common market.

Joint European Statement on Data Protection by European Commission Vice-President Viviane Reding and U.S. Secretary of Commerce John Bryson, Mar. 19, 2012.[1]

In March 2012, the European Commission DG Justice hosted a conference on "Privacy and Protection of Personal Data" that was held simultaneously in Washington, D.C. (at the U.S. Institute of Peace) and in Brussels, in which senior officials of the European Commission, the Obama Administration, the Federal Trade Commission (FTC), NGOs, and corporate representatives participated. As reflected in the agenda[2]

* Chris Wolf presented this paper at the 6th Privacy Law Scholars Conference, June 2013, University of California, Berkeley.

1 http://europa.eu/rapid/press-release_MEMO-12-192_en.htm [hereinafter E.U.-U.S. Joint Statement].

2 http://ec.europa.eu/justice/data-protection/files/eu-us-data-programme_en.pdf.

and in the Joint Statement of European Commission Vice-President Reding and then–U.S. Commerce Secretary Bryson, the focus of the gathering was intended to explore the "common principles" of the two jurisdictions, heralded as "partners," with a focus on "compatibility, compliance and accountability at global scale." The borderless nature of the Internet and the global nature of digital trade was recognized as a strong motivation for common and compatible approaches to the protection of personal data.

Yet, the jointly acknowledged "shared commitment" and "joint leadership," and the need for "stronger transatlantic cooperation" on privacy, have not changed the innate opinion of the relevant European authorities that the U.S. privacy framework is "inadequate," an opinion that hinders or encumbers cross-border data flows and, ultimately, international trade and economic growth. In truth, the U.S. never formally has requested an adequacy determination (beyond that for the limited U.S. – E.U. Safe Harbor framework), likely because of the well-understood outcome: request denied.

Just over a year after the European Commission's March 2012 "charm offensive" at the Institute of Peace session in which a thaw in E.U. – U.S. privacy relations seemed possible, FTC Commissioner Julie Brill went to Brussels to reprise the favorable comparison of the E.U. and U.S. privacy regimes. The speech she gave came at a time when the proposed E.U. Regulation was entering crucial consideration in the European Parliament and when European perceptions of significant (negative) differences between the E.U. and U.S. regimes were intensifying. Commissioner Brill reminded Europeans that there is a "central reality that lies at the interface between E.U. and U.S. privacy law: while many commenters dwell on the significant differences between the E.U. and U.S. privacy regimes, I believe it is important to recognize that we also have much in common."[3]

Indeed, both the U.S. and E.U. privacy frameworks are based on the "Fair Information Practice Principles" (FIPPs), "first articulated in a comprehensive manner in the United States Department of Health, Education and Welfare's seminal 1973 report entitled *Records, Computers and the Rights of Citizens"* and following which "a canon of fair information practice principles has been developed by a variety of governmental and inter-governmental agencies,"[4] such as the privacy guidelines issued in 1980 by the Organization for Economic Co-operation and Development (OECD).[5]

The E.U. and U.S. have taken divergent approaches to implementing the FIPPs.[6] In the U.S., where privacy interests are balanced with the right to free expression, and in recognition of the fact that – as a practical matter – not every piece of personal information can be protected and policed, the framework provides highest levels of protection for sensitive personal information – such as health,[7] financial,[8] and children's[9] information. In addition, targeted enforcement actions against bad (or negligent) actors – principally by the FTC – have created a "common law" of what is expected from business when it comes to the collection, use and protection of personal information. A web of state data security and data security breach notification laws, as well as enforcement actions at the state level in the

> "A canon of fair information practice principles has been developed by a variety of governmental and inter-governmental agencies."

3 Julie Brill, Commissioner, FTC, Remarks to the Mentor Group Forum for E.U.-U.S. Legal-Economic Affairs 1 (Apr. 16, 2013), *available at* http://www.ftc.gov/speeches/brill/130416mentorgroup.pdf.

4 FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 48 n.27 (1998), available at http://www.ftc.gov/reports/privacy3/priv-23a.pdf.

5 OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

6 Christopher Wolf & Winston Maxwell, So Close, Yet So Far Apart: the E.U. and U.S. Visions of a New Privacy Framework, ABA ANTITRUST MAG., Summer 2012, at 8, available at http://law.duke.edu/sites/default/files/images/centers/judicialstudies/Visions_New_Privacy_Framework.pdf.

7 See, for example, the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.), and its implementing regulations.

8 See, for example, the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in scattered sections of 12 and 15 U.S.C.), and its implementing regulations.

9 See, for example, the Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–07, and its implementing regulations.

U.S. have added to the protections for personal data consistent with the FIPPs.

The U.S. privacy framework is far from perfect. New technologies for the collection, combining and sharing of personal data allow some privacy-insensitive businesses to act inconsistently with consumer expectations, or to act with little to no transparency, and even well-intentioned businesses sometimes push the envelope in terms of data collection and use.

The E.U. privacy law regime purports to deal with the U.S. kind of imperfections by providing substantive protections for all personal data. (In reality, however, the broad protections are not matched by E.U. enforcement of those protections.) The European Union's 1995 Data Protection Directive[10] lays out prescriptive rules regarding the processing – including collection, storage, use, and disclosure – of all personal data. The E.U. enacted the Directive following the creation of the Union in large part to harmonize its member states' laws to facilitate the transfer of personal data among member states while ensuring similar levels of data protection. The level of E.U. protection is in furtherance of Article 8 of the Charter of Fundamental Rights of the European Union, which provides;

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.[11]

A major difference between the U.S. and E.U. privacy regimes is the way in which each regulates cross-border data flows. In the U.S., enforcement of privacy protections across borders has "relied on holding those who transfer data accountable for its safe-keeping, and self-regulatory codes of conduct to protect the privacy of personal information that flows across borders."[12] The E.U., on the other hand, has a more formal approach. Article 25 of the Directive generally prohibits transfers of personal data to a third country unless that third country "ensures an adequate level of protection."[13]

The U.S. approach to cross-border transfers is consistent with the OECD's 1980 privacy guidelines that do not require evaluating the "adequacy" of third countries' privacy practices for purposes of data transfer and that specifically addresses the need for countries to facilitate cross-border data transfers.[14] The Asia-Pacific Economic Cooperation (APEC) Privacy Framework, issued in 2005, covers a wide range of privacy protections but does not involve the process of making adequacy determinations. The APEC Privacy Framework instead opts for an accountability principle: "When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles."[15]

That is not to say that the adequacy approach exists solely in Europe. A 2011 review of worldwide privacy laws revealed that 25 of the 29 non-European countries with data privacy laws had "border control data export limitations," although the review notes that the strength of those limitations "varies a great deal, and [the limitations] are not yet in force in the laws of Malaysia and Hong Kong."[16] As one scholar noted, it is no surprise that the adequacy approach has been adopted in many countries because the Directive has had a significant worldwide impact in encouraging "the

10 See Directive 95/46, 1995 O.J. (L 281) 31.

11 Charter of Fundamental Rights of the European Union, *available at* http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

12 Brill, supra note 3, at 5.

13 Directive 95/46, art. 25(1) ("The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.").

14 OECD, *supra* note 5, para. 20 ("Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are *simple and compatible with* those of other Member countries which comply with these Guidelines" (emphasis added)); see also id. para. 20 explanatory memorandum paras. 71–73 (discussing the need for international cooperation)

15 APEC PRIVACY FRAMEWORK 28 (2005), *available at* http://publications.apec.org/publication-detail.php?pub_id=390.

16 Graham Greenleaf, *Do Not Dismiss 'Adequacy': European Data Privacy Standards Are Entrenched,* PRIVACY LAWS & BUS. REP., Dec. 2011, at 16, 17.

rise of omnibus legislation throughout the E.U. and most of the world" modeled on the Directive (including its adequacy mechanism).[17]

Both the U.S. and Europe are considering major overhauls to their respective privacy regimes. In January 2012, the European Commission unveiled a proposed Regulation[18] to supplant the existing Directive. Unlike a directive, which requires each E.U. member state to pass implementing legislation, an E.U. regulation is directly binding on all member states. Thus the proposal seeks to further harmonize E.U. data privacy law by establishing uniform data protection requirements across all E.U. member states. In addition, the proposed Regulation may also add new privacy rights, such as the so-called "right to be forgotten," by which individuals could request that information about them be removed from the Internet entirely.[19]

17 Paul M. Schwartz, The E.U.-U.S. Privacy Collision: A Turn to Institutions and Procedures, 126 HARV. L. REV. (forthcoming 2013); (attributing the spread to "harmonization networks" because worldwide privacy policymaking "has not been led exclusively by the E.U., but has been a collaborative effort marked by accommodation and compromises").

18 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 (Jan. 25, 2012) [hereinafter Proposed Regulation].

19 Id. art. 17; see also infra note 107 and accompanying text.

In February 2012, President Obama unveiled his Consumer Privacy Bill of Rights as part of his administration's comprehensive blueprint to enhance U.S. privacy protections.[20] The Privacy Bill of Rights calls for baseline privacy legislation largely modeled on the FIPPs. Commissioner Brill remarked in her 2013 Brussels speech that the Bill of Rights reflects that "there is always room for improvement," which is why she supports such comprehensive privacy legislation even while recognizing the strength of the existing U.S. framework.[21] Separately, several agencies have recently updated the regulations associated with the privacy laws that they enforce. For example, in December 2012 the Federal Trade Commission updated the regulations protecting children's privacy.[22] And in January 2013, the Department of Health and Human Services released a substantial update to health privacy regulations.[23]

20 WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

21 Brill, *supra* note 3, at 6.

22 *See* Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972 (Jan. 17, 2013) (to be codified at 16 C.F.R. part 312).

23 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 78 Fed. Reg. 5566 (Jan. 25, 2013) (to be codified at 45 C.F.R. parts 160 and 164).

Along with attempting to reshape their individual privacy frameworks, the U.S. and E.U. are working to establish a new trade agreement. In his 2013 State of the Union, President Obama announced that the U.S. and E.U. would begin talks on a comprehensive Transatlantic Trade and Investment Partnership (TTIP),[24] and those talks are expected to begin in the Summer of 2013 and continue for some time. Because modern trade invariably involves the transfer of personal data, the level of U.S. privacy protections and U.S. adequacy as determined by E.U. law likely will be a focus in the negotiations, as the parties attempt to develop a durable trade discipline facilitating the free flow of data while protecting privacy.[25]

> “Now is the time for earnest discussion about how U.S. privacy law compares to E.U. standards.”

Against this backdrop of evolving frameworks and trade negotiations, now is the time for earnest discussion about how U.S. privacy law compares to E.U. standards. This discussion should take into account the inherent cultural, political, and constitutional differences between the two legal systems. The U.S. and E.U. have the opportunity to work towards interoperability and mutual respect by recognizing how both of their approaches to privacy satisfy the core privacy protections embodied in international standards.

24 President Barack Obama, State of the Union Address (Feb. 12, 2013), available at http://www.whitehouse.gov/state-of-the-union-2013.

25 *See, e.g., E.U. Officials Want U.S. to Bolster Data Privacy Protections in Trade Talks*, INSIDE U.S. TRADE, Feb. 21, 2013, available at http://insidetrade.com/Inside-US-Trade/Inside-U.S.-Trade-02/22/2013/eu-officials-want-us-to-bolster-data-privacy-protections-in-trade-talks/menu-id-172.html; Christopher Wolf, *Trade Law and Privacy Law Come Together,* IAPP PRIVACY PERSPECTIVES, Feb. 21, 2013, *available at* http://www.privacyassociation.org/privacy_perspectives/post/trade_law_and_privacy_law_come_together.

I. How the Adequacy Mechanism Works

The E.U. Data Protection Directive generally prohibits transfers of personal data to a third country unless that third country “ensures an adequate level of protection.”[26] Article 26(1) lists six exceptions to the general requirement that a third country ensure an adequate level of protection.[27]

Article 26(2) allows E.U. member states to authorize transfers where “appropriate contractual clauses” are in place to provide “appropriate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights.”[28]

The Directive, under Article 29, established a “Working Party on the Protection of Individuals with regard to the Processing of Personal Data” (the “Article 29 Working Party”). The Article 29 Working Party is responsible for, among other things, giving the European Commission its opinion on the level of protection in third countries.[29] And the European Commission may issue a decision that a third country ensures an adequate level of protection, which is binding on all E.U. member states.[30]

26 Directive 95/46, art. 25(1) (“The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.”).

27 Article 26(1) includes the following six exceptions:

(a) the data subject has given his consent unambiguously to the proposed transfer; or
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject’s request; or
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
(e) the transfer is necessary in order to protect the vital interests of the data subject; or
(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

28 Id. art. 26(2).
29 Id. art. 30(1)(b).
30 Id. art. 25(6).

The Directive provides very broad guidance on how to assess whether a third country ensures an adequate level of protection:

> The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.[31]

The Article 29 Working Party has issued two documents further discussing how adequacy of third countries should be assessed.[32] The Article 29 Working Party states that Article 25 reflects a "case by case approach whereby the assessment of adequacy is in relation to individual transfers or individual categories of transfers."[33] Thus the Article 29 Working Party takes the position that even where a third country is generally deemed adequate, any given data transfer could still be prohibited.[34] And there is nothing to stop the European Commission or an E.U. member state from revoking an adequacy determination at any time.

The Article 29 Working Party has provided additional guidance for making adequacy determinations. The Working Party's broad conclusion is that "any meaningful analysis of adequate protection must comprise the two basic elements: the content of the rules applicable and the means for ensuring their effective application."[35] The Working Party identified six core data protection content principles[36] and three core procedural/enforcement requirements,[37] "compliance with which could be seen as a minimum requirement for protection to be considered adequate."[38] No other guidance has been issued since 1998, so any further observations about what constitutes an adequate level of protection must be adduced from the small number of adequacy determinations issued by the Article 29 Working Party and the European Commission.

As of this Paper's writing, the European Commission has issued thirteen favorable adequacy determinations.[39] The Commission has recognized Andorra, Argentina, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay as ensuring adequate protection for all personal data transfers from the E.U. to those countries. Additionally, the Commission has recognized adequate protection for some types of transfers to Canada[40] and the U.S.[41]

It is worth noting, however, that nineteen European countries that are not part of the E.U. appear to enjoy a de facto adequacy determination. These countries have acceded to both Convention 108[42] and the Additional Protocol,[43] which together require signatories to have

31 Id. art. 25(2).
32 See ARTICLE 29 WORKING PARTY, WP 4, FIRST ORIENTATIONS ON TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES – POSSIBLE WAYS FORWARD IN ASSESSING ADEQUACY (1997); ARTICLE 29 WORKING PARTY, WP 12, WORKING DOCUMENT: TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES: APPLYING ARTICLES 25 AND 26 OF THE E.U. DATA PROTECTION DIRECTIVE (1998) [hereinafter WP 12].
33 WP 12, *supra* note 32, at 26.
34 *See id.* (noting that determinations that a third country generally ensures an adequate level of protection "would be 'for guidance only', and therefore without prejudice to cases which might present particular difficulties").
35 Id. at 5.
36 The content principles are (1) the purpose limitation principle, (2) the data quality and proportionality principle, (3) the transparency principle, (4) the security principle, (5) the rights of access, rectification, and opposition, and (6) restrictions on onward transfers. Id. at 6. The 1998 Working Document also lists three additional principles for certain types of processing: sensitive data, direct marketing, and automated individual decision. Id. at 6–7.
37 The procedural/enforcement principles are (1) to deliver a good level of compliance with the rules, (2) to provide support and help to individual data subjects in the exercise of their rights, and (3) to provide appropriate redress to the injured party where rules are not complied with. Id. at 7.
38 Id. at 5.
39 See European Commission, Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries, http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (last visited May 1, 2013). Separately, the European Union has entered into agreements with Australia and the United States to allow the transfer of Passenger Name Record data by air carriers.
40 The Commission has recognized as adequate Canada's handling of Passenger Name Record (PNR) data and transfers to recipients subject to the Personal Information Protection and Electronic Documents Act (PIPEDA). See Commission Decision 2006/253, 2006 O.J. (L 91) 49 (PNR); Commission Decision 2002/2, 2002 O.J. (L 2) 13 (PIPEDA).
41 The Commission has recognized that the Safe Harbor Framework ensures an adequate level of protection. *See infra* note 97 and accompanying text.
42 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Eur. T.S. No. 108 [hereinafter Convention 108].
43 Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows, Nov. 8, 2001, Eur. T.S. No. 181 [hereinafter Additional Protocol].

laws that meet all the key requirements of the EU Directive.[44] Thus, as one scholar notes, "no such country has bothered to apply for a[n] adequacy finding, even though they are the most likely countries to be successful" because "there is, in practice, simply no need for an adequacy declaration."[45] And "the E.U. has in most cases awaited requests from third countries to initiate the process" of adequate determinations.[46]

Other factors have contributed to the low number of published adequacy determinations. Several commentators have noted that the E.U. could be "more pro-active and more transparent about its processes."[47] For example, the E.U. does not generally publish negative or unfavorable adequacy determinations.[48] The Article 29 Working Party has never made a negative adequacy opinion public, and the only published negative opinions come from external consultants.[49] The pool of adequacy opinions providing guidance therefore is quite limited.

A review of some of the published adequacy determinations reveals some trends and potential inconsistencies in how the adequacy mechanism has been employed in practice. For example, New Zealand is the most recent country to be deemed to ensure an adequate level of protection.[50] But Professor Greenleaf notes that the Article 29 Working Party opinion on New Zealand's adequacy "found seven instances of where New Zealand's content principles were not fully 'adequate.'"[51] Most noteworthy among these is that the Article 29 Working Party had concerns with New Zealand's restrictions on onward transfers to other countries (*i.e.,* New Zealand's adequacy mechanism) and concluded that New Zealand law did not comply fully with the EU Directive on this point.[52] Yet the Article 29 Working Party seemed to downplay this concern due to New Zealand's "geographical isolation," "the size and the nature of its economy," and the low probability that "significant volumes of E.U.-sourced data" would be transferred to third countries.[53]

In effect, the Article 29 Working Party's opinion on New Zealand's adequacy may highlight a tale of two standards. The decision reflects an underlying rationale along the lines of "[i]t will be relatively rare that personal data on EU citizens ends up in New Zealand, so a good deal of tolerance of variation from the core principles previously set out by the Working Party is permitted by them in delivering an adequacy opinion."[54] Meanwhile, "[i]n a country like India, where outsourcing of the processing of European data is of large scale, as are other forms of business and travel involving personal data, different considerations are likely to apply."[55] Professor Greenleaf concludes that the Article 29 Working Party's opinion reflects "significant pragmatic preparedness on the part of the Working Party."[56] But the opinion may also be seen to illustrate a different standard for large- versus small-scale data-processing countries when seeking adequacy determinations.

Argentina's favorable adequacy determination illustrates another nuance in the E.U.'s approach to adequacy. Argentina passed its comprehensive privacy law in October 2000, issued an implementing/clarifying regulation in December 2001, and then requested an adequacy determination from the E.U. in January 2002. In October 2002,[57] the Article 29 Working Party released its favorable adequacy opinion,[58] and in June 2003 the European Commission decided that Argentina ensured an adequate level of protection.[59]

44 *See, e.g.,* Convention 108, ch. II (laying out privacy safeguards and data subject rights akin to E.U. Directive); Additional Protocol, art. 1 (requiring DPA); id. art. 2 (requiring adequacy determinations for nonparties to Convention 108).
45 *See* Greenleaf, *supra* note 16, at 17.
46 Alex Boniface Mukalilo, *Data Protection Regimes in Africa: Too Far from the European 'Adequacy' Standard?*, INT'L DATA PRIVACY L., Nov. 2012, at 8.
47 Greenleaf, supra note 16, at 17.
48 Id.
49 Mukalilo, supra note 46, at 8.
50 Commission Decision 2013/65, 2013 O.J. (L 28) 12.
51 Graham Greenleaf, *Not Entirely Adequate But Far Away: Lessons from How Europe Sees New Zealand Data Protection*, PRIVACY LAWS & BUS. REP., July 2011, at 8, 8.
52 ARTICLE 29 WORKING PARTY, WP 182, OPINION 11/2011 ON THE LEVEL OF PROTECTION OF PERSONAL DATA IN NEW ZEALAND 9–10 (2011).
53 Id. at 10 ("In reality, given the geographical isolation of New Zealand from Europe, its size and the nature of its economy, it is unlikely that New Zealand agencies will have any business interest in sending significant volumes of E.U.-sourced data to third countries.").
54 Greenleaf, supra note 51, at 9.
55 Id. at 3.
56 Id. at 2.
57 ARTICLE 29 WORKING PARTY, WP 63, OPINION 4/2002 ON THE LEVEL OF PROTECTION OF PERSONAL DATA IN ARGENTINA 2–3 (2002).
58 Id.
59 Commission Decision 2003/490, 2003 O.J. (L 168) 19.

The Article 29 Working Party gave a favorable opinion on Argentina's adequacy despite substantial concerns with its procedural/enforcement mechanisms. For instance, the Working Party expressed concern that the DPA was not guaranteed independence and lacked jurisdiction over all data controllers and processors.[60] And the Working Party noted that it relied heavily on the Argentinean Government's assurances with respect to how the law was being implemented.[61] Thus, the Working Party concluded by stressing that its opinion was "drafted on the basis of these assumptions and explanations and in the absence of any substantial experience with the practical application of the legislation."[62]

This conclusion stands in stark contrast to more recent adequacy opinions commissioned by the European Commission. For example, Burkina Faso was among four African countries that recently sought adequacy determinations from the E.U.[63] The advisory opinion on Burkina Faso's adequacy "refrained from giving its conclusion whether Burkina Faso provides an 'adequate level of protection of personal data."[64] It based this decision in part on the opinion that "'the existence of actual enforcement mechanisms is an important part of the criteria to meet before being possibly considered as a country offering an adequate protection in the sense of article 25.'"[65] Yet the Article 29 Working Party offered a favorable opinion as to Argentina at a time when Argentina's DPA had issued no significant guidance and pursued no enforcement. Indeed, Argentina's low number of enforcement actions to date, coupled with insight gleaned from discussions with Argentinean practitioners, suggest that Argentina may still lack effective enforcement mechanisms in practice – even if effective mechanisms exist on paper.

Another issue with the adequacy mechanism is the potential for the process to become politicized. The Article 29 Working Party itself recognized the potential for political tensions surrounding adequacy determinations, noting that "some third countries might come to see the absence of a finding that they provided adequate protection as politically provocative

60 ARTICLE 29 WORKING PARTY, supra note 57, at 14.
61 Id. at 17.
62 Id.
63 Mukalilo, supra note 46, at 1–2.
64 Id. at 4.
65 Id. at 5 (quoting advisory opinion).

or at least discriminatory, in that the absence of a finding is as likely to be the result of their case not having been examined as of a judgment on their data protection system."[66] According to Mukalilo, this is why the E.U. generally avoids releasing negative adequacy opinions.[67] More troubling, although ultimately of no effect, was Ireland's objection in 2010 to the adequacy determination for Israel. After Israel received a favorable adequacy opinion from the Article 29 Working Party, Ireland officially objected and delayed the European Commission's decision.[68] Ireland raised its objection ostensibly based on minor concerns with the Israeli protections for manual data processing and the DPA's independence.[69] But Ireland admitted to making an objection for reasons wholly unrelated to privacy, as it was outraged by the use of fake Irish passports by alleged Israeli agents in a targeted killing.[70] Use of the adequacy mechanism to achieve unrelated political ends could threaten the legitimacy of the system and undermine third countries' confidence that their privacy regimes were being evaluated purely on the merits.

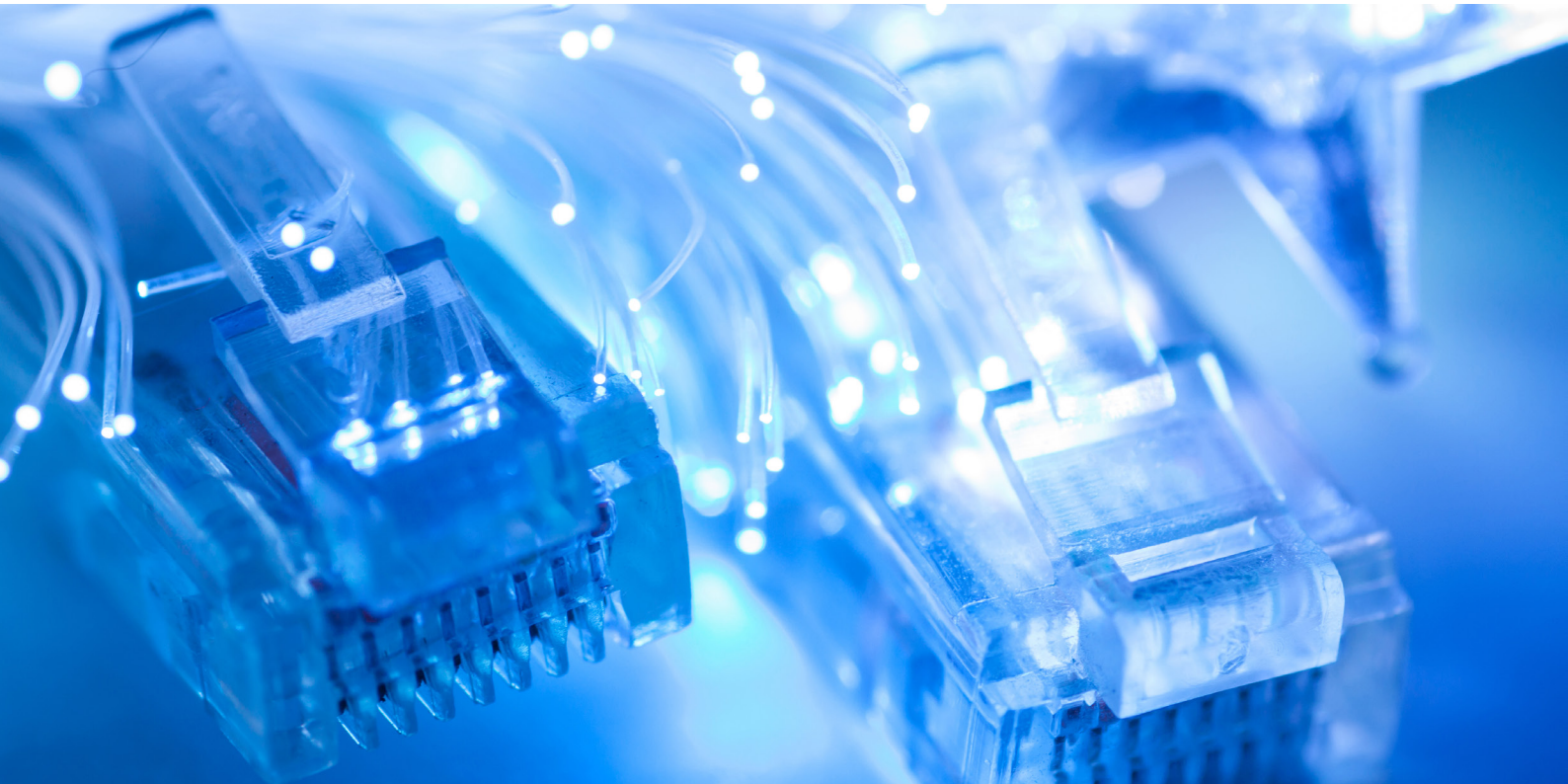
66 WP12, *supra* note 32, at 27.
67 Mukalilo, supra note 46, at 8.
68 Laurence Peter, *Ireland Delays E.U. Deal with Israel on Data Transfers*, BBC NEWS (Sept. 3, 2010), available at http://www.bbc.co.uk/news/world-europe-11176926.
69 Id.
70 Id.

We are in the early days of modern international data privacy law – privacy law that addresses the use of technology, and it is understandable why the form of a nation's privacy law regime has been used as a convenient surrogate for adequacy. But now that multiple national regimes have had the chance to mature, and regulators in Europe have had a decade or more to observe them, it's reasonable and desirable for the Article 29 Working Party to apply the full-factors approach that E.U. law allows them to use in recommending adequacy.[71]

II. The Case for U.S. Adequacy

It has been said that the United States and England are two countries separated by a common language. Something similar can be said with respect to the U.S. and E.U. when it comes to privacy: both the U.S. and Europe fundamentally agree on the need for privacy protections and the core tenets of what those protections look like. The differences are largely in form, not substance.

71 The European Commission itself has had very few opportunities directly to consider adequacy and to bring the full range of stakeholder interests to bear in consideration of adequacy.



Privacy law worldwide has evolved from a set of core principles. As discussed earlier, the 1980 OECD privacy guidelines identified eight FIPPs to guide all data collection, use, and disclosure.[72] The OECD guidelines were formally ratified by 24 OECD member countries, including the U.S. and many European nations. These eight FIPPs have been highly influential in the development of privacy laws and regulations worldwide. The FIPPs form the foundation of almost every nation's information privacy protections, including both the U.S. and the European Union's privacy regimes.[73] Historically, however, the E.U. and the U.S. have taken divergent approaches to implementing the FIPPs.

In the U.S., the legal framework for information privacy has focused on providing protections tailored to specific areas of concern, such as health records and children's personal information. This sectoral approach, with its focus on sensitive personal information, has deep roots in American law. In large part, it reflects that privacy interests are balanced with competing interests, such as the right to free speech and respect for free-market solutions.

The U.S. passed one of the very first privacy laws back in 1970, ten years before the OECD privacy guidelines, when Congress enacted the Fair Credit Reporting Act (FCRA).[74] At the time, there was widespread concern with how credit reporting agencies would use the vast troves of information becoming available through automated processing of credit transactions. (Remember that computing was still in its infancy, and thus the ability to computerize record-keeping was just starting to revolutionize society.) As a result, Congress passed the FCRA to ensure the accuracy, fairness, and privacy of personal information assembled by the credit reporting agencies.

The next major U.S. privacy law came as a result of the Nixon administration's privacy abuses. Mere months after Nixon's resignation, Congress enacted the Privacy Act of 1974 to apply the FIPPs to U.S. federal agencies' collection, storage, use, and disclosure of the personal information of U.S. citizens.[75]

Starting in the 1980s, Congress enacted a series of privacy laws targeting specific sectors. These laws often passed in response to publicized incidents demonstrating a lack of privacy protections in a certain sector. For example, Congress enacted the Electronic Communications Privacy Act of 1986[76] in response to concerns with electronic surveillance technologies. Then in 1988, Congress enacted the Video Privacy Protection Act[77] after a reporter published the video rental records of Robert Bork, at the time a Supreme Court nominee.

The 1990s saw the passage of several blockbuster privacy laws in the U.S. Congress enacted laws addressing health privacy, financial privacy, and children's privacy.[78] In each area, Congress enacted legislation that also called for the appropriate federal agencies to enact accompanying regulations fleshing out the details of the law. For example, Congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA) with minimal detail regarding health privacy protections. But the law called on the Department of Health and Human Services to enact a detailed Privacy Rule. This hybrid law-and-regulation approach has allowed Congress to pass high-level privacy guidance for a specific sector, and give the federal agency with sector-specific subject matter expertise the authority to elaborate the nuances and address the low-level implementation details.

Perhaps the most significant legislative action on privacy in the U.S., however, has come through state data breach notification statutes. California passed the first such law,[79] in the early 2000s, and now almost every state, commonwealth, and territory in the U.S. has a similar statute.[80] Generally speaking, these laws require entities to notify affected individuals

72 See OECD, *supra* note 5, paras. 7–14 (identifying the eight FIPPs as collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability).

73 See, e.g., John W. Kropf, Independence Day: *How to Move the Global Privacy Dialogue Forward*, BLOOMBERG BNA PRIVACY & SECURITY LAW, Jan. 2008 ("The Guidelines have been highly influential, and are at the heart of most countries' privacy legislation . . . .").

74 Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, tit. VI, 84 Stat. 1114, 1128 (codified as amended at 15 U.S.C. §§ 1681–81x).

75 Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a).

76 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–22).

77 Video Privacy Protection Act, Pub. L. No. 100-618, 102 Stat. 3195 (1988) (codified as amended at 18 U.S.C. § 2710).

78 *See supra* notes 7–9.

79 See CAL. CIV. CODE § 1798.29.

80 See Nat'l Conference of State Legislatures, State Security Breach Notification Laws, http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx (last visited May 1, 2013) ("Forty-six states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.").

and/or regulators whenever entities experience a data breach. A data breach can include losing a computer or flash drive containing personal information, having an employee steal personal information to commit identity theft, or experiencing an attack that results in hackers gaining access to company databases.

The effect of these laws cannot be overstated. According to the Privacy Rights Clearinghouse, since 2005 over 3,700 breaches involving over 600 million compromised records have been reported under these state laws.[81] Breach notification laws have resulted in greater transparency into entities' privacy and security practices, as well as raising consumer interest in privacy protections. There are obvious costs associated with a data breach, such as the money spent investigating and reporting the incident, and the costs associated with providing affected individuals with credit monitoring services.[82] Companies suffering a data breach also pay a reputational penalty, as consumers are less likely to trust the company with their business in the future.[83] The result has been an incredible increase in attention paid to preventing data breaches, with a resulting increase in privacy protections across the board.

U.S. privacy protections, however, are not limited to specific laws and regulations. The Federal Trade Commission (FTC) has played an increasingly active role in shaping what privacy protections are expected for all U.S. businesses. The FTC Act gives the FTC authority to regulate all "unfair or deceptive practices or acts in or affecting commerce."[84] Starting in the 2000s, the FTC began to invoke this authority to govern companies' privacy practices. Commissioner Brill has stated that "privacy protection is 'mission critical'" at the FTC.[85]

81 See Privacy Rights Clearinghouse, Chronology of Data Breaches, http://www.privacyrights.org/data-breach (last visited May 1, 2013) (providing a list of disclosed breaches).
82 See PONEMON INSTITUTE, 2011 COST OF DATA BREACH STUDY (2012), available at http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-cost-of-a-data-breach-2011 (noting that the average breach results in a cost of approximately $200 per compromised record).
83 ADVISEN, THE REPUTATIONAL RISK OF DATA BREACH 4 (2012), *available at* http://corner.advisen.com/pdf_files/Reputational_Risk_Data_Breach_2012NAS.pdf.
84 See 15 U.S.C. § 45.
85 Brill, *supra* note 3, at 2.

The FTC has acted through two mechanisms. First, the FTC has brought hundreds of enforcement actions concerning privacy.[86] The earliest actions focused on holding companies to the promises included in their online privacy policies; violation of a privacy promise constituted a deceptive practice under the FTC Act. Increasingly, however, the FTC has invoked its unfairness authority to affirmatively state what privacy practices are reasonably expected for all companies. Recent FTC enforcement actions have resulted in settlements whereby the company agrees to implement a comprehensive and auditable privacy program.

> "The FTC has brought hundreds of enforcement actions concerning privacy."

Second and complementary to its enforcement efforts, the FTC has increasingly sought to provide companies guidance on privacy best practices. To that end, the FTC has published a series of reports, most recently on issues regarding privacy in mobile apps. In March 2012, the FTC also published a fairly comprehensive guide to privacy best practices.[87] And the FTC has convened workshops to promote broad discussions regarding privacy issues. These workshops bring together the regulators, company and industry representatives, and privacy advocates to debate the appropriate privacy safeguards that should be considered best practices. These workshops often result in publication of reports or guidelines summarizing the FTC's advice – which then become the baseline by which the FTC brings future enforcement actions.

86 For a listing of the FTC's enforcement actions, see FTC Bureau of Consumer Prot., Legal Resources, http://business.ftc.gov/legal-resources/all/35 (last visited May 1, 2013).
87 See FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

The net impact of the FTC's two mechanisms has been to raise the privacy floor. Companies doing business in the U.S. are now expected to have published privacy policies and privacy programs – even though no federal law imposes these requirements on the vast majority of businesses (with the exception of companies operating in highly regulated sectors, such as healthcare). And the thousands of companies that have self-certified to the Safe Harbor Framework[88] (which allows personal data to be transferred from the E.U. to the U.S., as discussed below[89]) have both imposed these requirements on themselves and subjected themselves to FTC enforcement.

There are also significant extra-legal forces operating in the U.S. that contribute to providing broad privacy protections. For example, the past fifteen years has seen an explosion in companies hiring Chief Privacy Officers (CPOs). In 2000, the few companies that had created CPO positions actually issued press releases announcing their actions.[90] Now there are thousands of CPO positions at companies across the U.S. The existence of a C-level position focused on privacy elevated corporate America's focus on privacy and resulted in substantial increases in time and resources devoted to privacy protections.

The privacy profession has been further enhanced through professional associations. A professional organization known as the International Association of Privacy Professionals (IAPP), formed in 2000 to provide a venue for CPOs to discuss privacy issues and share best practices. In early years, the IAPP had conferences where tens of CPOs would gather to share knowledge. For the 2013 Global Privacy Summit,[91] over 2,000 people were in attendance. The organization now boasts nearly 10,000 members in the U.S. alone, and provides numerous certifications for individuals seeking to establish their credentials as privacy professionals in the marketplace.

88 See, e.g., E.U.-U.S. Joint Statement, supra note 1 (noting that "over 3,000 companies have self-certified" to the Safe Harbor Framework).
89 *See infra* notes 95–97 and accompanying text.
90 See, e.g., Press Release, IBM, IBM Names Harriet P. Pearson as Chief Privacy Officer (Nov. 29, 2000), available at http://www-03.ibm.com/press/us/en/pressrelease/1464.wss.
91 See IAPP, Global Privacy Summit 2013, https://www.privacyassociation.org/events_and_programs/global_privacy_summit_2013 (last visited May 1, 2013).

There are also numerous privacy lawyers – working with policymakers, engineers, and others – engaged in privacy compliance advice, representation, advocacy, and scholarship. Privacy law articles have influenced privacy professionals and policymakers alike. The field of privacy law itself originated with the seminal law review article by Warren and Brandeis on *The Right to Privacy*.[92] Privacy advocacy groups also play a significant role in enforcement. Companies often pay a monetary penalty when settling FTC enforcement actions, and these settlements typically include money contributions to various privacy advocacy groups for use in educational efforts. As a result, privacy advocacy groups have been able to increase their advocacy efforts, as well as their oversight capacity. Indeed, many FTC enforcement actions start with complaints filed by these very advocacy groups, which leads to a feedback loop of increasing funding for these advocacy groups to serve as privacy watchdogs.

Finally, litigation has served as a backstop to keep pressure on companies to implement and maintain robust privacy programs. These days, a company announcement of a data breach or media reports on a privacy slip-up frequently results in the filing of class-action lawsuits within days of the news. While these class-action suits on the whole have not been generally successful in establishing liability and damages,[93] they have provoked numerous settlements from companies averse to public litigation with customers. The cases increase the bottom-line costs that companies weigh in deciding how they allocate their resources and that weighing means increased attention to privacy programs.

Berkeley Professors Ken Bamberger and Deirdre Mulligan have extensively researched the role that extra-legal forces play in protecting privacy. In their landmark study of privacy "on the ground," they interviewed several CPOs to assess the state of privacy protections in the U.S.[94] Their findings suggest that the extra-legal forces described above, coupled with the various laws and regulations on the books, have resulted in privacy becoming more embedded into U.S. corporate culture and business operations. More importantly, their research suggests that formalistic reviews of privacy "on the books" might substantially underestimate the strength of a third country's privacy protections overall.

III. So Why Isn't the U.S. Considered Adequate?

Despite the many layers contributing to robust privacy protections in the U.S., the E.U. continues to view the U.S. privacy framework as inadequate under E.U. law – although the issue has never been squarely addressed, as the U.S. has never applied for a finding of adequacy and the E.U. has never stated that it has denied or would deny any U.S. application. When the Directive entered into force in 1998, however, it was widely accepted that the U.S. lacked adequate privacy protections to qualify as adequate under E.U. law.[95] Thus the U.S. and E.U. promptly began negotiating a way for U.S. businesses to be able to engage in certain international data transfers involving E.U. personal data. The U.S. goal was to create a "safe harbor" under which some U.S. businesses could receive E.U. personal data. The challenge, however, was to bridge the gap between two very different approaches to privacy protections.

> "The Safe Harbor Framework has facilitated cross-border data transfers for thousands of companies."

92 See Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193 (1890).

93 But see Des Hogan, Michelle Kisloff, Christopher Wolf & James Denvil, *Regulators and Plaintiffs' Lawyers Are Ready to Pounce on Privacy and Data Security Missteps: A Guide to Limiting Corporate Risk*, BLOOMBERG BNA PRIVACY & SECURITY LAW REPORT, 12 PVLR 586, Apr. 8, 2013, available at http://www.hldataprotection.com/files/2013/04/PDFArtic.pdf (noting that "[t]he plaintiffs' bar has won a string of recent victories in privacy class actions, which could light a path for others seeking to bring similar cases").

94 See Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011).

95 See, e.g., ARTICLE 29 WORKING PARTY, WP 15, OPINION 1/99 CONCERNING THE LEVEL OF DATA PROTECTION IN THE UNITED STATES AND THE ONGOING DISCUSSIONS BETWEEN THE EUROPEAN COMMISSION AND THE UNITED STATES GOVERNMENT 2 (1999) ("[T]he Working Party takes the view that the current patchwork of narrowly-focused sectoral laws and voluntary self-regulation cannot at present be relied upon to provide adequate protection in all cases for personal data transferred from the European Union.").

It took two years of negotiating, but eventually both sides reached an agreement that was acceptable to all. The result was the Safe Harbor Framework.[96] The framework requires eligible companies to certify their compliance with seven broad principles: notice, choice, restrictions on third-party transfers, security for personal data, data integrity, individual access rights, and submission to the FTC's jurisdiction for enforcement purposes. In 2000, the European Commission recognized that the Safe Harbor Framework ensured an adequate level of protection under the E.U. Directive,[97] and the Safe Harbor Framework has facilitated cross-border data transfers for thousands of companies in the intervening years.

Only companies subject to the jurisdiction of the FTC are eligible for participation in the Safe Harbor (as the FTC is the agency charged with enforcing Safe Harbor principles). Thus, broad swaths of U.S. commerce, including transportation companies, communication common carriers, certain regulated financial services firms, and non-profits, are not eligible to participate in the Safe Harbor.

After the 9/11 attacks, the U.S. and E.U. entered into a separate arrangement providing for sharing of airline passenger information involving E.U. personal data.[98] This second agreement allowed for the transfer of Passenger Name Records to U.S. government authorities for anti-terrorism purposes.

These are the two primary agreements existing between the U.S. and E.U. regarding international data transfers.[99] As previously noted, the U.S. has never formally sought a full adequacy determination, but it's no secret that the E.U. sees major shortcomings in the U.S. regime. The principal perceived shortcomings are that the E.U. generally disfavors a sector-by-sector approach, instead viewing comprehensive legislation as the superior method to ensure privacy protections. And the E.U. considers the lack of an independent data protection authority to be a serious shortcoming.

Some in the E.U. also criticize the effectiveness of the Safe Harbor.[100] These criticisms arise despite the European Commission's continuing support for the Safe Harbor Framework's adequacy, which was reaffirmed even after the release of the proposed Regulation.[101] And evidence suggests that the Safe Harbor Framework has played a key role "in raising privacy awareness and acceptance of privacy protection in the U.S."[102]

The sectoral approach that has received European criticism has some advantages that may be underappreciated in Europe. For example, U.S. privacy law has been tailored across sectors to provide varying levels of protection appropriate for the sensitivity and use of personal information. This flexibility also permits quicker changes in response to new threats to privacy, without having to establish rigid protections that prevent flexibility. As to health privacy in the U.S., for example, a detailed and robust framework exists under HIPAA and HITECH.

> "The E.U. continues to view the U.S. privacy framework as inadequate under E.U. law."

96 The U.S. government maintains all documentation associated with the U.S.-E.U. Safe Harbor Framework online at http://export.gov/safeharbor/eu/eg_main_018365.asp.

97 See Commission Decision 2000/520, 2000 O.J. (L 215) 7.

98 See Commission Decision 2007/551, 2007 O.J. (L 298) 29.

99 There have been other discussions and understandings reached regarding specific types of transactions, such as data transfers for anti-terrorism purposes, but these are beyond the scope of this Paper.

100 See, e.g., Peter Schaar, Transatlantic Free Trade Zone? But Only When the U.S. Provides Improved Data Protection!, German Federal Commissioner for Data Protection and Freedom of Information Blog, Feb. 13, 2013, http://www.bfdi.bund.de/EN/PublicRelations/SpeechesAndInterviews/blog/TransatlanticFreeTradeZone.html?nn=1269676.

101 See E.U.-U.S. Joint Statement, *supra* note 1 ("[T]he United States and the European Union reaffirm their respective commitments to the U.S.-E.U. Safe Harbor Framework. This Framework, which has been in place since 2000, is a useful starting point for further interoperability."). Note, however, that the official Rapporteur for the proposed Regulation proposed that there be a regular reevaluation of the Safe Harbor arrangement. *See* JAN PHILIPP ALBRECHT, RAPPORTEUR, DRAFT REPORT ON THE PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON THE PROTECTION OF INDIVIDUAL WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA (GENERAL DATA PROTECTION REGULATION) 144–47 (2013), available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.

102 Damon Greer, *Safe Harbor – A Framework that Works*, 1 INT'L DATA PRIVACY L. 143, 147 (2011).

The E.U. believes that the U.S. affords too much governmental access to personal data and that also affects its view of the U.S. privacy framework. These concerns are rooted in the powers authorized by the USA PATRIOT Act, which was passed after the 9/11 attacks. It is true that the Patriot Act provides the U.S. government with authority to access personal data in certain situations. But the E.U. is wrong to paint the U.S. government's access as exceptional. A legal review of ten different countries across the globe assessed their governments' level of access to information stored in the cloud.[103] The survey included the U.S., several European countries, Canada, Australia, and Japan. The results were clear: all ten countries permitted their governments similar levels of access to data stored in the cloud in the interests of national security and law enforcement. But several countries actually enabled entities to voluntarily share such information with the government, without legal protections – and the U.S. was not one of them.[104]

Finally, the E.U. criticism of the lack of a centralized enforcement authority for privacy in the U.S. should not be dispositive. The FTC has broad but not unlimited jurisdiction to police privacy violations in the U.S. Influential scholars have made the case that enforcement efforts in the U.S. are very strong.[105] This is especially so when one considers the robust and increasing enforcement activity at the state level.[106]

Complicating matters, however, is the potential for greater separation between the U.S. and E.U. privacy regimes once the E.U. adopts the proposed Regulation. The proposed Regulation includes several elements not reflected in current or proposed U.S. law. For example, the proposed Regulation would give individuals a "right to be forgotten," which would allow individuals

103 See Winston Maxwell & Christopher Wolf, *A Global Reality: Governmental Access to Data in the Cloud*, Hogan Lovells White Paper (2012), available at http://www.hldataprotection.com/uploads/file/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf.

104 *See id.* at 13 (presenting a chart showing countries that allowed voluntary disclosure of personal data in response to informal governmental requests).

105 *See, e.g.*, Bamberger & Mulligan, *supra* note 94; Brill, supra note 3, at 6.

106 *See, e.g.*, Nat'l Ass'n of Attorneys Gen., Attorney General Gansler's Presidential Initiative: Privacy in the Digital Age, http://www.naag.org/privacy-in-the-digital-age.php (last visited May 1, 2013) (describing the 2013 nationwide focus by state attorneys general on addressing privacy issues).

to compel deletion of their personal data.[107] In the U.S., such a right would likely run afoul of the First Amendment. Additionally, the proposed Regulation would provide a "right to data portability."[108] Finally, the proposed Regulation would expand the privacy rules' jurisdictional reach directly to companies processing E.U. personal data outside the EU.[109] U.S. privacy law, however, remains restricted to governing companies located within the U.S., and instead makes the companies that transfer personal information outside the U.S. accountable for the actions of their third parties operating abroad.

> "The proposed Regulation would provide a "right to data portability."

The day after President Obama announced the new trade negotiations, the U.S. Trade Representative highlighted "the issue of cross-border data flows as one of those next-generational issues that should be addressed" during the negotiations.[110] That same day, an E.U. data protection official noted that the trade negotiations would present an opportune time to "broaden the insufficient level of data protection in the U.S."[111]

The E.U. critique of the U.S. approach to privacy overlooks fundamental structural differences between the two legal regimes. For example, the U.S. has had to balance its robust privacy protections against strong constitutional protection for free expression. At times, the constitutional protections of the First Amendment may trump otherwise strong privacy interests.[112] In the E.U., by contrast, the balance between the rights to privacy and free expression is less clear – but wherever the exact line falls, the protections for free expression in the E.U. do not rise to the level of First Amendment protections.[113]

While many E.U. member states employ a civil law system, the U.S. has a rich history of relying on the common law. Indeed, the FTC's "enforcement efforts have established what some scholars call 'the common law of privacy' in the United States."[114]

IV. Conclusion

Despite their similar origins in the FIPPs, the U.S. and E.U. privacy regimes have evolved in different ways over the past forty years. But their differences do not necessarily suggest a lack of equivalence or interoperability to satisfy common goals. As Commissioner Brill notes, "[A]lthough the U.S. may for historic reasons approach privacy through our different legal tradition – one that uses a framework approach, backed up by strong enforcement – I believe this approach achieves many of the same goals as those embraced by E.U. data protection authorities."[115]

Why, then, has the U.S. approach been consistently viewed as providing an inadequate level of protection by E.U. officials? The reason seems to be the E.U.'s emphasis on the form of a third country's privacy framework, rather than its substance. This trend is evidenced in the Article 29 Working Party's published adequacy opinions, as well as several statements by E.U. data protection officials, in emphasizing the differences in the U.S. approach.

107 Proposed Regulation art. 17 (providing in enumerated circumstances that a "data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data").

108 Proposed Regulation art. 18 (providing data subjects with the right to obtain a copy of their personal data and transfer it to another system).

109 Proposed Regulation, art. 3(2) ("This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to: (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour.").

110 Transcript of Press Conference, Feb. 13, 2013, http://www.ustr.gov/about-us/press-office/press-releases/2013/february/transcript-briefing-us-eu (statement of Ron Kirk, U.S. Trade Representative).

111 Schaar, *supra* note 100.

112 See, e.g., Florida Star v. B.L.F., 491 U.S. 524 (1989) (holding that a Florida statute prohibiting the publication of names of victims of sexual offenses violated the First Amendment); Jacob Gershman, *When the First Amendment Trumps Privacy Concerns*, WALL ST. J. LAW BLOG, Apr. 10, 2013, http://blogs.wsj.com/law/2013/04/10/when-the-first-amendment-trumps-privacy-concerns/ (noting that a magazine's publication of recordings from private meetings likely is protected by the First Amendment); see also Sorrell v. IMS Health Inc., 131 S. Ct. 2653 (2011) (holding that a Vermont statute restricting the sale, disclosure, and use of prescription records violated the First Amendment).

113 See, e.g., William Echikson, *Judging Freedom of Expression at Europe's Highest Court*, GOOGLE EUROPE BLOG, Feb. 26, 2013, http://googlepolicyeurope.blogspot.com/2013/02/judging-freedom-of-expression-at.html (discussing litigation currently pending before the European Court of Justice involving Spanish citizens' efforts to have Google remove search results about them); Peter Fleischer, *The Saga Continues . . . Now to the Italian Supreme Court,* PRIVACY...?, Apr. 17, 2013, http://peterfleischer.blogspot.com/2013/04/the-saga-continuesnow-to-italian.html (discussing the continuing legal case involving Italy's prosecution of Google executives for violating Italian privacy law by not taking preemptive steps to block a user-uploaded video containing bullying from being posted).

114 Brill, *supra* note 3, at 3 (*citing, inter alia,* Bamberger & Mulligan, *supra* note 94).

115 *Id.* at 6.

But as noted previously, there is substantial common ground between the two approaches, and many differences can be attributed to fundamental characteristics of the respective regimes. As Commissioner Brill observes, "We will not erase the differences in our privacy regimes. And . . . we need not erase them, because we have plenty of common ground for mutual recognition of our different, but equally effective, privacy frameworks."[116] In many other contexts, legal interoperability is achieved by recognizing these fundamental differences and embracing a flexible approach to managing cross-border issues.

Furthermore, the Article 29 Committee's reliance to date on form as a surrogate for effectiveness of a nation's privacy regime overlooks the robust privacy protections currently available in the U.S., as well as the different constitutional and legal structures in place. The Safe Harbor Framework has demonstrated one possible approach to mutual recognition and interoperability, and indeed the U.S. and E.U. have continued to reaffirm their commitment to that approach even as both sides consider revisions to their respective privacy frameworks.[117] The U.S. and E.U. jointly referred to the Safe Harbor Framework in March 2012 as "a useful starting point for further interoperability."[118]

The TTIP presents a golden opportunity to embrace interoperability outright and recognize solutions that give credit to the different ways the two systems achieve substantially similar aims. Perhaps foreshadowing the TTIP negotiations, the E.U.-U.S. joint statement in March 2012 included the following proclamation:

> As the E.U. and the United States continue to work on significant revisions to their respective privacy frameworks over the next several years, the two sides will endeavor to find mechanisms that will foster the free flow of data across the Atlantic. Both parties are committed to work towards solutions based on non-discrimination and mutual recognition when it comes to personal data protection issues which could serve as frameworks for global interoperability that can promote innovation, the free flow of goods and services, and privacy protection around the world.[119]

Part of that effort to find solutions rooted in mutual recognition should be a fresh look at the overall adequacy of the U.S. framework.

More flexible approaches to cross-border data transfers could provide robust privacy protections while facilitating free trade and the free flow of information. As Commissioner Brill noted, "Given the complexity of international data flows and different legal regimes around the globe, I think that providing more flexibility for cross-border data transfers could enhance privacy protection, spur innovation and trade, and help us achieve interoperability between our two systems."[120] Whether that flexibility arises within the framework of the E.U. adequacy approach, the TTIP trade agreement, or alternative measures, the end result should be the same: it is time for the U.S. and E.U. to reach a workable long-term solution to facilitating cross-border data transfers that both protects privacy and promotes international economic growth.

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

Christopher Wolf leads the global Privacy and Information Management practice at Hogan Lovells US LLP, and is the founder and co-chair of the Future of Privacy Forum think tank. In the Spring of 2013, following the announcement of U.S.-E.U. negotiations towards a Transatlantic Trade and Investment Partnership (TTIP), he organized the Coalition for Privacy and Free Trade. Special thanks to Hogan Lovells colleague Paul Otto for his substantial assistance in the preparation of this article.

116 Id.
117 See E.U.-U.S. Joint Statement, *supra* note 1 ("In line with the objectives of increasing trade and regulatory cooperation outlined by our leaders at the U.S.-E.U. Summit, the United States and the European Union reaffirm their respective commitments to the U.S.-E.U. Safe Harbor Framework.").
118 Id.
119 Id.
120 Brill, *supra* note 3, at 5–6.

Can U.S. Attorneys Provide Privileged Advice In Europe?

Many types of attorney-client communications routinely assumed to be privileged in the U.S. may not receive protection in the E.U.

The United States exported an all-time record high of $2.2 trillion worth of goods and services in 2012. But while U.S. business has gone global, the attorney-client privilege has not always come along for the ride.

In 2010, the European Court of Justice (ECJ) in *Akzo Nobel Chemical Ltd. and Akcros Chemical Ltd. v. European Commission* confirmed prior case law that only communications between external lawyers and their clients benefit from attorney-client privilege during investigations by the European Commission (EC). The EC has controversially read prior case law as limiting attorney-client privilege to EU-qualified lawyers and it was hoped that the ECJ would clarify this position in *Akzo Nobel*. It did not do so with the result that many types of attorney-client communications routinely assumed to be privileged in the U.S. may not receive protection in the European Union.

The cloud around the scope of U.S. attorney-client privilege in the E.U. extends inter alia to:

- U.S.-based in-house counsel advising their European-based company;
- U.S.-based outside counsel advising a European-based company;
- U.S.-based company executives disclosing information to E.U.-based in-house counsel;
- U.S. privilege rights being waived by parties involved in EC investigations; and
- EC investigations being conducted outside of *Akzo Nobel*'s specific antitrust context.

In the wake of *Akzo Nobel*, any U.S. company conducting business in Europe must ensure all of its attorneys take special care to preserve attorney-client privilege.

Background on *Akzo Nobel* & EU Privilege Law

Understanding the full scope – and limitations – of the *Akzo Nobel* decision requires some background in E.U. privilege law. The foundation for attorney-client privilege in the E.U. comes from a 1982 decision, *AM & S Europe Limited v. Commission of the European Communities (AM&S)*, in which the ECJ recognized legal profession privilege (LPP) at the E.U. level when two prerequisites were present. The critical elements are:

(i) the correspondence in question must have been made "for the purposes and interests of the client's rights of defence;" and

(ii) the correspondence must also "emanate from independent lawyers, that is to say, lawyers who are not bound to the client by relationship of employment."

The ECJ further stated that the protection of LPP applied to any (external) lawyer entitled to practice in any of the E.U. member states, which has been restrictively interpreted by the EC subsequently as limiting LPP to E.U.-qualified lawyers.

Turning to *Akzo Nobel*, in 2003, anti-trust investigators for the EC seized two e-mails between Akzo Nobel's U.K.-based managing director and the company's Dutch in-house competition lawyer. Challenging the seizure, Akzo Nobel argued in court that the e-mails were privileged. Applying *AM&S,* though, the lower court held that in-house lawyers were not truly "independent" and therefore could not qualify for privilege.

Appealing the decision to the ECJ, *Akzo Nobel* argued that *AM&S*'s "independence" requirement had been satisfied because in-house lawyers were required to adhere to the external ethical and professional standards of their E.U. Member State's Bar. The ECJ rejected the company's arguments and affirmed a strict interpretation of *AM&S*'s two-prong LPP framework. The Court held that an in-house lawyer's employment relationship precluded the possibility of truly independent decision-making, notwithstanding the existence of external professional obligations, making their communications and work product ineligible for LPP.

Implications for U.S. Parties

Akzo Nobel confirmed that a wide gulf exists between U.S. and E.U. approaches to privilege for in-house attorneys. Because of this asymmetry and the EC's stance towards non-E.U. qualified lawyers, U.S. parties face an increased risk of unwanted or unforeseen disclosures when they store or transmit sensitive information in the E.U.:

1. *Privilege risk for U.S.-based in-house counsel*

Communications emanating from U.S.-based in-house counsel may no longer be privileged during EC investigations because *Akzo Nobel*'s reasoning applies equally to in-house counsel based in the E.U. and in the U.S.

2. *Privilege risk for U.S.-based outside counsel*

Akzo Nobel confirmed that LPP may attach to communications between company executives and "independent," outside counsel. However, the ECJ failed to clarify whether "independence" requires enrollment in an E.U. Member State's Bar or Law Society. In *AM&S*, the ECJ hinted that E.U. legal qualifications were a freestanding prerequisite for LPP; the advisory opinion of the Advocate General in *Akzo Nobel* affirmed this view, arguing that the extension of privilege to non-E.U. lawyers "would not under any circumstances be justified." Absent further clarification by the E.U. courts, it is possible that even outside counsel will not qualify for LPP if they are not licensed to practice law within the E.U.

3. *Privilege risk for confidential information provided to E.U. in-house counsel*

Akzo Nobel's categorical denial of privilege for E.U.-based in-house lawyers indicates that information provided by U.S. actors may be discoverable during EC investigations. In addition to the potential impact of these disclosures on the European investigation, there is an added risk that the EC will turn over discoveries to U.S. authorities for use in subsequent domestic investigations.

4. *Potential for inadvertent waivers of U.S. privilege*

Unlike in the E.U., in-house lawyers are eligible for attorney-client privilege in the U.S. However, that privilege can be waived if a party "voluntarily" compromises the confidentiality of relevant communications. The turnover of documents to the EC following *Akzo Nobel* may be interpreted as such a waiver. In order to preserve their U.S. privilege rights, companies under investigation by the EC may have to affirmatively demonstrate that their document turnovers are not voluntary; however, the procedural requirements for such a showing of "involuntariness" have yet to be fully defined.

> "In-house counsel and corporate executives based in the U.S. may no longer be protected by attorney-client privilege outside the U.S."

5. *Uncertain scope of the Akzo Nobel ruling*

The underlying facts of *Akzo Nobel* involved an antitrust investigation by the EC. However, the ECJ's holding was broad enough to encompass any kind of information-gathering activity conducted by the EC. At least until the issue is clarified by the E.U. courts, in-house counsel and U.S. executives may be vulnerable to disclosure and/or waiver in all areas where the EC has native investigative capacities.

Following *Akzo Nobel*, sensitive information shared with E.U. in-house counsel and corporate executives may no longer be protected by attorney-client privilege. Collaboration with E.U.-qualified outside counsel may be necessary to satisfy the ECJ's strict eligibility requirements for LPP. To ensure the client may speak frankly and freely with legal counsel and to preserve attorney-client privilege in the event of a dispute, therefore, attorneys supporting multinational corporations and others with business abroad are well advised to collaborate with counsel experienced in cross-border case management.

Suyong Kim
Partner, London
T +44 (0) 20 7296 2301
suyong.kim@hoganlovells.com

Matthew Levitt
Partner, Brussels
T +32 (2) 505 0903
matthew.levitt@hoganlovells.com

Singapore announces new licence for online news sites

Owners of online news sites that regularly report on Singapore must apply for a new government license or risk fines or imprisonment.

As of 1 June 2013, online news sites that regularly report on Singapore matters and which are accessed by a significant number of Singapore readers will need to apply to the Media Development Authority of Singapore ("MDA") for a new individual licence.

The MDA contends that the new licensing regime has been implemented in order to create greater consistency amongst other news platforms. However, concerns have been raised that the new licensing regime will hinder the free flow of information online, and will prevent smaller online news sites or blogs from being run.

We outline below the new licensing requirements and key concerns regarding it.

Online News Licence

Online news sites must now apply for an individual licence ("Licence") from the MDA if, over a period of two months, they:

(a) are visited by at least 50,000 unique IP addresses from Singapore each month; and

(b) publish on average at least one article per week on news and current affairs of Singapore (which includes any news, intelligence, report of occurrence or any matter of public interest, about any social, economic, political, cultural, artistic, sporting, scientific or other aspect of Singapore, in any language whatsoever, and whether or not it is accessed for free or subject to a charge).

Online news sites that are granted a Licence will be required to remove any content that is found by the MDA to be in breach of its standards, i.e. prohibited content, within twenty-four hours. The online news sites will also be required to put up a performance bond of SG$50,000 (about US$ 39,784 or HK$ 308,830), which may be forfeited if the MDA regulations are breached.

The Licence would be valid for a year, and the MDA will determine whether the Licence should be renewed.

Prior to the new licensing regime, online news sites were automatically class-licensed under the Singapore Broadcasting Act. If the MDA now determines that

an online news site meets the above criteria, it will formally notify the online news site and work with them to move it to the new licensing regime. The following is a list of the online news sites that MDA has so far indicated that it has or will be issuing a licensing notification to:

(a) asiaone.com
(b) businesstimes.com.sg
(c) channelnewsasia.com
(d) omy.sg
(e) sg.news.yahoo.com
(f) stomp.com.sg
(g) straitstimes.com
(h) tnp.sg
(i) todayonline.com
(j) zaobao.com.

The new licencing regime is currently limited to local Singapore based sites, which appears to include sites owned by foreign entities but with the ".sg" domain name. It is intended that the Singapore Broadcasting Act will be further amended in 2014 to more broadly cover any foreign news sites targeting the Singapore market.

Concerns

Over 150 sites, including the popular socio-political blog The Online Citizen, protested against the new licensing regime by participating in a twenty-four hour online "blackout" on 6 June 2013. Participants in the protest blocked access to their sites and redirected users to a page called "Free My Internet," an online movement started by the blogging community to protest against the new changes. A further protest was also held at Hong Lim Park in Singapore on 8 June 2013.

The main concerns appear to be: (i) the new twenty-four hour deadline to take down prohibited content; (ii) the large performance bond; and (iii) the potentially broad applicability of the new licensing regime, and the implications that the foregoing may have on freedom of speech.

Twenty-four hour deadline

Even prior to the application of the new licensing regime, online news sites were required to comply with the MDA's Internet Code of Practice, including removing any "prohibited material" if required to do so by the MDA. However, a new twenty-four hour deadline to remove any content that the MDA deems to be prohibited material is now imposed on online news sites that are subject to a Licence. Previously no time limit was specified.

> "It will be up to the MDA's discretion whether or not a site will be required to obtain a Licence."

Under the MDA's Internet Code of Practice, "prohibited material" is broadly defined as being any material that is deemed to be "objectionable on the grounds of public interest, public morality, public order, public security, national harmony, or is otherwise prohibited by applicable Singapore laws."

Concerns have been raised regarding the ability of online news sites to comply with a direction from the MDA within such a short time period, as well as the number of directions it may receive. Failure to comply with the twenty-four hour deadline may result in the MDA imposing financial penalties or suspending or revoking the relevant online news site's Licence.

Performance bond

Whilst online news sites run by large corporations may be able to afford the SG$50,000 performance bond required to be put up in order to obtain the Licence, popular sites (especially free sites) run by smaller organisations or individuals, may not be able to do so.

This may hinder the running of or result in the shutting down of popular blogs run by individuals or free online sites reporting on any news, events, etc., concerning Singapore.

Applicability of the new licensing requirements

As stated above, the new licensing regime applies to online sites that provide any programme (whether or not the programme is presenter-based or provided by a third party) containing news, intelligence, reports of occurrence or any matter of public interest, about any social, economic, political, cultural, artistic, sporting,

scientific or other aspect of Singapore, in any language whatsoever, and whether or not it is accessed for free or subject to a charge. This broad scope has raised confusion as to the application of the new licensing regime on certain sites. For example, would it apply to a popular blog started by an individual that reports on the current affairs in Singapore?

Whilst the MDA have assured the public on their Facebook page that "an individual publishing views on current affairs and trends on his/her personal website or blog does not amount to news reporting," it is not clear whether or not this extends to blogs or sites that are run by individuals attempting to report the news rather than expressing their own comments. It seems that it will be up to the MDA's discretion whether or not a site (including a blog) will be required to obtain a Licence.

However, it appears that an online news site will only be subject to the new licensing regime if the MDA issues a formal notice to the site requiring it to obtain a Licence after the MDA completes its assessment on whether or not a site meets the Licence criteria. Prior to the receipt of such a notice, an online news site will not be required to obtain a Licence. As stated by the MDA on its Facebook page, "the licensing framework only applies to sites that focus on reporting Singapore news and are notified by MDA that they meet the licensing criteria."

Continuing to run an online news site without obtaining the necessary Licence may result in the MDA exercising its general powers under the Singapore Broadcasting Act, and the site owner may be liable on conviction to a maximum fine of SG$200,000 and/or to imprisonment for a maximum term of 3 years.

Karen Lee*
Associate, Hong Kong
T +852 2840 5081
karenk.lee@hoganlovells.com

* Gabriela Kennedy also contributed to this article

Take down, stay down: Paris Court of Appeal confirms hosting providers have no general monitoring obligation

A French court confirms that providers of hosting services do not have an obligation to monitor the content they host.

> The SPPF noticed that several videos and music belonging to its register were made available online on YouTube without the authorisation of the rights-owners.

In a recent decision dated 21 June 2013, the Paris Court of Appeal endorsed the reasoning adopted a year ago by the French Supreme Court in three decisions involving Google (French Supreme Court, 12 July 2012, no. 11-13.666, 11-15.165/11-15.188, 11-13.669) and decided that there is no obligation for providers of hosting services to prevent the reappearance of contents they have already taken down (often referred to as "*notice and stay down*" principle), except if they are formally notified by rights-owners (http://www.hoganlovells.com/french-supreme-court-invalidates-take-down-and-stay-down-rule-11-07-2013/).

The SPPF (*Société des Producteurs de Phonogrammes en France*) is a French company which is in charge of the collective administration and protection of record and video producers' rights. In May 2008, the SPPF noticed that several videos and music belonging to its register were made available online on YouTube without the authorisation of the rights-owners. Following receipt of several notices, YouTube promptly withdrew the litigious contents from its website. Several months after that, the SPPF noticed that most of the contents that had been taken down had reappeared on YouTube. Therefore, the SPPF sued YouTube notably to get compensation for the loss sustained by the rights-owners and to compel YouTube to make sure that the litigious content would not reappear for a 10-year period.

On 28 April 2011, the Paris Civil Court rejected the SPPF's claims on the ground that YouTube was not liable as a hosting provider for the reappearance of the contents hosted. The Paris Civil Court notably pointed out that the SPPF had refused YouTube's offer to subscribe to "Content ID" which is a technology comparing videos uploaded to YouTube against reference files provided by rights-owners. The SPPF lodged an appeal against this decision on the ground that YouTube had been negligent as it had to prevent the reappearance on its website of the litigious contents, especially through the use of the "Content ID" technology.

> Providers of hosting services do not have the obligation to monitor the contents they host.

The Paris Court of Appeal, in its decision dated 21 June 2013, confirmed the judgment of the Paris Civil Court. The Court notably stated that, pursuant to both the e-commerce Directive no. 2000/31/EC and French implementing provisions (Law no. 2004-575 dated 21 June 2004 for the confidence in digital economy, "LCEN"), only national judicial authorities can require providers of hosting services to monitor the contents they host, provided the hosting is temporary and limited in its scope (Article 6-I-7 of the LCEN and recital 47 of the e-commerce Directive). Indeed, the general principle must remain that providers of hosting services do not have the obligation to monitor the contents they host. It stems from this that the withdrawal of a content is in any case subject to the receipt of a formal notice by the provider of hosting services; this is the case even though the said content may, in the past, have been noticed. If providers of hosting services were compelled to withdraw contents reappearing online following a first notice, it would amount to

a general monitoring obligation, which is expressly prohibited by the e-commerce Directive.

The Paris Court of Appeal also rejected the SPPF's claim to compel YouTube to prevent the reappearance online of contents already notified and withdrawn during a 10-year period, on the grounds that this claim was imprecise, and neither temporary nor limited in its scope.

Interestingly, the Paris Court of Appeal goes even further than the French Supreme Court in considering that SPPF committed a fault when it refused to subscribe to the "Content ID" technology offered by YouTube. Not only was it not YouTube's duty to generate referenced files of the contents hosted without any control of the rights-owners but refusing to use a reporting tool system offered by a provider of hosting services can be considered as a fault on the part of rights-owners.

This decision is an important one as the Paris Court of Appeal confirmed and implemented the decisions adopted one year ago by the French Supreme Court, which strike a fair balance between the rights and obligations of providers of hosting services on the one hand, and rights-owners on the other.

Christine Gateau
Partner, Paris
T +33 (1) 5367 1892
christine.gateau@hoganlovells.com

Pauline Faron
Associate, Paris
T +33 (1) 5367 2289
pauline.faron@hoganlovells.com

Germany: Inspection of source code – Federal Supreme Court strengthens protective interests of copyright holders

Germany's highest civil court finds that copyright holders claiming infringement can request inspection of even partially-open source software applications.

Copyright holders can request inspection of source code at the defendant's premises by court experts if reasonable grounds indicate unlawful use of copyright protected software by the defendant. According to a recent decision of the Federal Court of Justice ("FCJ"), published mid-April, this also applies if the copyright holder only claims infringement of parts of his software and even if these parts in question comprise sequences that are in the public domain (FCJ, decision of 20 September 2012, docket no.: I ZR 90/09 – "UniBasicIDOS").

1. Scope of the decision of FCJ

In the decision at issue, the plaintiff claimed copyright infringement committed by a licensee of a migration software that was designed for software converting purposes. In particular, the software in question could transfer software applications under the outdated operating system "IDOS" into current versions of the operating system "UniBasic." Whilst the licensee was appointed and entitled to develop a previous version of the software at issue, there were indications that he unlawfully and without consent of the licensor refined and transferred a later version of the migration software to a third party. The FCJ overturned a decision of the Appellate Court of Munich (Decision of the Higher Regional Court of Munich, 28 May 2009, docket no. 29 U 1930/08) that had rejected the plaintiff's motion for software inspection.

2. Preliminary injunction and independent evidentiary proceedings

According to German copyright law the copyright holder can request an inspection of source code in preliminary injunction proceedings based on Article 101a (3) Federal Copyright Act and apply for examination of the defendant's premises and technical devices like computers and storage media (including webserver access). However, the courts regularly stress that the defendant's legitimate interest of non-disclosure and protection of trade secrets have to be considered as well. In order to comply with these interests, the inspection of source code has to be executed by IT experts appointed by the court (the copyright holder is allowed to make proposals for the appointed person).

Afterwards the court expert will evaluate and compare the source code seized at the defendant's premises with the original source code provided by the copyright holder in an independent evidentiary proceeding (i.e. prior to a civil lawsuit based on cease and desist and damage claims). Matching parts of the source code components recorded in the court expert's opinion may then form grounds for subsequently raised cease and desist and damage claims.

> "It is irrelevant that the source code may comprise open source code or unprotected components."

3. What's new in the decision of FCJ

In their recent decision the FCJ confirms the principles of source code inspection. In contrast to the Appellate Court, the FCJ held that the copyright holder does not have to prove which particular piece of the software application is affected by the alleged copyright infringement. In the case at issue, the defendant fruitlessly argued that the migration software comprised a number of components and codes in which the plaintiff cannot claim any copyrights or property rights. According to the view of FCJ, it is irrelevant that the source code may comprise open source code or unprotected components, as long as the plaintiff is able to show a likelihood that copyright protected parts of the software were unlawfully taken by the defendant for the illegitimate software development.

Christian Tinnefeld
Counsel, Hamburg
T +49 (40) 41993 186
christian.tinnefeld@hoganlovells.com

Hosted Satellite Payload Procurement: A Brief "How-To" Guide

Satellite owners and hosted payload operators have a wide variety of decisions to make in crafting hosted payload agreements.

Overview

Our prior article, "Satellite Systems Procurement: A Brief 'How-To' Guide," outlined the considerations to take into account in procuring a satellite system, whether commercial or government.

In this article, we will extend our examination of the satellite procurement process to focus on the "how to" of a specialized variation– procurement of a hosted payload. Many of the general elements applicable to procuring satellite systems will apply, but there are many unique considerations involved in a hosted payload arrangement.

What is a "Hosted Payload"

A "hosted payload" situation occurs when a third party's communication mission (or other) payload is "hosted" on the "bus" of another company's satellite. The system architecture of the "host" satellite is developed or modified to accommodate one or more third party "hosted" payloads, by specifically including a location(s) for the payload on the bus and adjusting the satellite design to account for the payload weight, power requirements, technology and other characteristics to be supported by the satellite platform. The hosted payload is typically owned by the third party operator, but can also be subject to a leasing, operational or other funding arrangement where the third party operator may have the right of use as to the hosted payload but not actual title.

A hosted payload may be a substantial payload, perhaps as large or costly as the satellite owner's payload, and may be designed and constructed by the satellite manufacturer (sometimes referred to as a "condosat" arrangement). More commonly the phrase "hosted payload" refers to a significantly smaller payload which puts a much lower demand on the satellite's resources and may be designed and constructed by a third party manufacturer other than the prime contractor for the satellite itself.

Why a Hosted Payload

A hosted payload can provide a "win-win" opportunity for both the host (satellite owner) and the owner of the hosted payload. The cost of procuring a satellite and a launch is quite high, and there is also the cost of an orbital slot, mission planning and execution costs and other expenses. A hosted payload provides an opportunity to share these costs for the benefit of both parties. The host obtains payments for providing the opportunity for the secondary payload to be supported by and launched on its satellite bus, and the secondary payload operator can obtain a much less expensive program by being included on a satellite already being built for other purposes.

In addition, the host may have a unique satellite system that cannot be replicated by the party whose payload is being hosted other than through the hosting arrangement. The unique features may include satellite location (LEO or MEO, for example, or a particular orbital slot), having numerous satellites in the constellation that allow multiple hosting opportunities or time to market advantages in the case of host satellites already in construction.

> "There needs to be a basic hosting arrangement between the hosted payload owner and the satellite owner."

Issues to Consider in Structuring a Hosted Payload Arrangement

The financial benefits of the hosting arrangement are clear, but they come with additional issues and complexities. The obvious one is how to divide the savings that come from the hosting arrangement. There does not seem to be any established or formulaic approach to this, and given the customized nature of many of these arrangements the economics are most often agreed by a case-specific negotiation.

But there are also complexities that arise from the hosting arrangement itself, including a number of key differences in the structure, consideration and risks in establishing a "hosted payload" structure. This article focuses on the extra business, financial, technical and legal arrangements attendant to a hosted payload arrangement not generally contained in a more-straightforward satellite procurement.

Additional Parties and Additional Agreements

Satellite system procurements typically involve one purchaser and its selected satellite system vendors and financing arrangements, which by itself provides significant challenges. The dollar amounts are high, and potential liabilities are substantial. As outlined in our prior article, "Satellite Systems Procurement: A Brief 'How-To' Guide," the agreements that implement these arrangements have a number of unique provisions, almost all of which include limitations on liability, specified remedies for specific failures and clauses that allocate power and control between the parties in specific situations.

By adding in a hosted payload owner and its respective vendors and financing, the number of parties and sets of arrangements multiplies. There needs to be a basic hosting arrangement between the hosted payload owner and the satellite owner, perhaps the primary agreement that implements the hosting arrangement. There is also a procurement contract between the hosted payload owner and the payload manufacturer, which is by itself a negotiated transaction with technical complexities. And there is the task of integrating the hosted payload into the satellite, which could be reasonably straightforward or technically quite complicated, resulting in additions to the satellite procurement contract and the need for arrangements (often not separately documented) between the payload manufacturer and satellite manufacturer.

In some cases the arrangements and agreements are all entered into roughly at the same time, but this is more common in a "condosat" arrangement where the satellite and all payloads are being built by the same manufacturer but the payloads are separately owned. "Hosted payload" situations more frequently see the hosting agreement being entered into at a different time than the satellite procurement, and the hosted payload procurement also happens at a different time with different players.

Having multiple agreements that must fit with each other puts an additional burden on the drafters. Should special provisions be made between the agreements with the respective vendors as to their rights, obligations, and contract adjustments relative to each other, including insurance coverage, excusable delay, risk of loss and passage of title? Or are certain players immune from the risks of the hosting arrangement, and able to proceed with contracts that make no reference to the hosting? Pulling this all together adds several layers of complexity and chances for things to go wrong.

Financial Terms for the Hosting Arrangement

The satellite owner and the hosted payload owner must agree on the financial arrangements for the hosting. There does not seem to be an accepted paradigm for how to do this, and many variants have been used or suggested.

The host may charge a hosting fee, which can be a one-time fee or series of prelaunch (and possible post launch) payments for the hosting. A key issue in this variation is whether the hosting fee is fully earned by the satellite owner redesigning the satellite to accommodate the hosting, and whether the fee is therefore due even if the hosted payload owner discontinues the project.

In other projects there is an ongoing fee (possibly in addition to the initial hosting fee) for the continued hosting. This structure may have "performance" elements, meaning that the hosted payload owner pays so long as it receives the benefit of the hosting services. There is an issue here regarding the cause of the payload owner not receiving the benefit of the hosting services. If the hosted payload is malfunctioning and has to be shut down or modified in some manner, the satellite owner has "performed" but the payload owner is not actually receiving the benefit of the hosting services, so the agreements need to address whether all or some portion of the fee is due.

In still other projects, particularly the "condosat" projects with multiple payloads being built by the satellite manufacturer, the hosted payload owner may pay a share of the satellite construction cost, and ongoing satellite operational costs such as tracking, telemetry and control (TT&C) and satellite operational staff, consistent with being a part owner of the satellite itself.

In addition to documenting the unique fee or cost sharing provisions, there are a number of questions and issues to consider:

- If the satellite or the hosted payload is delayed or for any reason has to be cancelled (such as technical issues), is any portion of the hosting fee refundable? What about the costs of the hosted payload itself, does the owner have to absorb the entire cost of construction of a hosted payload which can no longer be hosted? (Probably yes, but the hosted payload owner may have a termination for convenience provision in its contract with the manufacturer.)
- If the hosted payload is being constructed by the satellite manufacturer, the hosted payload owner may want its own termination for convenience provision with a cap on its exposure. This seems reasonable, but there is then an impact on the owner of the "original" or non-hosted payload, which has to absorb additional satellite construction cost now that the hosted payload owner has left the project (assuming some but not all of the costs it was supposed to bear).
- What occurs in the case of a financial default by either the satellite owner or the hosted payload owner? And does the outcome change if the hosted payload has already been integrated into the satellite or even launched?

Timing Considerations

Satellites and payload programs are often delayed, both as to the procurement of the satellites and payloads as well as the building of the satellites and payloads. Given the multitude of players in a hosted payload program, the delay in either program will impact the other program, creating at minimum incremental program costs and/or risk to the core business, government or scientific mission if the satellite launch is delayed.

Satellite industry players are used to the delay risks associated with launch, where delays in one program can have real effects on others. A prime example is a shared launch, where the two satellites need to be ready at the same time, and delays on one program will force the other to wait or require re-matching of parties sharing the launch (taking into account heavy and light satellites for an optimal pairing).

However, with the hosted payload situation, where there are two manufacturers, the very real possibility exists that a delay by the hosted payload manufacturer may result in the hosted payload not being ready for integration in time to maintain the launch schedule. The satellite owner may (or may not) be willing to tolerate some delay, but in any event there will be a limit, creating the chilling prospect for the hosted payload owner of being left with no host. And since hosts are not fungible and there isn't a robust market for hosting opportunities, loss of the original host may effectively terminate the program for the hosted payload owner, who may have paid for the entire payload and all or most of the hosting fee and then has no project. And there may well be no insurance for these kinds of delay. There is, of course, no one way to address this risk, and it can be a significant challenge for the hosted payload owner and its advisers.

Insurance Considerations

It is no surprise that the presence of a hosted payload complicates the placement of launch and in-orbit insurance. There are also manufacturer insurance issues relating to coverage of the hosted payload through integration, but these are reasonably straight forward.

The good news is that launch and in-orbit insurance can be placed on hosted payloads for the benefit of the payload owner. How and when to place it is less clear, other than that there seems to be a benefit to having the insurance for both the satellite and the hosted payload placed at the same time rather than separately. Particularly in the case of a large hosted payload, there may be limitations on the overall amount of insurance that can be placed, and insurance advisers may counsel that placing the insurance all at once will maximise the amount that can be placed and yield the best rate.

In the case of a small hosted payload, particularly a one-time project for a particular mission rather than part of what will ultimately be a constellation of hosted payloads, the hosted payload owner may benefit from having the satellite owner lead the placement, or even purchase the insurance. This is particularly true if the satellite owner is a well-known operator with significant experience in the insurance market.

The key for the drafting the insurance provisions in the hosted payload agreements is to build in flexibility, so that unexpected twists or turns in the insurance market can be accommodated, while building in the general agreement of the players to cooperate and coordinate.

And (as is the case with many programs) there is a clear benefit to bringing in insurance advisers early, so they can advise on structure and contract issues up front.

Technical Compatibility and Integration

Of all the issues facing a hosted payload arrangement, perhaps the least difficult to accommodate is the technical coordination, non-interference and compatibility of the hosted payload with the satellite and the payload(s) designed as part of the satellite, and the process of integration.

If the satellite design has already been prepared before the hosting arrangements are put in place, the design may need to be re-considered to ensure technical and operational compatibility. In many (most) cases the hosted payload does not overly tax the satellite's resources, and although there need to be some design changes they are fairly minor and straight forward in comparison to the overall satellite design and other changes that the satellite owner and manufacturer have already worked through. Similarly there is an integration process that must be provided for and implemented. In most cases this process is no more complicated than integration of satellite systems and subsystems, and is taken in stride by the manufacturers.

Of course the re-design, however modest, is a "change" that produces increases in cost, which must be negotiated and covered by the respective sets of agreements. If the satellite design has not been set, and accommodations for the hosted payload are part of the initial design, it is less easy to determine the incremental cost of the arrangement to the satellite owner, complicating the economics. On the other hand, including the hosted payload in the original design is almost certainly a less costly alternative than a later re-design.

In a minority of cases the addition of a hosted payload does strain the satellite's resources, particularly the power requirements, and the new design must address how to balance the power needs of the different payloads. In the case of communications payloads that experience much higher and lower levels of usage at different times of the day, the power can be shifted

during lower usage periods to hosted payloads primarily designed for scientific or other purposes. These complexities also may necessitate a hierarchy and priority scheme for allocating power or other satellite resources in the case of scarcity or conflict of needs. Also in a minority of cases the integration can be quite complex, requiring special design efforts and the addition of an integration period to the assembly and launch schedules.

Naturally all of this needs to be documented in the agreements, and lots of "what if" scenarios need to be considered by the parties. How do the respective parties address ownership rights, access to the bus system, power priority issues, access to redundant units, rights to conduct testing or other satellite operations which have some risk to the other payload, etc.? Many agreements do not go into detail on these issues, since the "what if" scenarios are too numerous or too complicated, and just have a simple priority scheme for resolving issues (or leave the satellite owner in control of these issues, which in effect sets the priority in favor of the satellite owner). This in turn needs to be considered in structuring provisions for insurance to ensure that the arrangements will not negatively impact the insurability and recovery by either party.

Operational and Anomaly Considerations

Although in many programs the initial technical considerations in developing the hosted payload arrangement may be no more complex than the numerous other technical issues addressed in satellite procurements, more daunting is the task of anticipating those technical and operational considerations that might arise over the lifetime of the satellite and the hosted payload, and the implications for the hosting arrangement.

Some issues encountered in drafting agreements for the hosting arrangement include the following questions, among others:

- If either the satellite or the hosted payload does not operate as predicted, such as drawing more (or providing less) than expected power or creating some interference issues, how is the situation handled? It may not be possible following launch to re-optimize, and either the satellite or the hosted payload is going to suffer in some manner. It is certainly fair to start with a requirement that the component operating outside of specification be

adjusted or even shut down, but there should also be a process for remediation, re-testing and re-enabling the relevant components, even if they cannot come completely back into specification.

- There also are implications for the financial arrangements. If the hosted payload is shut down, is the hosting fee still paid or if paid retained, or is it refunded?
- What if the shut-down unit is still generating a problem for the rest of the satellite? What are the implications for liability of the parties and limitation on liability sections of the agreements?
- These issues become more complicated still if the cause of the problem cannot be identified, such as a satellite anomaly causing the hosted payload to operate outside of specification, or a power problem not being readily attributable to the satellite but possibly a shortcoming in the hosted payload design. Issues like this may result in a priority scheme being implemented in the hosting agreement on a "no-fault" basis – if there is a resource scarcity, whatever the cause, the parties have agreed how it is to be addressed, and which owner has priority.
- If the payloads are both of significant size and cost and the contracts are entered into concurrently (condosat), the issues are perceived differently than if a much smaller payload is added subsequent to the satellite project being put in place. However, even these smaller payloads can cost in the tens of millions of dollars and/or have significant importance to the scientific mission or business of the hosted payload owner.
- There is a separate series of issues relating to end of life, where the satellite owner wants to de-orbit, place in inclined orbit or replace the satellite. Or if the original host payload reaches end-of-life and the hosted payload has remaining useful life as does the satellite bus, the satellite owner would like the satellite to remain in service for a while before replacement. The agreements should address whether these decisions are at the discretion of the satellite owner at any time, are at the discretion of the satellite owner but only after the originally predicted useful life of the satellite or hosted payload has expired or involve input from both parties.
- Also, how do all of these technical decisions impact insurance coverage and/or the financial arrangements between the parties?

Legal Considerations

The existence of a hosted payload complicates the consideration of applicable regulatory and legal issues that need to be addressed with any satellite system. This includes, for example:

- Frequency coordination, filings and protections: The original coordination likely would not have included the hosted payload, which may involve different frequencies and coverages.
- Export issues in developing a joint satellite system including ITAR matters and TAAs do have the added burden of multiple parties.
- Legal considerations of, and approvals required to, implement ownership, operational and other rights.
- In the case of a highly regulated payload owner (government or civilian) that will own the hosted payload, there may be a separate set of issues and different contractual paradigms to be reconciled.
- Government jurisdictional issues.
- Government control issues.

Financing and Security Issues

Satellite systems procurements may require financing to be put in place concurrently with entering into the applicable contracts for construction and launch, and the same is true of hosting. Lenders (including the government export credit agencies) will require a clean security structure to access to the satellite assets that are being financed. In the case of a hosted payload structure, the host and the hosted payload owners will need clear provisions of ownership and the ability to assign for financing purposes.

Perhaps the biggest complication is the addition to the mix of parties of more than one lender, equity player or other source of financing, with its own requirements and preconceived notions as to how the arrangement will work. The financing and security agreements may need to be specifically tailored for the hosted payload arrangement. It may even be necessary for the parties to coordinate their financings to ensure the feasibility of two side-by-side financing packages, no simple task.

Accommodation of Business Plans

If the business plan of a satellite owner changes, it has to consider the various constraints on its ability to alter the series of preexisting arrangements put in place to support the prior business plan. These constraints are more numerous where a hosted payload is part of the arrangements:

- Satellite relocations, to address more urgent service needs, may be limited in a hosted payload agreement, and should be addressed in the hosting agreement. A relocation that does not have any significant impact on the hosted payload owner's business should certainly be permitted, but of course making that determination is not always easy.
- Changes in satellite operations to optimize satellite life (such as for inclined orbit) may result in unacceptable operations for certain payload services, and hence may cause a sub-optimal situation for one or the other of the host or hosted payload owners.
- Arrangements beyond the initial hosting should also be addressed in the agreements, as well as can be done given the limited ability of the parties to predict the future. Some sort of first refusal right on a successor or replacement satellite seems fairly straight forward, even though it may limit the satellite owner's flexibility to do something different the next time. Other first refusal rights or arrangements for additional satellites are also appropriate subjects to discuss and possibly add to the contract documents.

Company or Asset Sale Situations

Both the satellite and the hosted payload owner will want to carefully consider the implications to them in the event of a sale of the other party or its satellite asset. Both parties will want to ensure that the issues addressed include:

- Provisions on assignment, which may include a free right to assign in connection with a company sale, or may condition that right (subject to reasonability). While the satellite owner does not want to cause economic harm to the payload owner, these arrangements are relatively unique, and the prospect of starting over with a new owner may be unsettling. Accordingly, as part of a free assignment right there may be restrictions as to relocation or repurposing of the host satellite in connection with the sale.
- The satellite owner may want creditworthiness limitations on the assignment right, and there may be issues regarding a sale to a competitor or to a party that would cause a regulatory issue.
- Legal conditions to the transfer of the asset, such as obtaining full regulatory approvals, should be included if possible.
- Payment of costs associated with respect to such a transfer, and any increase in costs resulting to either party as a result of the transfer, needs to be considered.

Financial Issues and/or Insolvency Considerations
Satellite companies face significant challenges, and bankruptcy risks are not uncommon. Hosted payload arrangements create interdependencies between the two parties, and financial issues facing either company can present a challenge. The hosted payload party faces the most significant risks and challenges if the satellite owner goes into bankruptcy, including potential delays, opposition to any agreement modifications that would otherwise be readily implemented and even rejection of the contract/loss of hosting rights. The satellite host faces financial issues if the hosted payload party is in financial trouble and if it enters bankruptcy. The non-bankrupt party will need to continue to abide by the contract terms regardless of the status of pre-bankruptcy payments owed by the other party. Bankruptcy can be a multi-year process, and care needs to be taken to provide the optimum protective mechanisms in an agreement to protect your respective interests in the case of any insolvency situation.

> “Hosted payloads bring very significant advantages to parties.”

A Summary of Best Practices and Takeaways
As either a satellite owner or a hosted payload operator, you need to carefully consider all the issues that may arise during the life-cycle of your business and the life-cycle of your satellite or payload partner. Hosted payloads bring very significant advantages to parties, particularly in an era of scarce orbital slot opportunities and the financial costs and risks of a satellite business. These significant advantages are paired with significant issues which you need to consider to protect your interests.

- Consider the benefits to hosting/being hosted, which can be financially significant and may be the only way a hosted payload’s business plan can be achieved. Some of the risks are considerable, and unlike those encountered in non-hosting situations, but they need to be evaluated in light of the very real benefits.
- Consider the risks of the hosting structure with a multi-disciplinary team, including possible business, technical, government and regulatory outcomes during the life of the satellite and payload programs. Many of the issues are multi-faceted, and would benefit from a free exchange of views by different advisers.
- Know your hosting/hosted partner. As a practical matter, many of the risks that may occur will vary widely in significance depending upon the partner.
- Maintain the core business rights and flexibility you need in the structure and the documentation. All satellite programs are dynamic, requiring changes in understandings documentation during the life of the program, and hosted payload programs are certainly no exception to this.
- Try to anticipate every element of what can occur and address this in your agreements to protect your interests, at the same time appreciating and accepting that there will likely be a loss of flexibility for both parties in entering into a hosting arrangement.
- Consider how the numerous matters unique to the hosted payload arrangement will be reflected in the documents and how you will mitigate your risks in the document drafting. The lack of “standard” models of documentation and unusual risks will put a premium on creativity.

Steven Kaufman
Partner, Washington D.C.
T +1 202 637 5736
steven.kaufman@hoganlovells.com

Randy Segal
Partner, Northern Virginia Office
T +1 703 610 6237
randy.segal@hoganlovells.com

The Economics of Spectrum Sharing[1]

In this issue of the Global Media & Communications Quarterly, we feature a contribution by the leading U.S. economist Coleman Bazelon and his colleague Giulia McHenry, both from the Brattle Group in Washington D.C. Drs. Bazelon and McHenry present an economic approach to spectrum sharing, a policy option currently being considered both in the U.S. and Europe to increase effective spectrum usage.

Policy Background

In light of the growing demand for wireless broadband spectrum, significant attention is now being devoted to more effectively utilizing federal allocations of spectrum, either by entirely repurposing for commercial use, or sharing between federal and commercial users. Spectrum sharing is seen as one way to allow commercial users to access a band without incurring the costs of completely clearing existing federal users.[2] While spectrum sharing avoids costs of clearing incumbent users, it has its own costs and will impact the value of the shared spectrum. We consider the economic tradeoffs associated with various spectrum sharing arrangements, and suggest a method of weighing the tradeoffs and aligning the incentives of federal and commercial users.

There is no easy solution to the growing demands for commercial, federal and local public safety wireless services. The rising demand for commercial spectrum and wireless communication services is widely accepted, but that does not negate the demands for wireless technologies for defense, public safety, and other federal priorities. The challenge to policymakers is to weigh the tradeoffs and facilitate the appropriate spectrum allocations given these conflicting demands.

Efficient Spectrum Allocation

Efficient spectrum allocation decisions should maximize the total social and economic value of spectrum to all users, subject to the priorities set by policymakers. But, while valuing commercial spectrum licenses is more or less straight forward, quantifying the social welfare from a non-commercial spectrum allocation is challenging. It is difficult to directly quantify the welfare generated by defense training.

One concrete way to evaluate non-commercial allocations is to quantify the necessary economic tradeoff of not pursuing the economically efficient allocation.[3] This approach is consistent with maximizing welfare. Whatever the goals of policymakers, economically efficient use of spectrum creates value for achieving policymaker's goals.[4] Consequently, economically efficient spectrum allocations should only be sacrificed for explicit policy objectives that are considered more socially valuable than the forgone value of using the spectrum for its highest economic valued use.[5]

Shared Spectrum Value

In trying to achieve – or in evaluating proposed departures from – the economically efficient use of spectrum, it is crucial to know the costs and forgone opportunity associated with any allocation or assignment policy. This is especially true when evaluating spectrum sharing proposals, since any specific proposal inevitably involves a trade-off between costs and benefits of two or more competing users.

This tradeoff comes from the theoretical drivers of spectrum value. From a commercial perspective, the value of spectrum is essentially derived from the profitability of wireless services deployed on the spectrum. Similarly, the value of non-commercial spectrum is derived from the social welfare gained from its use. In both cases, value is benefits minus

1 This is a condensed version of a paper presented at the 41st Telecommunications Policy Research Conference. The full paper can be found at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2242008.

2 The causality could go both ways – some non-commercial uses of spectrum may look to sharing with commercial bands.

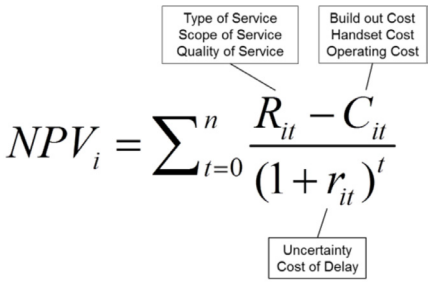
3 Quantifying costs is just one component of cost-benefit or cost-effectiveness analysis of a proposed regulatory policy. Assessing the expected results, direct and indirect costs, potential alternatives, and any anticipated but unintended consequences are just a few of the important factors to consider in a cost benefit analysis. Many federal agencies are required to conduct such analyses when considering new policies. See, Curtis W. Copeland, "Cost-Benefit and Other Analysis Requirements in the Rulemaking Process," Congressional Research Service Report, R41974 (Aug. 30 2011).

4 For instance, U.S. Congressional leaders have requested that, absent the need to meet conflicting policy objectives, the Federal Communications Commission (FCC) pursue an economically efficient, revenue maximizing spectrum license auction for the pending repurposed TV Broadcast spectrum and various allocations in the 1.7 GHz and 2.1 GHz bands. While legislators disagree on the value of specific policy measures, both sides agree that the goal of this approach is to maximize both the economic value created by the spectrum and the revenue due to the U.S. Treasury, subject only to other policy goals deemed at least as important as maximizing economic value. See Letter To FCC From U.S. House of Representatives Committee on Energy and Commerce ("Commerce Committee") Chairman Upton, et al, April 19, 2013; and Letter To FCC From Commerce Committee Ranking Member Waxman, et al, May 16, 2013, both available at: http://energycommerce.house.gov/letters (last visited Sept. 1, 2013).

5 These policies go beyond considerations of simply allocating spectrum to federal users. For instance, the FCC has considered several policies that arguably limit the economic value of spectrum to promote competition among commercial providers, including allocating smaller regional license areas, implementing limits on the amount of spectrum held by a single entity, or offering bidding credits to less competitive auction bidders.

costs. For commercial users, this is profit; for non-commercial users, this is net social welfare.

The impact of sharing on spectrum value is best understood through the components of value as illustrated in the figure below. The value of spectrum to any user is the present value of profits from using the spectrum; profits are revenues less costs, discounted to the present. Anything that impacts revenues, costs or the discount rate will flow back into a change in value of spectrum to a user.



Components of Spectrum Value

In the case of shared spectrum, the total value of the spectrum is the sum of the value to each shared use.[6] Sharing typically decreases the value of spectrum to a given user by limiting revenue, adding costs, or increasing uncertainty. To the extent that sharing restricts the operations or increases the costs of deployment for the highest value user, it diminishes that user's profitability or social welfare generating activities. Only if the sharing arrangement increases the value to all other sharing users by a greater amount than is lost to the highest valued user will the total value of the band of spectrum increase. If the total value of the spectrum for all shared uses is less than the value for a single user, then spectrum sharing diminishes the potential value of the spectrum.

In general, four scenarios are possible:

- First, if value of the spectrum to a new user is greater than the cost of clearing the incumbent user, reallocating the spectrum increases welfare.
- Second, if the costs of moving an incumbent user from a band exceed the value created by a new user, there is no reason to reallocate.

6 For non-shared uses, this framework reduces to the value associated with the single user.

- Third, when introducing new user(s) creates more value than what is lost to the incumbent user(s) sharing enhances welfare.
- Finally, when the loss to the incumbent user(s) exceeds the value created by the new users, sharing is not welfare enhancing.

Empirical Example: Sharing in 1695 MHz – 1710 MHz

In practice, changes in the components of spectrum value – revenues, costs and the discount rate – are not mutually exclusive. To some extent, there are potential tradeoffs between increasing costs, reducing revenues and increasing uncertainty. Moreover, a single shared deployment may result in impairments to revenue, costs and cost of capital. For example, proposals for sharing in the 1695-1710 MHz band from CSMAC Working Group 1 (WG-1) band are likely to reduce expected revenues, and increase costs and uncertainties.

WG-1 was tasked with evaluating the potential for harmful interference between meteorological satellite ground stations and future commercial wireless broadband operations, particularly Long-Term Evolution (LTE) technology.[7] The National Oceanic and Atmospheric Administration (NOAA) operates orbital satellites in the 1695-1710 MHz band and geostationary weather satellites in the adjacent 1675-1695 MHz band. The earth station locations for these satellites would require protection from harmful interference if commercial LTE base stations operated in the 1695-1710 MHz band.

Based on its evaluation, WG-1 recommended 27 geographic protection zones. These protection zones comprise approximately 10% of the 2010 U.S. population, including nine top 100 mobile wireless markets representing approximately 8% of the U.S. population.[8] This proposal was a refinement to the National Telecommunications and Information Administration (NTIA) Fast Track Report proposal to entirely exclude commercial service from 18 zones representing 13% of the population.[9] Protection zones would be areas in which commercial wireless services would not be permitted, unless the commercial licensee could coordinate with NTIA and FCC to ensure that there would be no harmful interference.[10]

Sharing these protection zones is likely to have two negative effects on the commercial spectrum value. First, while the protected area represents approximately 10% of the population, given the areas in top 100 markets, the reduction in value of the commercial spectrum compared to when commercial operations are allowed in the protection zones represents more than 10% of the value. Moreover, by reducing the band to less than a nationwide footprint, sharing may further reduce the value of the spectrum, depending on the size of any premium for nationwide spectrum allocations. Clearing the technical and regulatory hurdles to coordinate commercial operations is still uncertain and potentially costly. If, in fact, the spectrum near these facilities is usable on a predictable basis, this may increase the scope and value of service, and reduce the importance of the nationwide premium.

WG-1 also identified several potential opportunities to further mitigate the impact of these protection zones, which they recommended for further analysis.[11] One of these proposals was to eliminate the need for sharing in the most valuable markets, by moving certain earth stations to less populated areas. The nine protection zones in top 100 markets represent approximately 8% of the U.S. population. If these sites were moved to areas with roughly 1/3 of this population, the total population affected would be reduced to 5%.[12] By excluding only 5% of the U.S. population outside of the Top 100 markets, the scope of the exclusion would be less than 5% and the reduction in nationwide spectrum allocation premium is likely to be minimal. Second, coordinating operations with the geostationary satellites in 1675-1695 MHz may be possible by improving filtering of out-of-band emissions (OOBE). While this would increase the scope of service, it would also increase the cost of deployment in these areas. Only if the added value to commercial users exceeds the additional costs would this mitigation be welfare enhancing.

The extent to which NOAA is likely to negotiate with commercial users to consider any of these proposals for mitigating interference may depend on their incentive to do so. For instance, if NOAA were to reduce its own spectrum costs by moving operations to more rural, less valuable markets, they may be

7 *See* Commerce Spectrum Management Advisory Committee, Final Report Working Group 1 – 1695-1710 MHz Meteorological-Satellite Rev. 1, July 23, 2013 (herein "WG-1 Report Findings"), page 1.
8 *See* WG-1 Report Findings, Table 2.
9 *See* NTIA Fast Track Report. Some of these 18 zones included more than one satellite base station site. The actual footprint of the 27 zones is still smaller than the originally proposed 18 zones.
10 *See* WG-1 Report Findings, page 5.
11 *See* WG-1 Report Findings, Appendix 5.
12 8%/3 = 2.67%. The sites outside top 100 markets represent an additional 2% of the U.S. population. Combined, these moved sites would represent approximately 4.67% of the U.S. population.

more inclined to consider this option. Similarly, if federal users could reduce costs by narrowing their interference zone even further, they may be more willing to allow commercial use inside the protection zone. New equipment with increased functionality may provide additional incentives.

Facilitating Sharing: Incentivizing Federal Users

It is widely accepted that until Federal users internalize the costs associated with their spectrum use, Federal users have no incentive for using spectrum more efficiently or maximizing spectrum's total social value. While quantifying the foregone value is one way for policymakers to weigh the tradeoffs of conflicting demands, it still leaves at least two long term challenges for efficient spectrum sharing.

First, just as commercial users' spectrum demands evolve, government spectrum users' needs are likely to vary over time. As constraints on spectrum get tighter, spectrum will be more heavily used – both temporally and between frequencies. This is the impetus for spectrum sharing. For it to work, however, policymakers need a mechanism for government users to adjust their spectrum usage – and even assignments – according to current needs and cost-effectiveness. Rather than holding spectrum assignments for some future objective or utilizing more spectrum in lieu of potentially more spectrum efficient alternatives, agencies should have a reason to relinquish assignments they are no longer using, or adjust usage to increase the overall efficiency of spectrum, including through increased sharing. An important component of this, however, is that federal users must be assured that they will be able to acquire spectrum assignments when they have a justifiable need. Otherwise, they will still not have an incentive to relinquish spectrum they are not using.

Second, to weigh the true costs and benefits of a wireless communication service, government users need a way to internalize the cost of the spectrum they use. Spectrum is a highly valued, scarce resource. However, once they receive an assignment, federal users do not incur costs for holding on to the asset. This valuable asset is essentially free to them. Federal users typically incur costs associated with utilizing many other valuable assets. For instance, the Government Services Administration charges federal users rent for office space. The Department of Defense pays for artillery and machinery. If federal users paid for spectrum, they would internalize the cost associated with holding the spectrum. This would incentivize them to adjust their usage to reduce costs. For instance, federal users may choose to adjust the timing of their spectrum related missions; invest in higher quality filters to limit their spectrum needs; lease capacity from commercial carriers rather than deploy their own services; or more readily accommodate sharing with other users.

Such an approach is consistent with general Presidential directives and Office of Management and Budget (OMB) guidance. A Presidential memorandum released in June 2013 called for an evaluation of spectrum efficiency in procurements and market-based incentives for the efficient use of federal spectrum.[13] The 2013 OMB guidance instructs federal agencies to consider the economic value of spectrum in weighing alternative proposals for deploying spectrum based services.[14] This guidance is intended to ensure "proper stewardship of the spectrum resource."[15] However, government spectrum users still have no basis or incentive to quantify the economic value of spectrum. Federal users should have an incentive to adjust their spectrum usage to their need, either in real time, or over time.

Several critical stakeholders have already endorsed a fee based approach.[16] FCC Commissioner Rosenworcel voiced similar sentiments in late 2012.[17] While there are

13 *See* Presidential Memorandum, 2013, sections 4 and 6.

14 *See* Office of Management and Budget, Preparation, Submission, and Execution of the Budget, Circular No. A-11, 2013, section 31.12, available at: http://www.whitehouse.gov/omb/circulars_a11_current_year_a11_toc (last visited Aug. 11, 2013). According to this guidance: The value of radio spectrum required for telecommunications, radars, and related systems should be considered, to the extent practical, in economic analyses of alternative systems/solutions. In some cases, greater investments in systems could enhance Federal spectrum efficiency (e.g., purchase of more expensive radios that use less bandwidth); in other cases, the desired service could be met through other forms of supply (e.g., private wireless services or use of land lines). Therefore, to identify solutions that have the highest net benefits, agencies should consider greater investment to increase spectrum efficiency along with cost minimizing strategies. To this end, section 6411 of the Middle Class Tax Relief and Job Creation Act directed that A–11 be updated with sections (a) and (c). Subsection (b) provides a methodology for determining a baseline to evaluate improvements in spectrum efficiency.

15 Ibid.

16 *See* GAO, *Federal Government's Use of Spectrum and Preliminary Information on Spectrum Sharing,* Testimony Before the Subcommittee on Communications and Technology, Committee on Energy and Commerce, House of Representatives, GAO 12-1018T, September 13, 2012.

17 *See* Remarks of Commissioner Jessica Rosenworcel at Silicon Flatirons: The Next Ten Years of Spectrum Policy, November 13, 2012, *available at* transition.fcc.gov/Daily_Releases/Daily.../2012/.../DOC-317319A1.pdf (last visited Aug. 11, 2013).

limitations to a fee-based approach,[18] it would require government users to incur some cost for spectrum usage. By imposing a spectrum based fee, the cost of spectrum based services for federal users will reflect the use of this scarce resource. The question is: what should the fee be tied to?

Consistent with the principle that government spectrum users should consider the forgone economic value of spectrum deployed for their services, we suggest that the fee should be based on the commercial value of spectrum. It may be difficult to calculate the precise forgone economic value to a federal user, but if spectrum is efficiently allocated this should generally be equivalent to the economic value of the spectrum used – either shared or used exclusively. While the theoretical economic value of a band of spectrum is difficult to determine, the commercial price of spectrum realized at auction or in secondary trades is one observed estimate of this value. By tying the fee for federal spectrum to spectrum's commercial price, federal users would be recognizing the foregone economic value or opportunity cost of the spectrum in deploying these federal services. This would ensure that the spectrum would only be used if it was the most economically efficient way to achieve policymakers' goals.

Calculating the fee would be a two-step process. In the first step, commercially attractive swaths of spectrum currently occupied by federal users would be identified. This may be a 50 MHz or 100 MHz band, the exact size depending on several factors including the currently preferred size of commercial deployments. The commercial value of the band if it were unencumbered by federal users can be calculated using standard spectrum valuation techniques.[19] This value represents the opportunity cost of the band remaining exclusively under federal control.

The second step of the fee calculation would then be to allocate the opportunity cost of the band to the individual federal users. This allocation exercise would consider the relative value of all of the users in the band. Agencies that thought they were allocated too large a share of the band's costs would be well incentivized to produce analysis correcting the record. This would also create a cost to agencies that exaggerate the importance of their spectrum based missions. Note that under this scheme, if a federal user chose to stop using a specific band of spectrum, the opportunity cost associated with that band (from step one) would not change and that cost would now be allocated to a smaller group of users. Such an approach would also incentivize spectrum sharing because introducing commercial users in a band would reduce the portion of opportunity costs that would need to be covered by the federal users.

Coleman Bazelon
coleman.bazelon@brattle.com

Giulia McHenry
giulia.mchenry@brattle.com

The Brattle Group
1850 M Street, NW Suite 1200
Washington, DC 20003
Phone: 1.202.955.5050
Fax: 1.202.955.5059

18 As discussed above, since agencies are still dependent on Congress to set its budget, any reduced costs would essentially mean a reduced budget from Congress, rather than a reallocation of resources to other important missions of that agency.

19 *See* Coleman Bazelon and Giulia McHenry, "Spectrum Value," Journal of Telecommunications Policy, forthcoming.

www.hoganlovells.com

Hogan Lovells has offices in:

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

* Associated offices