Telecommunications and Internet Services: The digital side of the TTIP

Andrea Renda and Christopher Yoo

Paper No. 8 in the CEPS-CTR project 'TTIP in the Balance' and CEPS Special Report No. 112 / July 2015

Abstract

In the overall negotiations on the Transatlantic Trade and Investment Partnership (TTIP), the digital chapter appears to be growing in importance. This is due to several factors, including the recent Datagate scandal that undermined trust between the negotiating parties and led to calls to suspend the US-EU Safe Harbour agreement as well as the furious debate currently ongoing in both legal systems on key issues such as policies to encourage broadband infrastructure deployment, network neutrality policies and the application of competition policy in cyberspace. This paper explores the current divergences between the two legal systems on these key issues and discusses possible scenarios for the ultimate agreement to be reached in the TTIP: from a basic, minimal agreement (which would essentially include e-labelling and e-accessibility measures) to more ambitious scenarios on network neutrality, competition rules, privacy and interoperability measures.

This paper is the eighth in a series produced in the context of the "TTIP in the Balance" project, jointly organised by CEPS and the Center for Transatlantic Relations (CTR) in Washington, D.C. It is published simultaneously on the CEPS (www.ceps.eu) and CTR websites (http://transatlantic.sais-jhu.edu). For more information about the project, please see the penultimate page of this paper.

The views expressed in this report are those of the authors only and do not necessarily represent those of CEPS, CTR or the institutions with which they are associated.

ISBN 978-94-6138-469-0

Center for Transatlantic Relations, Johns Hopkins University SAIS ▪ 1717 Massachusetts Ave., NW, Suite 525 Washington, D.C. 20036 ▪ Tel 001.202.663.5880 ▪ http://transatlantic.sais-jhu.edu

Centre for European Policy Studies ▪ Place du Congrès 1 ▪ B-1000 Brussels ▪ Tel: (32.2) 229.39.11 ▪ www.ceps.eu

TABLE OF CONTENTS

Telecommunications and Internet Services: The digital side of the TTIP

Andrea Renda and Christopher S. Yoo*

Paper No. 8 in the CEPS-CTR project "TTIP in the Balance" and CEPS Special Report No. 112 / July 2015

Introduction

As negotiations on the Transatlantic Trade and Investment Partnership (TTIP) have progressed, the digital component appears to be growing in importance. This is due to a number of recent events that have led digital issues to increasingly occupy the spotlight in the negotiations. First, the Datagate scandal, spurred by the revelations of Edward Snowden, has seriously undermined trust between US and EU authorities, leading the European Parliament to call for the suspension of the Safe Harbour agreement, which allows smooth flows of data between the two sides of the Atlantic. Tensions between the parties at the table are so heightened now that it is widely thought that there can be no TTIP agreement without an agreement on data protection (possibly outside the TTIP and before its conclusion). Second, the growing importance of the data economy and the enabling nature of ICT as a driver of productivity and innovation in many other sectors makes the Digital TTIP a key complement, if not a precondition, to a successful and comprehensive agreement between the US and the EU. Third, the evolution of the debate over network neutrality in both legal systems has led the general public to focus on the possibility for the two superpowers to achieve some consistency in the regulation of traffic management practices on the Internet. Last but not least, all of this is occurring as the stalemate in other chapters (e.g. agriculture, financial services, and others) is motivating the parties to revert to the digital transatlantic economy as a natural candidate for a resounding agreement.

To date, however, the evidence on convergence between the two major blocs is mixed at best. In fact, while there have been some timid attempts to reach agreement on delicate issues such as data protection and cybersecurity, differences in the application of competition law and regulation in a number of crucial policy areas (such as online search, e-commerce and copyright) seem to be growing, rather than shrinking, undercutting the preconditions for creating a vibrant transatlantic digital economy. One easy example is the evolution of the European Commission's antitrust investigation against Google, now coupled with the launch of an extensive sectoral inquiry into e-commerce and a pompous campaign against geo-blocking practices, both likely to target US-based IT giants such as Amazon. More generally, the European Parliament and some national authorities (primarily France and Germany) are extensively campaigning against the so-called 'GAFA' (Google, Amazon, Facebook, Apple), or even the 'GAFTAM' (Google, Amazon, Facebook, Twitter, Apple, Microsoft), all companies headquartered in the US. And to some extent, similar signals are also sent by large-scale

* Andrea Renda is Senior Research Fellow at CEPS and Christopher Yoo is Professor of Law, Communication, and Computer and Information Science at the University of Pennsylvania Law School.

government policies on advanced manufacturing, which seem to be developing incompatible standards in essential fields such as the Internet of Things and cloud computing.

Many of these initiatives are now included in the new Digital Single Market Strategy adopted by the European Commission on 6 May 2015. The strategy, expected to contribute €415 billion per year to the EU economy, includes 16 targeted actions based on three pillars: i) better access for consumers and businesses to digital goods and services across Europe, ii) creating the right conditions and a level playing field for digital networks and innovative services and iii) maximising the growth potential of the digital economy. The Commission wants to complete the package by 2016, noting that all proposals have to go through the European Parliament and the Council: the first initiatives have mostly focused on copyright reform (see below).

Against this background, what are the prospects for a comprehensive Digital TTIP? In an unprecedented effort to increase the transparency of the ongoing negotiations, the European Commission has recently stated that its primary objectives in the negotiations on the ICT chapter are to improve enforcement of regulations and consumer protection, to make it easier for EU firms to export to the US and to cut unnecessary costs. It also stated that the agreement will not lead to any lowering of safety and security standards for EU citizens, an outcome that some commentators and advocacy groups had otherwise considered likely. Current documents released by the European Commission suggest that the parties may be able to reach agreement on an initial set of important issues.[1] These include:

- *e-labelling*: setting standards for providing product information to consumers in electronic format, replacing labels and stickers;
- *e-accessibility*: making ICT easier to use for people with disabilities and
- *cryptography*: setting common principles for certifying ICT products, especially for encoding and decoding information.

However, the Digital TTIP has the potential to become much more ambitious, covering issues such as network neutrality and data protection, if not also intermediary liability, cybersecurity and copyright. Already in its first document released in early 2015, the European Commission mentions one issue that appears simple, but can prove very controversial in practice: the potential for an agreement on data interoperability, which would enable users to exchange data easily between different products or platforms. In addition, a 'non-paper' presented at the EU Council Trade Policy Committee by the French and Austrian delegations in October 2014 contained a much more comprehensive list of issues, including an adaptation of the concepts of 'essential facilities' and 'major suppliers' to the digital environment, an agreement on the treatment of digital platforms concerning privacy, interoperability and competition, and agreement on network neutrality principles.

In this paper, we explore the current divergence between the US and the EU on a number of issues and comment on potential consequences for the TTIP. Section 1 below discusses rules on infrastructure-sharing and network neutrality and the prospects for convergence between the two legal systems on these crucial issues. Section 2 contains an illustration of the divergence between the US and the EU on antitrust rules. Section 3 compares the approach followed by the two jurisdictions in the online search market and in e-commerce, in what has

[1] The European Commission published in February 2015 a series of 2-page factsheets and EU textual proposals on parts 2 and 3 of the TTIP (see http://trade.ec.europa.eu/doclib/press/index.cfm?id=1230).

been termed the 'platform regulation' debate. Section 4 addresses issues related to user information and in particular e-labelling and e-accessibility. Section 5 compares US and EU public-policy initiatives for the transition towards the Internet of Things. Section 6 compares data protection legislation in the US and the EU and comments on possible scenarios for transatlantic data flows, including the possible suspension of the Safe Harbour.

1. Broadband infrastructure and net neutrality

1.1 Infrastructure-sharing: Between competition and investment

Over the past decade, the regulatory approach to broadband telecommunications in the US and the EU has diverged widely. On the one hand, the US Federal Communications Commission (FCC) has actively pursued a deregulatory approach in order to stimulate the deployment of high-speed broadband networks, which resulted in the lifting of infrastructure-sharing obligations on high-speed broadband networks since 2003. The presence of a pervasive legacy cable infrastructure, which itself could be upgraded to high-speed networks thanks to new technologies and standards such as DOCSIS 3.0, has led to the emergence of vibrant facilities-based competition throughout the US.[2]

On the other hand, the absence (in many countries) of a legacy cable infrastructure in Europe has led regulators to opt for infrastructure-sharing, which was made even more extensive and invasive after 2003, exactly as the US was going in the opposite direction. The application of the so-called 'ladder of investment' model to encourage the entry of new players in each of the EU member states has led to a significant fragmentation of the market, with hundreds of telecoms operators now populating the continent.[3] While offering consumers a variety of alternative providers, in many countries this fragmentation has led to a catch-22 situation, in which the obligation to share any improvements at regulated prices deters incumbent players from upgrading their infrastructure and the ability to access the existing infrastructure on quite favourable terms discourages new entrants from investing as well. European regulators once placed great hopes in the so-called 'ladder of investment' model, under which infrastructure-sharing served as a stepping stone to full facilities-based competition. Empirical studies have shown that although existing policies have encouraged entrants to shift from resale to bitstream access to accessing unbundled local loops, they have failed to encourage them to make the final step to full facilities-based competition.[4] The result is new entrants compete only by squeezing margins ever closer to the wholesale price rather than by investing in improved services. Against this background, the only (limited) investment in ultra-fast broadband in Europe has come from cable operators and electric companies or from municipalities, often using EU cohesion funds.[5]

The impact of these policies is most visible in the availability of Next Generation Networks (NGNs) capable of providing service of 30 Mbps. Studies commissioned by the US and the EU

[2] See Renda (2007, 2009) and Yoo (2014).

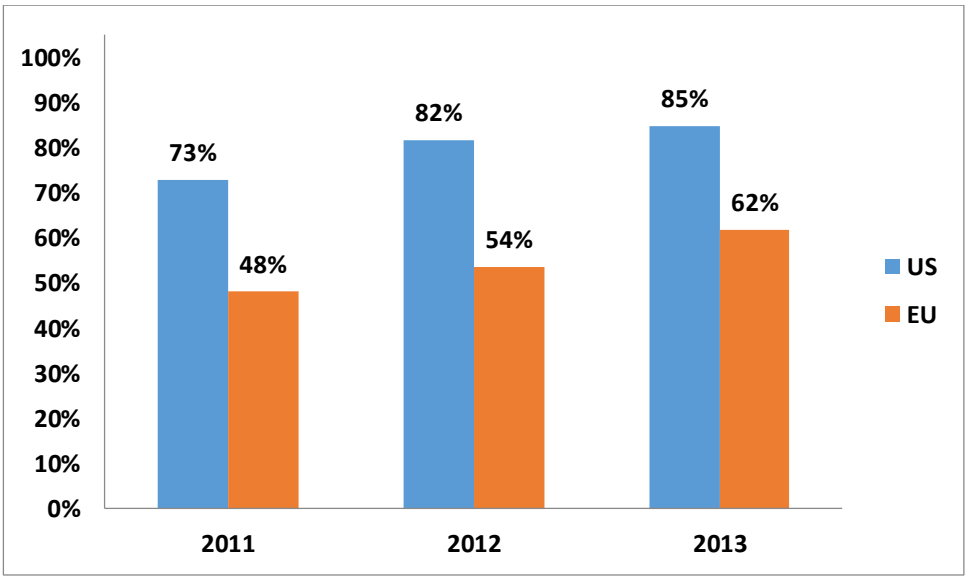
[3] For a description, see Renda (2009) and Pelkmans & Renda (2011).

[4] See e.g. Bourreau et al. (2010).

[5] Yoo (2014).

on broadband coverage in 2011, 2012 and 2013 reveal that the US has consistently outpaced Europe in NGN coverage (see Figure 1).[6]

Figure 1. Next generation coverage in the US and EU, 2011-13



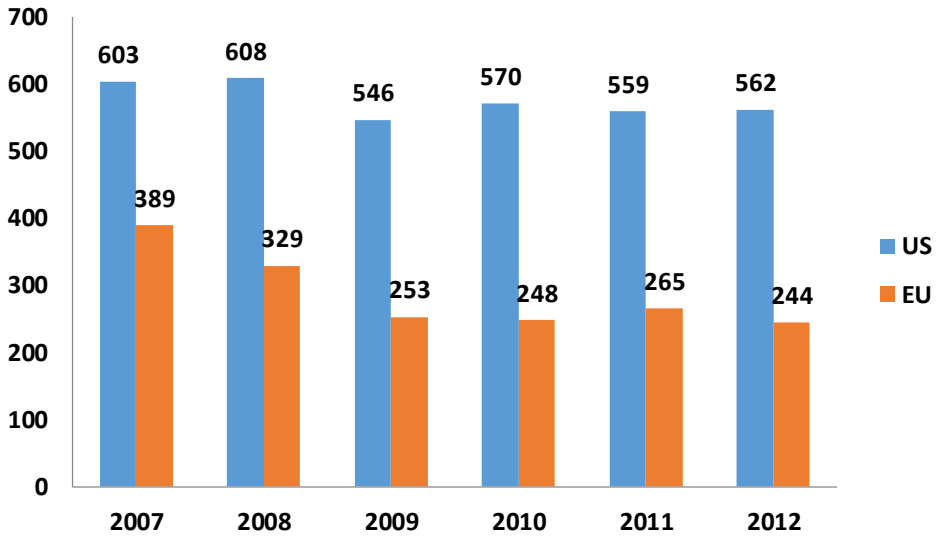
Data source: Yoo (2014).

Data on investment levels reveal the same pattern. From 2007 to 2012, US providers invested on average more than twice as much per household as their European counterparts. Since 2008, European investment levels have languished at 35% below their pre-2008 peak, while the drop-off in the US has been more modest 7% (see Figure 2).[7]

[6] Note that although the European Commission defines NGN as 30 Mbps service, it collects data on 25 Mbps service.

[7] Yoo (2014).

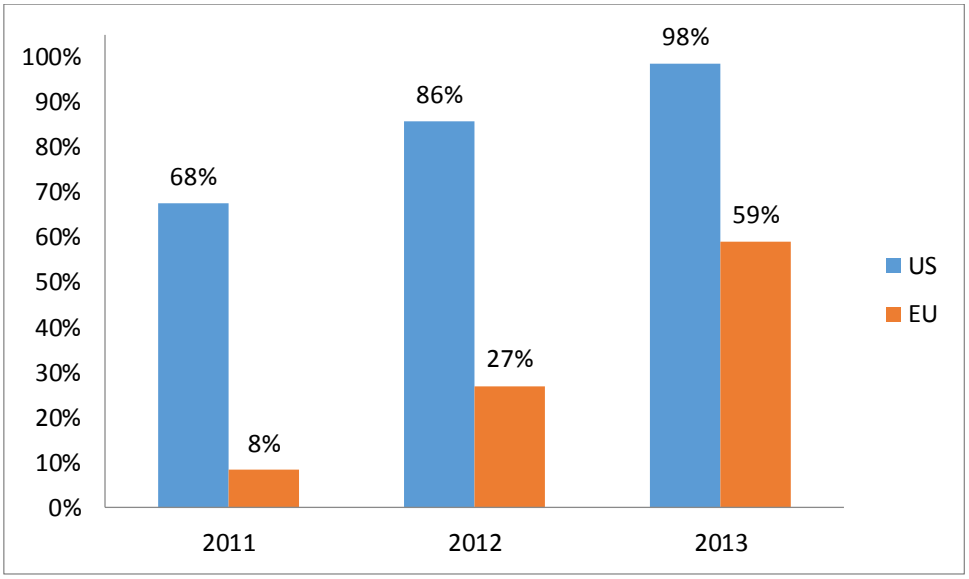
Figure 2. Electronic communications sector investment per household in the US and EU, 2007-12



Data source: Yoo (2014).

At the same time, a proactive spectrum policy by the FCC has led to the early auctioning of the digital dividend spectrum (e.g. the 700 Mhz band), which enabled the early deployment of very high-speed mobile broadband networks such as 4G (Long-Term Evolution, LTE). Likewise, difficulties in achieving the needed coordination between national authorities have led to significant delays in the reallocation of spectrum to mobile operators in key bands such as 800Mhz and 700Mhz. The absence of a timely, coordinated EU spectrum policy has made Europe a laggard in the deployment of 4G broadband (see Figure 3). The US market has also become quite competitive. As of December 2014, AT&T served 99% of the US population with LTE, with Verizon serving 96%, Sprint serving 78% and T-Mobile serving 72% (FCC, 2014b). This makes it quite likely that more than 70% of the population can choose from among three, if not four, LTE providers.

Figure 3. 4G LTE coverage in the US and EU, 2011-13



Data source: Yoo (2014).

This stark divergence of regulatory approaches has led to the exact result one would expect: while in the US the FCC has started to worry about vertical exclusion, in Europe the priority is now stimulating investment and possibly achieving a degree of industry consolidation. Both stances bear important consequences for the current debate on network neutrality, since recent initiatives in the two jurisdictions on this issue have been grounded in (or heavily affected by) the current state of the telecommunications infrastructure.

1.2 Network neutrality

One of the policy areas in which the divergence between the US and the EU has been most evident over the past decade is network neutrality, defined as a rule prohibiting network operators from discriminating between types of Internet traffic and thus obliging them to treat all bits in the same manner. Companies operating at the application and content layers of the Internet ecosystem have advocated such a rule since the mid-2000s. Their efforts have triggered a furious debate first in the United States and later in the EU and globally. Arguments in favour of regulatory intervention to mandate network neutrality and to keep telecoms networks as 'dumb pipes' developed mostly with reference to the infrastructure and logical layers of the Internet value chain. On the one hand, telecoms operators claim that disabling them from managing traffic on their networks would jeopardise the quality of the user experience, deny the possibility of a more efficient and effective provision of the Internet service and leave the whole Web prey to spam and illegal peer-to-peer file-sharing, which – despite its illegality – has continued for many years to represent roughly half of all Internet traffic. On the other hand, 'neutralists' challenged this view by stating that the end-to-end nature of the Internet should not be contaminated by intelligence in the core of the network, which would reduce the value of the network due to filtering of content and speech and the narrowing down of spaces for creativity at the edges.

The network neutrality debate can be approached from several angles. From a competition policy perspective, network neutrality is more needed if consumers do not have sufficient choice between alternative Internet Service Providers (ISPs): the existence of a single ISP with

significant market power could lead to situations in which blocking or throttling of competing applications or 'unwanted' content could be the equivalent of discrimination or refusal to deal (see below, section 2). From a dynamic efficiency perspective, a relaxation of network neutrality rules could allow ISPs to monetise investment in new networks by charging 'bandwidth hogs', such as Netflix, a fee for the occupying their networks or by offering certain application providers a 'toll lane' over the public Internet, where quality of service would be guaranteed. Moreover, the neutrality debate has been approached from the standpoint of data protection (Should ISPs inspect the traffic that flows over their networks?), innovation (Will the new Google be forced to bribe an ISP to be visible on the Internet?), and even freedom of expression and media pluralism (Will ISPs decide which content should be prioritised, and which one should be delayed? or Should ISPs be free to decide which content to prioritise, in the name of freedom of expression?). While a full account of all these positions would fall outside the scope of this paper, appreciating the complexity of the debate is critical for anyone seeking to assess the likelihood that the US and the EU will find common ground.

1.2.1 Network neutrality in the United States

Although the controversy over network neutrality can trace its roots to disputes over open access to cable modem systems that took place during the late 1990s, the debate began in earnest in 2002, when the FCC issued a ruling to classify cable modem systems as 'information services' instead of 'telecommunications services', which exempted them from Title II regulation, including, inter alia, network-sharing obligations (FCC, 2002b).[8] The US Supreme Court eventually upheld the FCC's action in *Brand X Internet Services v. FCC* (2005).

In response to concerns raised in the aftermath of this ruling, then-FCC Chairman Michael Powell (2004) called upon the industry to voluntarily embrace a series of Internet freedoms that would ensure end users' ability to access content, run applications and attach personal devices as they saw fit, subject only to restrictions needed to manage networks, ensure quality experiences, prevent disruption of the network and prevent theft of service. Powell also called for the industry to provide consumers with clear and meaningful information regarding the terms of their broadband service plans.

Concerns about blocking were heightened when a small local telephone company known as Madison River Communications prevented its DSL (digital subscriber line**)** customers from using the ports needed to access Internet telephony (also known as Voice over Internet protocol or VoIP) The FCC (2005a) invoked Title II when approving a consent decree settling this matter. The FCC (2005b) reversed course after the US Supreme Court's decision in *Brand X*, classifying DSL and other wireline forms of broadband Internet access constituted an information service. Shortly thereafter, the FCC also classified broadband over powerline and wireless broadband as information services as well (FCC, 2006 and 2007).

Since then, the FCC has constantly been under pressure to strengthen network neutrality rules. For example, at the same time that the FCC classified DSL as an information service, it issued

[8] As the cable modem declaratory ruling noted, the federal government had never subjected cable systems to common carriage regulation (FCC, 2002b). Just the FCC concluded that broadband was an information service did not necessarily mean it would not be regulated. With respect to both DSL and cable modem service, the FCC sought comment on what regulations, if any, the FCC should impose under its general rulemaking authority (FCC, 2002a, pp. 3040-3048; 2002b, pp. 4839-4854).

a Policy Statement recognising the agency's intent to preserve consumers' rights to access content, run applications and attach devices as they saw fit. As such, the rule prohibited the blocking of content, but did not explicitly prohibit non-discrimination and even acknowledged the need for exceptions to the no-blocking principle for the needs of law enforcement and for "reasonable network management" (FCC, 2005c). But the Policy Statement did not formally adopt any regulatory mandates, and network neutrality proponents began to regard non-blocking obligations as insufficient. Also the US Congress began to debate the issue during its consideration of major telecommunications reform legislation in 2006.[9] Although attempts to introduce network neutrality into the legislation were rejected by wide margins in the House of Representatives, the issue proved more controversial in the Senate, where an evenly divided Commerce Committee rejected a network neutrality amendment by a vote of 11 to 11. The underlying bill was never brought to the floor of the Senate.

During the Obama Administration, calls for stronger network neutrality have become even more frequent.[10] After taking office, the Obama Administration included provisions in the stimulus package that required that that broadband infrastructure grants made by the National Telecommunications and Information Administration comply with the 2005 policy statement on network neutrality (American Recovery and Reinvestment Act of 2009). This new momentum led the FCC to issue a notice of proposed rule-making recommending the adoption of formal network neutrality rules for the first time in 2009: the proposed rule also included provisions on non-discrimination, while maintaining exceptions for reasonable network management and law enforcement/public safety and applying a lower standard to wireless networks. At that time, the FCC decided against reclassifying broadband as a Title II telecommunications service. Although the FCC's first Open Internet Order was adopted at the end of 2010, it was not published in the *Federal Register* until 23 September 2011. Shortly thereafter, Verizon challenged the 2010 order in court, with the court resolving the matter in January 2014 (*Verizon v. FCC* 2014). The court ruled that the FCC has ancillary authority over the broadband Internet as a general matter, but struck down the FCC's non-discrimination and non-blocking rules as improper exercises of that authority, while providing guidance on how to reframe those rules so that they would comply with the statute.[11]

In May 2014, four months after the court's opinion in *Verizon v. FCC*, the agency proposed new rules that followed the approach described by the court (FCC, 2014a). But while the FCC seemed to favour a compromise solution in which non-blocking rules would be coupled with exceptions for specialised services and reasonable traffic management, the political landscape changed abruptly in November 2014, when the President endorsed Title II as the basis for

---

[9] For a review of the history of this legislative debate, see Yoo (2006).

[10] Barack Obama endorsed network neutrality both as a Senator and a candidate during the 2008 presidential campaign (http://change.gov/agenda/technology_agenda/).

[11] Specific exercises of ancillary authority under Title I are subject to the constraint that they not contravene any other specific statutory provision. The statute provides that the FCC can impose common carriage obligations only on providers of telecommunications services, not on providers of information services. Because the prohibition of unjust and unreasonable non-discrimination is the quintessential obligation borne by common carriers, mandating non-discrimination would represent an improper imposition of common carriage obligations onto an information service. The court similarly concluded that the anti-blocking rule combined with prohibition of charging edge providers any fee for providing connectivity essentially imposed common carriage obligations with a price of zero. The court did uphold the transparency rules as a valid exercise of the FCC's ancillary authority under Section 706.

network neutrality in a public speech. This speech heavily influenced the content of the new Open Internet Order adopted by the FCC on 26 February 2015, and released on 12 March 2015.

The new Open Internet Order reclassified broadband Internet access services (BIAS) as a telecommunications service governed by Title II of the Communications Act of 1934, completing what can only be seen as a U-turn from the direction the FCC had taken since 2002.[12] The Order establishes three 'bright-line rules' prohibiting blocking, throttling and paid prioritisation, with all other conduct being governed by a general standard prohibiting unreasonably interfering with disadvantaging consumers' ability to reach the content, applications, services or devices of their choice or edge providers' ability to access consumers using the Internet. The order created exceptions for reasonable network management, defined as practices primarily used for and tailored to achieving a legitimate network management purpose as opposed to a business purpose. Another new feature of the Order is that it extends full network neutrality protection to wireless networks.[13] With respect to specialised services, which the order renamed non-Broadband Internet Access Services (non-BIAS) data services, the FCC continued to permit providers to offer these services while continuing to monitor their development and use. But perhaps the biggest change in the scope of the order is the inclusion of interconnection in its regulatory purview. Until the adoption of the 2015 order, network neutrality sought to equalise how traffic is handled within a broadband network. Regulating interconnection, in contrast, seeks to equalise the terms under which how traffic arrives at a network.

What is most striking is the extent to which network neutrality has represented a moving target. What began in 2005 as a prohibition on blocking also became in 2010 a prohibition on discrimination and in 2015 direct regulation of interconnection as well. At the same time, the jurisdictional foundation for network neutrality has shifted from the general, more flexible provisions of Title I to the more intrusive framework of Title II. What will happen next is anyone's guess, since (as occurred in 2010 after the adoption of the first Open Internet Order) network providers have brought a judicial challenge to reclassification of broadband as a Title II service.

1.2.2 Network neutrality in Europe

Back in 2005, when the *Madison River* case was intensifying the network neutrality debate in the US, the European Commission was deeply convinced that the debate would never gain traction in Europe. Ten years later, it is clear that these early predictions were wrong: since 2009, Europe has been trapped in a fierce discussion, which – as will be clarified at the end of this section – seems to have been recently affected also by the resurgence of protectionism and industrial policy at the EU and at the national level and is likely to reach new policy areas, such as platform neutrality and search neutrality.

The first EU rules on network neutrality were adopted in 2009 and included in Articles 20 and 22 of the then-amended Universal Service Obligations (USO) Directive. Article 20 of the USO

[12] The FCC has also stated it will refrain from applying as many as 27 provisions of Title II, and as many as 700 codified rules, resulting in what the Commission calls a "light-touch" approach for the use of Title II" See FCC (2015, p. 12).

[13] Instead of a separate rule for wireless, the FCC ruled that it would instead simply take engineering attributes into account when assessing reasonable network management.

Directive mandates that network operators that manage traffic should inform end users in a transparent way of the practices they adopt so that users can make an informed choice when deciding whether to subscribe. Article 22 of the USO Directive introduced the possibility for national regulators to intervene and impose a minimum quality-of-service level in case the quality of certain applications became unacceptable for end users, arguably due to traffic management practices.

Despite difficulties faced by national regulators in applying this rule, in late 2013 the 'Connected Continent' proposal presented by the European Commission contained a very similar approach. On the one hand, the proposed package recognised that network neutrality is what keeps the Internet open and as such should be the default principle for all ISPs (Internet service providers) in the EU-28. On the other hand, the proposed rule left the door open to the creation of specialised services through agreements between ISPs and application/content providers, under the condition that such services do not disrupt the open Internet. However, in April 2014, the proposal was significantly modified by the European Parliament, which basically rejected the possibility of specialised services and reinstated network neutrality as an almost insuperable principle for ISPs.

The text of the Connected Continent package is currently under trilogue (negotiations between the European Commission, the European Parliament, and the Council), but a political agreement was announced by the European Commission on 30 June 2015. Under the new agreement, the principle of net neutrality will for the first time be enshrined into EU law: users will be free to access the content of their choice, they will not be unfairly blocked or slowed down anymore and paid prioritisation will not be allowed. In parallel, Internet access providers will still be able to offer specialised services of higher quality, such as Internet TV and new innovative applications, so long as these services are not supplied at the expense of the quality of the open Internet. These rules will be a reality across all member states as soon as the text officially applies on 30 April 2016.[14] Accordingly, the final compromise is closer to the original position of the European Commission and, as such, contemplates the possibility of specialised services and reasonable traffic management. More specifically, the Commission explains that "all traffic will be treated equally, subject to strict and clearly identified public-interest exceptions, such as network security or combating child pornography, and subject to efficient day-to-day network management by Internet service providers".[15]

In summary, the EU position on network neutrality is likely to remain controversial in the coming years: despite the recent political agreement, which will take effect in April 2016, implementation issues are still far from settled.[16] Meanwhile, a number of member states have taken the initiative to regulate the issue, leading to remarkable inconsistencies across the EU. While countries like the Netherlands, Finland and Slovenia have enacted very strict neutrality rules, France has explicitly allowed traffic management practices, and the United Kingdom regards the possibility to charge quality of service fees as a much-needed opportunity for ISPs to monetise their investments in broadband networks.

[14] http://europa.eu/rapid/press-release_IP-15-5265_en.htm.

[15] Ibid.

[16] See Renda (2013) on the lack of detail on the implementation of a rule based on the co-existence of best effort Internet and specialised services.

1.2.3 Will there be convergence on network neutrality rules in the TTIP?

Despite the similarities of the terms of the debate on both sides of the Atlantic, there are many reasons to doubt that there will be explicit convergence on network neutrality in the Digital TTIP, even if – as seems straightforward – such a result would be greatly beneficial for all the players in the Internet ecosystem. First, the state of competition and investment in broadband networks is very different, and accordingly the rationale for intervening on network neutrality (and the likely impact of neutrality rules on the market) is also likely to be very different. Not surprisingly, the FCC has mentioned the lack of real alternatives (beyond one fibre, one cable and wireless network) for consumers in many parts of the United States as the basis for mandating network neutrality in the 2015 Open Internet Order. In Europe, if anything, there is a growing concern that there might be too many telecommunications operators, hence the calls for industry consolidation and the need to foster investment.

Second, the recent ruling of the FCC and the upcoming Connected Continent package in the EU incorporate slightly different rules on network neutrality. A deeper look at the text of the two rules reveals a remarkable degree of uncertainty, both due to the threat of extensive litigation in the United States and to the implementation challenges that the rules will pose on both sides of the Atlantic. As these uncertainties are unlikely to be solved in the coming months, a meaningful agreement on network neutrality seems incompatible with the timing of the first version of the TTIP.

To be sure, finding an agreement on specific issues would be advisable and would add to legal certainty and overall market performance both in the United States and in the increasingly fragmented European Union. Examples include a black list of practices that are always to be considered prohibited (regardless of the market power of the ISP); a grey list of practices that are to be prohibited under well-detailed circumstances; and a white list of allowed practices, to be consistently interpreted and regularly updated in what could become a very useful living agreement.

Finally, the prospects for an agreement on network neutrality chiefly depend on the position that the EU will take in related fields, and most notably in its regulatory reforms on e-commerce and copyright and in the antitrust investigations against Google. All these dossiers are deeply intertwined with network neutrality, not only because they call into question the potential introduction of platform-neutrality obligations; but also since they all directly or indirectly refer to the conduct of US companies in the European territory. We deal with these issues in the sections 2 and 3 below.

2. Antitrust and cyberspace

2.1 How similar are antitrust rules in the US and the EU?

Nowhere have the United States and Europe shown signs of convergence in the past century as they have in the area of antitrust. As a matter of fact, the introduction of rules on competition in the Treaty of Rome in 1957 is seen as largely inspired by the US tradition, starting with the 1890 Sherman Act and the 1914 Clayton Act. And indeed, the rules contained in the antitrust legislation of the two blocs are quite similar. When it comes to antitrust, however, the devil is the details, and the details are numerous. Without pretending to provide an exhaustive explanation, this section explores existing differences with a specific focus on digital markets and the Internet ecosystem.

First, even if the wording of sections 1 and 2 of the Sherman Act and Arts 101 and 102 TFEU is comparable, the two jurisdictions have taken divergent approaches to single-firm conduct ('abuse of dominance' in the EU jargon), due to the prevalence of the Chicago School of economics in the United States and the influence of the more structuralist 'Ordoliberal school' in Europe, starting from the early days of the debate on the Treaty of Rome.[17] This is not only a matter for historians or a subject for academic writings: the different approach has resulted in starkly divergent positions being adopted in merger control (e.g. the *GE/Honeywell* merger cleared in the US but was rejected in the EU in 2001) and also most notably in the area of single-firm conduct (e.g. the US and EU *Microsoft* cases).[18]

Second, some of the most notable differences between the two legal systems on the treatment of single-firm conduct are highly relevant for the electronic communications sector. For example, EU antitrust rules (and consequently, also the 2003 e-communications package) rely heavily on the so-called 'essential facilities' doctrine, whereas the US Supreme Court has never embraced that doctrine. In practice, this means that EU authorities are more likely to mandate asset sharing or compulsory licensing in 'refusal to deal' cases than US authorities. Cases like *Trinko* in the United States contrast sharply with the interoperability stance taken by the European Commission and the Court of First Instance (now the General Tribunal) in their *Microsoft* decisions in 2004 and 2007, respectively. Moreover, the rulings of the Court of Justice of the European Union (CJEU) on issues of predation and margin squeeze (especially the *Telia Sonera* case) have confirmed that EU antitrust dances to a different drummer than the US. In particular, in Europe large companies are explicitly attributed a special responsibility vis-à-vis their market, which has recently led the Court to theorise that large firms should ensure, besides the survival, also the profitability of their smaller rivals.[19] By contrast, the US antitrust law has rejected price squeezes (*linkLine*) and is more equivocal than European law with respect to loyalty rebates (compare *LePage's* with *PeaceHealth*).

Third, differences in the way in which antitrust economics are applied in the two jurisdictions becomes even more acute when it comes to high-tech markets and in particular on the Internet, due to the prevalence of network externalities and multi-sided platforms. Many of these settings tend to be characterised by competition 'for' rather than 'in' the market, as firms compete in a high-risk, high-reward game that produces only one winner. The structuralist view of competition prevailing in the European Union reverberates on the authorities' distrust of this dynamic form of competition (regarding it as a 'sequence of monopolies', rather than a static situation of pluralism), despite the fact that in Europe, just as in the US, market power is not equated with market share, but in principle requires a finding of independence of behaviour.[20] The consequence is that the European Commission can regard certain companies as dominant companies even when they have a high chance of being displaced by market

[17] See Gerber (1994) and Akman (2009).

[18] Renda (2001 and 2004).

[19] See Petit (2014).

[20] Thus, as the European Commission explains on its website: "Market shares are a useful first indication of the importance of each firm on the market in comparison to the others. The Commission's view is that the higher the market share, and the longer the period of time over which it is held, the more likely it is to be a preliminary indication of dominance. If a company has a market share of less than 40%, it is unlikely to be dominant" (see http://ec.europa.eu/competition/antitrust/procedures_102_en.html).

competitors in the generation of their product in what is an ever-changing competitive landscape.

The continental drift in antitrust, exacerbated by the peculiar economics of high-tech markets, lies at the roots of many differences between regulatory practices in the two legal systems, particularly regarding infrastructure regulation and network neutrality. It underlies the US relatively hands-off approach to both merger regulation and single-firm conduct in cyberspace, which contrasts sharply with the EU interventionist approach. And while the numerous antitrust investigations against Microsoft in both jurisdictions over the past 15 years are probably the clearest illustration of the existing divergence, the current European Commission's case against Google is a good example of a case dismissed by the FTC in the United States and currently being re-proposed, with remarkable emphasis, in the European Union. The new European Commissioner for Competition Margarethe Vestager announced on 15 April 2015 that the Commission had sent a Statement of Objections to Google, arguing that the giant IT company abused its dominant position in the "general Internet search" market. The Commission has also launched a similar investigation with respect to the market for mobile operating systems, apps and services. Most importantly, Ms Vestager is accusing Google of having awarded preferential treatment to its own online comparison-shopping service to the detriment of competing services. In so doing, Google has allegedly leveraged its market power in searching into a neighbouring market, thereby foreclosing competitors from that market and thwarting competition on the merits.

2.2 Is an agreement on antitrust principles in cyberspace possible, and desirable?

In the case of antitrust rules, a full agreement between the two parties in the Digital TTIP (and on pending cases) is unlikely for a variety of reasons. First, full alignment of antitrust rules would neither be possible, nor advisable, particularly given that enforcement of antitrust rules is completely different in the two legal systems. The prevalence of private enforcement (i.e. actions before the court aimed at seeking injunctions and damage compensation) in the US contrasts with the almost-exclusive reliance on public enforcement in the European Union, which significantly limits the effectiveness of antitrust rules. To some extent, antitrust rules in the US that appear more light-handed may be more effectively enforced compared with the EU's stricter rules that omit such formidable tools as 'opt-out' class actions, criminal sanctions, punitive damages and contingent fees between lawyers and clients.[21]

Second, the Google investigation is a good example of the attempt to extend the net neutrality debate into the higher layers of the Internet. The main allegation against Google is indeed one of 'non-neutrality': Google is charged with unduly discriminating among Internet content by providing a non-neutral, non-objective view of the Internet. Without entering into the merits of the Google search investigation, which would exceed the scope of this paper, it is clear that advocating neutrality for search engines raises a range of complex issues. And it is also clear that in the United States, any attempt to compel a re-design of Google's home page or the disclosure of Google's algorithm would be seen as contrary to the narrow and deferential

[21] See Renda et al. (2006).

approach towards product design that US courts have followed since the antitrust cases against IBM in the 1970s.[22]

Third, any convergence on antitrust rules would have to dispel the suspicion that some of the most far-reaching antitrust investigations of the past years have been motivated by a combination of competition policy and industrial policy concerns. On the one hand, recent rumours have hinted at possible White House involvement in the FTC decision not to proceed against Google for anti-competitive conduct.[23] On the other hand, the European Commission's current investigation against Google is difficult to disentangle from the calls for enhanced regulation of online intermediaries launched by several institutions, including the European Parliament and the legislatures of France and Germany. If the Google antitrust investigation is part and parcel of a more general tendency towards platform regulation and neutrality, the United States is unlikely to follow Europe. This would not only go against the interests of many US-based companies; it would also contradict the way in which competition policy has been framed and applied in the United States for more than a century.

3. The EU's platform regulation debate: Towards the end of the 'mere conduit' principle?

As briefly mentioned in the previous section, while the network neutrality debate still looms, the Juncker Commission has also launched a new initiative to extend the neutrality principle to Internet platforms. Many official documents published by the European Commission and the European Parliament in the past months allude to the pressing need to limit US-headquartered companies' dominance over the value of the Internet. Since last year, French and German institutions have repeatedly called on the European Commission to split Google into two companies, a recommendation endorsed by the European Parliament in November 2014. The French Digital Council has vigorously called for legislation that would impose neutrality obligations on large Internet platforms, starting obviously from Google but then reaching all of the so-called GAFTAM companies.[24] And the first weeks of the Juncker Commission seem to have emphasised the need to go beyond a 'silo' approach in telecoms and media regulation to address the problem of the rising power of over-the-top (OTT) platforms through a consistent set of legal documents covering competition, copyright, privacy and security issues. What might emerge is an additional layer of regulation and responsibilities for Internet intermediaries, which would be a complete U-turn compared to the early days of the Internet, when legislation such as the EU e-commerce Directive and the US Digital Millennium Copyright Act provided for intermediary immunity to preserve the 'mere conduit' role of network operators as well as the neutrality of the Internet itself.

The most relevant issues currently being examined by EU policy-makers in this context (and most notably included in the Digital Single Market strategy presented by the European Commission on 6 May 2015) are the reform of copyright and e-commerce rules, in particular regarding the liability of online intermediaries. The two must be analysed together, since such

[22] See e.g. *Telex Corp. v. IBM* (1973); *Innovation Data Processing v. IBM* (1984).

[23] See "Inside the US Antitrust Probe of Google", *Wall Street Journal*, 19 March 2015 (www.wsj.com/articles/inside-the-u-s-antitrust-probe-of-google-1426793274).

[24] See Conseil National du Numérique (2014).

reform would represent the revision of a concept that has governed the relationship between both areas of legislation since the birth of the Internet, namely the 'mere conduit' principle.

Regarding copyright, the Commission plans to propose revisions by the end of 2015. The increasingly poor fit between the 2001 Information Society Directive and the features of the evolving Internet ecosystem make the need for such reforms particularly urgent.[25] In particular, the 2001 Directive was adopted at a time when the key principle of Internet regulation was immunising ISPs from liability for the conduct of their subscribers. The US Digital Millennium Copyright Act follows the same approach. Both enactments are strongly linked to the 1996 WIPO Copyright Treaty, which sought to strengthen technological protection measures while preserving the 'dumb pipe' nature of ISPs.[26] Moreover, the 2001 Directive clearly reflects the assumption that digital rights management technologies would become the dominant mechanism for protecting content online, an assumption that has proven wrong in many media sectors. Since then, many member states (with France often being the most vocal) have called for giving ISPs greater responsibility for detecting and even penalising copyright infringements, which would represent a sea change in EU copyright legislation and enforcement.[27] This issue has already proven extremely controversial in the negotiations over the copyright package: during the hectic debate that led to the European Parliament's rejection of the Anti-Counterfeiting Trade Agreement (ACTA) in 2012, ISP liability proved to be a sticking point for both IT companies and civil society.

Reforming the Information Society Directive to introduce ISP liability would also clash with the 'mere conduit' principle introduced in the 2000 e-commerce Directive.[28] This means that any reform of copyright reform necessarily requires reform of EU e-commerce rules as well. In this respect, the European Commission has recently announced a "comprehensive assessment of the role of platforms before the end of 2015 that will examine both the sharing economy, and online intermediaries. Issues will include such as (i) transparency, e.g., in search results (involving paid for links and/or advertisement), (ii) platforms' usage of the information they collect, (iii) relations between platforms and suppliers, (iv) constraints on the ability of individuals and businesses to move from one platform to another, (v) the best way to tackle illegal content on the Internet."[29] The underlying position of the Commission is that while the 'mere conduit' principle enshrined in the e-Commerce Directive has underpinned the development of the Internet in Europe, today blocking access to and removing illegal content by providers of hosting services can be slow and complicated, and "it is not always easy to define the limits on what intermediaries can do with the content that they transmit, store or host before losing the possibility to benefit from the exemptions from liability set out

[25] See Renda et al. (2015).

[26] See WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty, adopted in Geneva, 20 December 1996 (www.wipo.int/treaties).

[27] See France's HADOPI law (Haute Autorité pour la Diffusion des œuvres et la Protection des droits d'auteur sur Internet), which was introduced in 2009 to promote the distribution and protection of creative works on the internet.

[28] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17 July 2000.

[29] See the European Commission's Communication on "A Digital Single Market Strategy for Europe", COM(2015) 192 final, Brussels, 6.5.2015.

in the e-Commerce Directive".[30] In other words, the more ISPs manage and inspect traffic and use data generated by user behaviour, the weaker the justification for exempting intermediaries from liability becomes.

Just like the net neutrality debate, the war on copyright and the 'mere conduit' principle is extending from ISPs into the higher layers of the Internet ecosystem. After large EU countries like Germany, France and Spain have taken action to expand Google's liability for copyright infringement, the European Commissioner for the Digital Single Market Günther Oettinger recently stated that in future EU legislation, "when Google takes intellectual works from within the EU and works with them, then the EU can protect those works and demand a levy from Google." However, recent history about the likely impact of current plans to strengthen copyright liability are not encouraging: the two existing examples of ancillary copyright being rolled out nationally, in Germany and in Spain, seem to have largely backfired.[31]

Finally, one critical component of the current debate on copyright and e-commerce reform is the aggressive stance adopted by the European Commission against so-called 'geo-blocking' practices, now being considered as one of the worst obstacles on the way to market integration, and accordingly included in the new EU Digital Single Market strategy.[32] Geo-blocking refer to commercial practices that either prevent online customers from accessing and purchasing products and services from a website based in other member states or automatically re-route requests to a domestically located store. As a result of these practices, consumers are often charged more for products or services (particularly music or audio-visual) purchased online on the basis of their IP address, their postal address, or the credit card used to make the purchase. Again, practices adopted by US-based e-commerce giants like Amazon are often quoted as the real target of initiatives of this kind. This suspicion was strengthened by the launch, on 6 May 2015, of a Competition Sector Inquiry to assess whether geo-blocking restrictions (often embodied in contractual and distribution agreements for online trade of tangible goods but also in the licensing of audio-visual and content online services) constitute undue barriers to cross-border online shopping;[33] and finally confirmed by the subsequent opening, on 11 June 2015, of an antitrust investigation against Amazon for certain business practices adopted in the distribution of electronic books.[34]

In conclusion, the EU seems to have opened a debate on issues that are largely underexplored in the United States. This is partly justified by the greater integration of the US internal market (at least in terms of geo-blocking practices). But at the same time, it also reflects the fact that Europe is increasingly considering policies to re-distribute revenues along the Internet value chain, away from large IT intermediaries and towards content producers (in copyright

---

[30] Ibid.

[31] In Germany, local publishers were forced to grant Google free use of their text snippets and thumbnails after the company delisted them from Google News, and traffic to their websites predictably plummeted. In Spain, the severity of the local ancillary copyright law has created an even-worse situation – the publishers, who lobbied for the law, cannot grant Google free access even if they want to do so, and now Google has axed Google News in Spain altogether, again causing a precipitous drop in traffic to publishers' websites.

[32] European Commission's Communication, "A Digital Single Market Strategy for Europe", COM(2015) 192 final, Brussels, 6.5.2015.

[33] http://europa.eu/rapid/press-release_IP-15-4921_en.htm.

[34] http://europa.eu/rapid/press-release_IP-15-5166_en.htm.

legislation) and infrastructure operators (deviations from net neutrality). We consider it quite unlikely that any measure on intermediary liability and deviations from the mere conduit principle, if actively pursued by the European Commission within a Digital TTIP, would be subject of an agreement. Moreover, an agreement on platform liability based on the emerging EU approach would likely be unfortunate in economic and legal terms. Imposing heavy obligations on emerging Internet intermediaries both in terms of neutrality and liability for copyright and privacy would amount to a true oxymoron: treating them as dumb pipes on the one hand and as editors of content on the other.

4. End user information and accessibility issues

Among the many issues that are under discussion in the final TTIP agreement, one of the most promising relates to consumer protection issues, particularly e-labelling and e-accessibility. The first issue relates to the possibility of displaying some of the required and voluntary product information via a product's screen instead of physically affixing a permanent label to the product. Electronic marking would ensure that any changes to any labelling mandated by regulation can be updated more easily and therefore be more likely to remain current. In addition, the use of electronic marking would enhance consumers' ability to access and understand the regulatory information as well as facilitate access by disabled users. It would reduce costs and reduce time to market.

On the specific issue of e-labelling, legislation has already been enacted in both legal systems. However, the EU legislation was adopted specifically for medical devices and limited to the provision of instructions for use. In particular, Regulation 207/2012 on electronic instructions for use of medical devices specifies how to build the instructions for use in a medical device's label in an electronic format and the devices for which they may be used.

In the United States, the Enhance Labelling, Accessing, and Branding of Electronic Licenses Act of 2014 (E-LABEL Act) was signed by President Obama at the end of November 2014. The Act requires the FCC to allow manufacturers of radio-frequency devices to use electronic labelling for the equipment instead of affixing physical labels to the equipment. The statute defines "radio-frequency device with display" as any equipment or device that 1) requires the FCC's authorisation before the equipment or device may be marketed or sold within the United States and 2) is capable of digitally displaying required labelling and regulatory information. On 10 July 2014, the FCC also issued guidance describing how devices with integrated displays can present label information electronically.

Despite the differences in the frameworks adopted by the two legal systems, there should be no significant obstacle to the adoption of common solutions on e-labelling in the Digital TTIP. The starting point could be the US guidance on how to present information, with further discussions focusing on issues such as the clarity and user-friendliness of the message to be displayed, as well as the modalities of the transmission.

In contrast, e-accessibility has been one of the core issues discussed by the Transatlantic Economic Council throughout the past decade. Back in December 2005, the European Commission issued standards mandate n. 376 (M376) to harmonise and facilitate the public procurement of accessible ICT products and services and to enable public procurers to make use of these harmonised requirements in the procurement process. The intention of M376 was already aimed at achieving a degree of similarity with Section 508 of the US Rehabilitation Act of 1973 (S508), but the industry has long criticised the two standards as needlessly different,

and has been calling for further harmonisation for a long time.[35] Since then, the M376 and S508 teams have been working without frequent technical exchanges and on different schedules at a time when close cooperation is vital for success. Currently, work is underway to ensure better coordination, and the S508 standard is being revised following a proposal by the US Access Board, which aims to merge them with its guidelines for telecommunications equipment and customer premises equipment covered by section 255 of the Communications Act of 1934. The proposed revisions and updates to the section 508-based standards and section 255-based guidelines are intended to ensure that ICT covered by the respective statutes is accessible to and usable by individuals with disabilities. Both parties in the TTIP can use as a reference the Web Content Accessibility Guidelines (WCAG) 2.0, an international standard prepared by a working group composed of academics and corporate representatives within the World Wide Web Consortium (W3C).

Agreements on both e-labelling and e-accessibility appear to be attainable for the Digital TTIP chapter. The European Commission's TTIP factsheet on the information society concurs, and there is no reason to expect negotiations to fail on these issues.

In addition to these matters, which have been part of the transatlantic dialogue for quite some time, other related topics might also find their way into an initial agreement. These include consumer protection standards or rules for e-health and in particular M-health applications, on which the industry has been quite vocal over the past months.

5. The Internet of Things and smart manufacturing

One of the most important current developments in the digital sector is the advent of the Internet of Things (IoT). According to major IT companies such as Cisco and Huawei, the number of devices connected to the network globally is projected to grow from fewer than 10 billion to more than 50 billion devices by 2020. The quest for connecting the "remaining 99% of things" that have not been connected to date and for capturing market share in the run-up to the IoT age is one of the most vibrant competitive races of our time. Like all network-based phenomena, IoT is a natural candidate for global standards in order to allow market participants to fully realise the benefits of scale economies and network economic effects. As a result, one would expect the many industrial sectors involved to share an interest in developing standards and rules that will be adopted worldwide. Indeed, a number of industry players have called for including harmonised rules for IOT within the TTIP, especially on the manufacturing side. However, the temptation to develop incompatible standards as a way to protect domestic industry is reportedly emerging, in particular on the EU side.

In the US, since February 2010, manufacturing has added more than 700,000 jobs, the fastest pace of job growth since the 1990s. In order to continue this extraordinary momentum, the Obama Administration launched an Advanced Manufacturing Partnership (AMP) within the President's Council of Advisors in Science and Technology. President Obama then launched four manufacturing innovation institutes with four more on the way; invested nearly $1 billion

[35] The problems are exemplified by the delay in the publication of the latest US Advanced Notice of Proposed Rule-making (ANPRM) version of S508 that was announced by the US Access Board in early October 2011. Because of the lack of exchange of information, this delay has caused a problem for the EU M376 team that could lead to a harmonisation failure.

to upgrade our community colleges to train workers for advanced manufacturing jobs; expanded investments in applied research for emerging, cross-cutting manufacturing technologies; and launched a new initiative to deploy the talent of returning veterans to in-demand jobs, including advanced manufacturing. The AMP delivered its final report in November 2014, making recommendations addressing three key pillars that support American manufacturing: 1) enabling innovation, 2) securing the talent pipeline and 3) improving the business climate. These recommendations are now being followed up by executive actions in all three areas.

In Europe, work on advanced manufacturing has been underway, especially since the launch of the 7th Framework Programme for Research (followed in 2014 by the Horizon 2020 program) and the Europe 2020 strategy announced in 2010, which contained a flagship initiative dedicated to an Industrial Policy for the Globalisation Era. However, the March 2014 report of the European Commission's Task Force on Advanced Manufacturing for Clean Production acknowledged that initiatives so far have remained mostly patchy and isolated.[36] But the new European Commission seems willing to shift gears and is reportedly ready to adopt a non-legislative initiative that will expand the *Industrie 4.0* already launched by the German government in cooperation with industry and academia in 2011 to the pan-European level. The use of cyber-physical objects and equipment in the factories of the future is often described as the 'fourth industrial revolution', which might prove so disruptive that it is expected to bring about paradigm shifts in modes of production and distribution.

Industry 4.0 is indeed powered by a mix of technologies, which include nano-technologies and IoT technologies that design and realise smart objects, cloud computing technologies for the low-cost storage of data and applications, a mix of wireless technologies for always-on connectivity (including 5G), advanced robotics, 3D printing, and big-data analytics for optimised management of the supply chain. A report by PwC for the German government estimated that over the next five years, a yearly investment of as much as €40 billion might bring an 18% increase in the productivity of German industry and a 12% increase in the industry's turnover[37].

However, the Europeanisation of the German *Industrie 4.0* strategy will not come without consequences. First, it is to be anticipated that all other member states will find the initiative less attractive, since they do not feature the same industry leadership that Germany still enjoys in some sectors. Germany's market for embedded systems, i.e. computer *systems* with a dedicated function within a larger mechanical or electrical *system*, generates €20 billion annually (expected to reach €40 billion by 2020) and ranks third in the world behind the US and Japan. Other countries do not reach anywhere near these figures and thus have much lower chances to develop industrial leadership in most of the technologies involved. At the same time, countries like Italy (second only to Germany in terms of industry size in Europe) feature a completely different industry structure, with a myriad of micro-enterprises that would lack the scale to fully capitalise on a pan-European initiative of this size.

But perhaps the most worrying aspect of the European side of the debate is the possibility that some of the key industry players involved in *Industrie 4.0* might decide to develop standards

[36] See http://ec.europa.eu/growth/industry/innovation/advanced-manufacturing/index_en.htm

[37] See PwC, Opportunities and challenges for the Industrial Internet, 2014, available at http://www.pwc.nl/en/publicaties/industrie-4-0.jhtml.

that are incompatible with those being developed in the US, in particular when it comes to cloud computing, but also with respect to supply chain management. One possible example is the recent joint initiative launched by Deutsche Telekom and SAP to merge production technology with IT and telecommunications. The CEO of Deutsche Telekom recently observed: "We don't need to fear standards from the United States. We want Germany's voice to be heard as well on such an important issue."[38] The emergence of national standards in such a globalised industry is apparently motivated by industrial policy, such as the need to counter the current leadership of US-based companies, such as AT&T, Cisco, IBM, Intel and General Electric, which dominate the top standards alliances in this field, including the Industrial Internet Consortium, the Open Interconnected Consortium and the AllSeenAlliance. But an additional motivating factor is the desire to respond to the Snowden revelations by creating a national environment in which data will be preserved within German territory – the so-called 'German cloud' (or, at least, a European cloud), already invoked a few times by Chancellor Angela Merkel.[39]

In summary, an agreement on IoT standards would be highly desirable in the Digital TTIP and would likely speed up the deployment of *Industrie 4.0* technologies. However, such an agreement is unlikely to occur, since both parties are deploying advanced manufacturing strategies as part of their industrial policy initiatives and are therefore acting more as competitors than as allies. In addition, the NSA scandal seems to be making an agreement in this field harder to reach and appears to be spurring the development of incompatible standards.

6. A continental drift in data protection?

No other issue related to the online world has been as prominent in the debate over the TTIP as data protection. Even before the Snowden revelations, the issue was almost intractable in transatlantic regulatory cooperation. Against this background, the emergence of the Internet, and even more of cloud computing, creates significant legal challenges alongside undoubted potential benefits. Cloud computing permits a degree of flexibility that makes it increasingly difficult to identify who should be held accountable vis-à-vis cloud customers for the handling and processing of personal data and on the legal regime that should govern data transfers outside the US and EU jurisdictions (Hon et al., 2011a, 2011b, 2012; Schwartz, 2013; Schwartz & Solove, 2013). This section briefly describes the existing legislation on privacy in the US and the EU and the current debate on the regulation of transatlantic data flows. Section 6.1 introduces the main privacy laws (along with case law and enforcement practice) in the United States and the EU. Section 6.2 discusses the Safe Harbour regime and the Binding Corporate Rules. Section 6.3 briefly concludes by illustrating possible 'landing zones' in current TTIP negotiations or in separate deals.

6.1 Privacy law in the United States and in the EU

The United States and the European Union have always followed different legal approaches to privacy and data protection (Schwartz & Solove, 2013). First, the US has traditionally relied

[38] https://www.telekom.com/media/company/271966.

[39] See, inter alia, Hilmar Schmundt and Gerald Traufetter, "Digital Independence: NSA Scandal Boosts German Tech Industry", *Der Spiegel*, 4 February 2014.

on piecemeal, sectoral regulation and private ordering to address privacy issues. The European Union, in contrast, enacted the first horizontal, omnibus data protection laws in the 1970s followed by the adoption of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in 1981 and the enactment of the EU Data Protection Directive 95/46 in 1995. Moreover, in Europe privacy is explicitly considered as a fundamental right, whereas the US Constitution contains no explicit reference to privacy.[40] Many prominent US scholars consider privacy as amounting to a property right, i.e., an alienable commodity that can be traded in exchange for customised service. Finally, in the US privacy legislation and case law traditionally focused on the protection of the citizen against violations and misbehaviour of public authorities (also due to the scope of the Fourth Amendment), whereas in the EU the focus is rather on the private sector. In a widely cited article published in the *Yale Law Journal*, James Whitman (2004) interpreted the fundamental divergence between the legal approaches to privacy in the US and the EU as rooted in a cultural difference between those who view privacy as an aspect of liberty and those who regard privacy as an aspect of dignity.[41]

6.1.1 Privacy laws in the United States

In the United States, the right to privacy is historically and legally rooted in the Fourth Amendment, which provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The Supreme Court initially framed such a right with respect to the confidentiality of personal postal correspondence such as letters and sealed packages.[42] Over the past few decades, various scholarly approaches to privacy have emerged, mostly viewing privacy as control over data and framing it as a commodity rather than a fundamental right, with important consequences in terms of its alienability (Solove, 2006).

Regarding statutory law, early attempts to regulate privacy include the Fair Credit Reporting Act (FCRA) of 1970 and the Family Educational Rights and Privacy Act (FERPA) of 1974. Other federal statutes addressing specific privacy issues include the Children's Online Privacy Protection Act (COPPA), the Health Information Portability and Accessibility Act (HIPAA),

---

[40]The term 'privacy' does not appear explicitly in the US Constitution or the Bill of Rights. However, the US Supreme Court has ruled in favour of various privacy interests, deriving the right to privacy from the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments to the Constitution.

[41] See Whitman (2004, p.161) quoting Post (2001), and arguing: "Continental privacy protections are, at their core, a form of protection of a right to respect and personal dignity …By contrast, America, in this as in so many things, is much more oriented toward values of liberty, and especially liberty against the state."

[42] See *Ex parte Jackson* (1878) in which the US Supreme Court ruled: "The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be … No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the fourth amendment of the Constitution." Later, the US Supreme Court has ruled in favour of various privacy interests – deriving the right to privacy from the First, Third, Fourth, Fifth, Ninth and Fourteenth Amendments to the Constitution.

the Electronic Communications Privacy Act (ECPA), and the Gramm-Leach-Bliley Act (GLBA). Several of these federal statutes focused on the presence of 'personally identifiable information' while others focus on transparency and access to information, on protecting consumers from inappropriate use of their personal data or on imposing duties of confidentiality. Of these statutes, the most relevant are certainly ECPA (in particular its Title II, also known as the Stored Communications Act), the US PATRIOT Act and the FAA. All these statutes have received criticism over the past few years: while ECPA (and its Title II in particular) has been criticised for having been largely outpaced by technological innovation, and in particular by cloud computing, the *Uniting and Strengthening America Provide Appropriate Tools Required to Intercept and Obstruct Terrorism* (US PATRIOT) Act of 2001 was criticised for provisions that can lead companies to turn over data to the US government even without notice to the customer. Data stored outside US borders, if held in servers owned by a US company, are potentially covered by this provision: even contract provisions specifying that data will be governed by foreign law can be ignored by the US government.[43] But the most heavily criticised provision is certainly the Foreign Intelligence Surveillance Amendment Act (FAA), which amended the 1978 Foreign Intelligence Surveillance Act. Section 1881a of the FAA introduces the possibility for the US government to monitor foreign communications and access data of foreign citizens located outside of the US without a warrant (a requirement that, by virtue of the Fourth amendment, would apply only to US citizens). A recent report for the European Parliament observed that "while there has been a great deal of concern at the international level over the US PATRIOT Act, there has been virtually no discussion of the implications of … § 1881a of FAA," which "for the first time created a power of mass-surveillance specifically targeted at the data of non-US persons located outside the US, which applies to cloud computing" (Bigo et al., 2013).

Beyond privacy legislation and case law, which mostly focuses on the possibility for government institutions to inspect personal data and communications, an increasingly important player in the privacy domain is the Federal Trade Commission in its role of consumer protection enforcer. The number of investigations and sanctions accumulated by the FTC over the past few years is remarkable (Cline, 2014). To be sure, the FTC has filled an important gap in US privacy law by protecting customers against privacy- and security-reducing practices adopted by their providers. However, there seems to be significant space for a clarification of the FTC powers, as well as of the criteria and definitions used by the FTC in enforcing legislation to protect consumer privacy and data security.

All entities that store consumer information on the Internet face the threat of FTC enforcement if the way they store and secure information does not match their declarations to their customers. This unfair behaviour amounts to a deceptive or unfair practice under Section 5 of the FTC Act. In addition, the FTC enforces a handful of sector-specific privacy laws, including COPPA, GLBA, FCRA, TCPA and the Telecommunications Act, as well as the EU-US Safe Harbour (see below).[44]

---

[43] Specifically, section 215 of the Patriot Act allows the FBI to access data related to investigations in an *ex-parte* proceeding with the requirement that "no person shall disclose to any other person … that the [FBI] has sought beyond privacy legislation and case law … or obtained things under this section."

[44] Under Section 5, a trade practice is:

6.1.2 The EU legal framework for data protection

The first European data protection laws were enacted in the 1970s, followed by the adoption of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in 1981. At the EU level, the right to privacy has been so far regulated by Data Protection Directive 95/46 (1995) (DPD), which, however, does not cover judicial and police cooperation.[45] Other relevant legislation in force include the 2002 and 2009 e-Privacy Directives and the data retention Directive, which has however been declared invalid by the Court of Justice in a recent decision. The EU data protection Directive applies to data held both by the public sector and the private sector. There are, however, important exemptions that give government the possibility to access and process data for tax and criminal law purposes. As a result, it is fair to state that, contrary to what occurs under US statutory law, the main EU Directive applies far more stringently to the private sector than to the public sector.

In terms of scope, the DPD focuses on the protection of personal data, which it defines as "information relating to an identified or identifiable natural person". No data protection rules will apply at all where data are not personal but are instead anonymous, i.e. "data rendered anonymous in such a way that the data subject is no longer identifiable" (Recital 26). The DPD identifies three main classes of persons to whom EU data protection law applies:

- Data controllers, who are those persons who determine the purposes for which and the means whereby personal data are collected and processed;
- Data processors, who act under the instruction of controllers and do not themselves decide the processing purposes and
- Data subjects, the individuals whose personal data is being processed.

The DPD directed member states to impose legal obligations on controllers to protect personal data by complying with certain principles when processing personal data, including transparency, purpose specification and limitation and erasure, meaning that personal data that are not necessary anymore must be erased or truly anonymised.

Besides the DPD, privacy laws in the EU also include the e-Privacy Directive (as amended in 2009), which forms part of the regulatory framework for electronic communications and introduces obligations of security and confidentiality for providers of e-communications only. It deals with a number of important issues, such as confidentiality of information, treatment of traffic data, spam and cookies. Security of services includes the duty to inform the subscribers whenever there is a particular risk, such as a virus or other malware attack. Confidentiality obligations are addressed at member states, who should prohibit listening, tapping, storage, or other kinds of interception or surveillance of communication and related

- Deceptive, if it involves a "material representation, omission or practice that is likely to mislead a consumer acting reasonably in the circumstances, to the consumer's detriment";
- Unfair, if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits to consumers or competition" (the so called 'three-part test' of Section 5(n) of the FTC Act).

[45] Such area is currently covered by the Council of the European Union's 2008 Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

traffic, unless the users have given their consent or conditions of Article 15(1) have been fulfilled.

Finally, the data retention Directive (2006/24/EC) was adopted to amend the e-Privacy Directive to provide a more effective response to the terrorist attacks in New York 2001 and Madrid in 2004. It focused on the regulation of data retention to permit access by law enforcement authorities for a certain period if necessary as a means for prevention, investigation and prosecution of serious crime as defined by each of the member states in its national law. In April 2014, a judgment of the CJEU held that the directive was invalid as it "interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data". Hence, "by adopting the Data Retention Directive, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality". This judgment might constitute an important precedent for the interpretation of the validity of existing US legislation (e.g. the FAA) in the EU context and shows that even security issues are unlikely to trump privacy when it comes to EU legislation and CJEU case law.

Recently, in evaluating the data protection Directive and related legislation, the European Commission acknowledged that the legal framework needs an update, both in light of the new challenges posed by technological developments and differences in the ways that member states have transposed and enforced the DPD. Moreover, the application of the EU data protection *acquis* in the area of police cooperation and judicial cooperation in criminal matters, in particular the 2008 Framework Decision, resulted in gaps and inconsistencies (European Commission, 2012). Accordingly, the Commission proposed a strong and consistent legislative reform, which consists of a Regulation (replacing Directive 95/46/EC) setting out a general EU framework for data protection[46] and a Directive replacing the 2008 Framework Decision setting out rules on the protection of personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities.

The new proposed rules aim to improve individuals' ability to control their data by ensuring that when their consent is required, it is given explicitly, meaning that it is based either on a statement or on a clear affirmative action by the person concerned, and is freely given; equipping internet users with an effective 'right to be forgotten' in the online environment[47]; guaranteeing easy access to one's own data and a right to data portability; and reinforcing the right to information so that individuals fully understand how their personal data are handled, particularly when the processing activities concern children. The rules also seek to improve the means for individuals to exercise their rights by strengthening national data protection authorities' independence and powers and enhancing administrative and judicial remedies when data protection rights are violated. In particular, qualified associations will be able to bring actions to court on behalf of the individual. Finally, the new rules aim at reinforcing data security by encouraging the use of privacy-enhancing technologies, privacy-friendly default settings and privacy certification schemes and introducing a general obligation for data

[46] It should be noted that the choice of a Regulation replacing the DPD implies much less discretion in the implementation of the text at national level, as the Regulation is directly applicable and requires no transposition measure by EU member states.

[47] The right to be forgotten is described as the right to have one's data deleted if the owner withdraws his/her consent and if there are no other legitimate grounds for retaining the data (see European Commission, 2012).

controllers to notify both data protection authorities and data subjects about data breaches without undue delay. This implies measures aimed at enhancing the accountability of those processing data: companies with more than 250 employees and in firms that are involved in processing operations which, by virtue of their nature, their scope or their purposes, present specific risks to the rights and freedoms of individuals will be asked to designate a Data Protection Officer. The proposed regulation also foresees very harsh sanctions for non-compliance.

In a recent commentary, Berkeley Professor Paul Schwartz (2013) observed that the proposed new rules would significantly affect US companies' daily practice of authorising the sharing of personal information through simple 'notice and consent'. As mentioned, the Proposed Regulation lists 'consent' as one of the legal justifications for the processing of personal data, but requires that written consent for personal information processing be presented in a form 'distinguishable' from any other matter. More importantly, Article 7 of the proposed text places the burden of proof of demonstrating consent on the controller. This requirement "heightens the risk that a user's consent will not stand up if a data protection commissioner or the user herself challenges the assent after the fact."

Finally, and most problematically, the proposed Regulation states that consent "shall not provide a legal basis for the processing" when "there is a significant imbalance between the position" of the controller and the party to whom the data refers. Thus, Internet companies would not be able to justify processing by a party's consent if they offer take-it-or-leave-it terms for the processing of personal data or provide services for employees or other parties that lack effective bargaining power. As a consequence, Schwartz concludes that US IT companies will not be able to rely on one-sided click-through agreements. The new rules are far-reaching also in terms of jurisdiction, since the proposed Regulation potentially subjects all cloud services to EU privacy law.

The effect of the expansion of the remit of EU data protection rules is already being felt while the general Data Protection Regulation is still pending final approval by EU institutions. In May 2014, the European Court of Justice (CJEU) ruled against Google in *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*, a case brought by a Spanish individual who requested the removal of a link to a digitised 1998 article in *La Vanguardia* newspaper about an auction for his foreclosed home for a debt that he had subsequently paid.[48] The court ruled in *Costeja* that search engines are 'data controllers' and, as such, are responsible for the content to which they point. Thus, Google was required to comply with EU data privacy laws. In so ruling, the Court also clarified that even if the physical server of the search engine operator processing the data is located outside Europe, EU rules apply if the operator has a branch or a subsidiary in a member state that promotes the selling of advertising space offered by the search engine. Moreover, search engines are to be considered controllers of personal data. Google can therefore not escape its responsibilities under European law when handling personal data by saying it is a search engine. EU data protection law applies, and so does the right to be forgotten. Furthermore, the CJEU ruled that individuals have the right – under certain conditions – to ask search engines to remove links with personal information about

[48] Costeja initially attempted to have the article removed by complaining to Spain's data protection agency, which rejected the claim on the grounds that it was lawful and accurate, but accepted a complaint against Google and asked Google to remove the results. Google sued in the Spanish *Audiencia Nacional*, which referred a series of questions to the CJEU.

them. This applies where the information is inaccurate, inadequate or excessive and is subject to a balancing test with other fundamental rights such as freedom of expression. The responsibility for performing this test rests with the data controller in the first instance.

The *Costeja* case is a good example of the tendency, increasingly evident in Europe, to expand the territorial scope of EU data protection rules to avoid their circumvention by the locating of servers outside the territory of the EU and to increasingly ask online intermediaries to cooperate in the enforcement of the EU rules. The latter tendency is, indeed, consistent with other reforms currently being discussed in the EU, including the proposed reform of the 2001 Information Society Directive and the 2000 e-Commerce Directive.

6.2 Cross-border data flows: What future for the US-EU Safe Harbour?

The EU data protection Directive also governs the transfer of data, permitting data transfers only to other countries with an 'adequate' level of protection. The US does not appear on the list of countries with 'adequate' protection. However, the US Department of Commerce (DoC) in consultation with the EU developed a Safe Harbour agreement so that that US companies can transfer European data to the United States if the company handling the transfer essentially complies with the DPD in handling and processing the data. Today, almost 5,000 organisations are reportedly certified under the Safe Harbour framework.

Safe Harbour principles include the following:

- *Notice*: Individuals must be informed that their data are being collected and about how it will be used.
- *Choice*: Individuals must have the option to opt-out of the collection and forward transfer of the data to third parties.
- *Onward transfer*: Transfers of data to third parties may only occur to other organisations that follow adequate data protection principles.
- *Security*: Reasonable efforts must be made to prevent loss of collected information.
- *Data integrity*: Data must be relevant and reliable for the purpose for which it was collected.
- *Access*: Individuals must be able to access information held about them and correct or delete it if it is inaccurate.
- *Enforcement*: There must be effective means of enforcing these rules.

The Safe Harbour has always been controversial: in Germany, data protection authorities have voiced their concerns since 2010.[49] After the Snowden revelations, some member states, the European Commission and, in March 2014, the European Parliament called for a suspension and a thorough revision of the Safe Harbour.[50] Meanwhile, on the basis of a thorough analysis

[49] In 2010, the Dusseldorf Kreis, a working group comprised of 16 German state DPAs that are responsible for the private sector, issued a resolution requiring German data exporters to exercise additional diligence when transferring data to Safe Harbour-certified organisations, and prohibited German data exporters from relying solely on Safe Harbour in order to transfer data to the US, By requiring additional diligence, the resolution appeared to question Safe Harbour, and whether the system was sufficient to demonstrate an adequate level of protection for personal data.

[50] In July 2013, the Conference of the German Data Protection Commissioners, including both federal and state Commissioners, issued a press release stating that surveillance activities by foreign intelligence and security agencies threaten international data traffic between Germany and countries

and consultations with companies, the European Commission made 13 recommendations to improve the functioning of the Safe Harbour scheme. The Commission called on US authorities to identify remedies by summer 2014 (but the deadline was not met). The Commission would then review the functioning of the Safe Harbour scheme based on the implementation of these 13 recommendations.

The Commission's recommendations address four key areas.

- First, in terms of *transparency*, the Commission recommended that self-certified companies should publicly disclose their privacy policies, that online Safe Harbour privacy policies should include a link to the Department of Commerce's Safe Harbour list of current Safe Harbour members, that self-certified companies publish privacy conditions of any contracts they conclude with subcontractors, and that the DoC's Safe Harbour list clearly flags those companies that are not current members.
- Second, on *redress*, the Commission stated that online Safe Harbour privacy policies should include a link to the chosen Alternative Dispute Resolution (ADR) provider, that the ADR choice should be readily available and affordable, and that the DoC should systematically monitor ADR providers, specifically in relation to the transparency and accessibility of their procedures and how they follow up complaints.
- Third, concerning *enforcement*, Safe Harbour members should be subject to spot check *ex-officio* investigations in order to verify the substantive compliance of their privacy policies. In addition, where there has been a finding of non-compliance, follow-up investigations should be implemented after one year. The DoC should inform the competent EU DPA of pending complaints and suspected non-compliance. Finally, allegations of false claims of Safe Harbour adherence should be investigated thoroughly.
- Finally, on the issue of *access to data* by US authorities, the Commission stated that Safe Harbour privacy policies should specify the extent to which US law allows public authorities to collect and process data transferred under Safe Harbour and that the national security exception under Safe Harbour should be used only to the extent strictly necessary or proportionate.

In addition to the recommendations, new developments have created even more tensions between the two blocs. The concerns, initially voiced mostly with respect to existing legislation, have also gradually moved towards questioning the conduct of giant online intermediaries, accused of infringing even the principles of the Safe Harbour. Most notably, Austrian privacy activist Max Schrems argued that the National Security Agency's PRISM programme has shown that no meaningful data protection for Europeans exists under US law and that Facebook Ireland was "facilitating the processing of such data."[51] In a letter dated 26 July 2013, the Irish Data Protection Commissioner refused to investigate Facebook because the

outside the EEA. In light of these recent developments, the German Commissioners decided to stop issuing approvals for international data transfers until the German government can demonstrate that unlimited access to German citizens' personal data by foreign national intelligence services complies with fundamental principles of data protection law (namely, necessity, proportionality and purpose limitation).

[51] *Schrems v Data Protection Commissioner* [2014] IEHC 310; [2014] 3 CMLR 37 (text freely available at <www.europe-v-facebook.org/hcj.pdf> accessed 14 November 2014).

Irish branch of the company was registered under the Safe Harbour arrangement and provided access to US law enforcement. Following these considerations, the Irish High Court decided on 18 June 2014 to refer the case to the CJEU. While the ruling is expected by the end of 2015, various committees of the European Parliament have called for an official intervention in the case. The opinion of the CJEU's Advocate General on this case, originally expected on 24 June 2015, has meanwhile been delayed. At the same time, a coordinated series of investigations into Facebook's privacy practices is being carried out by privacy regulators in the Netherlands, Spain, France and Germany. On 15 May 2015, Belgium's Privacy Commission released a report examining the new privacy policies that Facebook implemented this year for use of data from its services, which include Instagram and WhatsApp, to target advertising. The report observes that Facebook processes the personal data of its members as well as other Internet users "in secret", without asking for consent or adequately explaining how the data would be used; and the president of the Belgian authority publicly stated: "The way in which [Facebook] is contemptuous of the private lives of its members and of all Internet users demands action."[52]

As tensions mount in the EU, the US has shown signs of reaction. In 2014, the FTC brought several instances of enforcement, including high-profile actions against MySpace, Facebook, and Google.[53] In 2015, actions were brought against companies that were falsely claiming to be under Safe Harbour certification in an attempt to show more concern for the adequacy of the Safe Harbour's self-certification procedure.[54] Similarly, the Department of Commerce, which is responsible for administering the programme, is likely to increase the rigor with which it oversees the programme. While the certification process is a self-certification programme and not subject to formal regulatory approval, an increase in substantive focus from the Department of Commerce during the certification phase and thereafter is likely as a result of the pressure from Europe.

Moreover, both courts and legislators have taken action to address the problem of bulk collection of metadata. An important legal clarification came recently from the US Court of Appeals for the Second Circuit in *ACLU v. Clapper*, in which the Court ruled that the NSA's bulk collection of phone and other records was never authorised under section 215 of the US

---

[52] See "Belgian Watchdog Raps Facebook for Treating Personal Data 'with Contempt'", Lisa Fleischer and Tom Fairless, *Wall Street Journal*, 15 May 2015 (www.wsj.com/articles/belgian-watchdog-slams-facebooks-privacy-controls-1431685985).

[53] See e.g. "Google, Facebook, MySpace: Privacy rule breakers or trend makers?", John Fontana, ZDNet (www.zdnet.com/article/google-facebook-myspace-privacy-rule-breakers-or-trend-makers/).

[54] In January 2014, the FTC announced settlements with 12 companies that allegedly falsely claimed they complied with Safe Harbour, even though there were no substantive violations of the Safe Harbour privacy principles. In February, the Commission announced a proposed settlement with Fantage.com for allegedly deceptively claiming in its privacy policy that it held a current Safe Harbour certification, when in fact its certification had lapsed in June 2012. In May 2014, the FTC announced a settlement with the clothing manufacturer American Apparel related to charges that the company falsely claimed to comply with Safe Harbour, even though it had allowed the certification to expire. In November 2014, the FTC announced that data privacy certifier True Ultimate Standards Everywhere, Inc. ('TRUSTe') agreed to settle charges that the company deceived consumers about its Safe Harbour recertification programme (see Press Release, "FTC Settles with Two Companies Falsely Claiming to Comply with International Safe Harbour Privacy Framework", 7 April 2015 at www.ftc.gov/news-events/press-releases/2015/04/ftc-settles-two-companies-falsely-claiming-comply-international).

PATRIOT Act. The appellate court's decision in *ACLU v. Clapper* is the culmination of a series of lawsuits by activists and the civil liberties community aimed at putting an end to the NSA's mass surveillance programmes.

This decision arrived just as the US PATRIOT Act (set to expire at the end of May 2015) was being replaced by the US Freedom Act, approved by the House Judiciary Committee on 19 May 2015, and now finally signed into law on 2 June 2015.[55] The new Act explicitly bans the limitless collection of telephone data by forcing the government to use a 'specific selection term' (SST) in any surveillance warrant and replaces the centralised bulk-data collection system with an obligation for network providers to store data and, upon request, deliver it to the government. More specifically, the Act requires the FBI, in applications for ongoing production of call detail records for investigations to protect against international terrorism, to show reasonable grounds to believe that the call detail records are relevant to such investigation; and a reasonable, articulable suspicion that the SST is associated with a foreign power or an agent of a foreign power engaged in international terrorism or activities in preparation for such terrorism.

The Act also requires a judge approving such an ongoing release of call detail records for an investigation to protect against international terrorism to limit such production to a period not to exceed 180 days but allow such orders to be extended upon application, subject to approval by the FISA Court. The Act will allow the government to require the production of an initial set of call records using the reasonable, articulable suspicion standard that the term is associated with a foreign power or an agent of a foreign power and then a subsequent set of call records using session-identifying information or a telephone calling-card number identified by the specific selection term that was used to produce the initial set of records (thus limiting the government to what is commonly referred to as two 'hops' of call records). The government should however adopt minimisation procedures requiring prompt destruction of produced call records that are not foreign intelligence information.

This new system has been criticised for failing to remove massive data collection (which, critics say, is only delegated to private corporations), and at the same time reducing the efficiency and effectiveness of government surveillance action. Criticisms have also been raised since a few hours after signing the act into law, the Obama administration reportedly asked the FISA court to restore the mass data collection at least for a transitional period of six months, even clarifying that the *ACLU v. Clapper* decision, being a second circuit ruling, does not constitute controlling precedent for the FISA court.[56] The Act also re-authorises Section 215 of the US PATRIOT Act and Section 702 of the FISA Amendments Act (see above) through to the end of 2017. Against this background, the new Freedom Act seems unlikely to achieve all the steps forward that EU authorities were expecting, and its actual impact on mass surveillance activities seems obscure at best at the time of writing.

Finally, another development in the United States is the introduction in the House of a proposed Judicial Redress Act of 2015 by Representatives from both of the leading parties. The

[55] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 or the USA FREEDOM Act of 2015.

[56] See, inter alia, S. Ackerman, "Obama lawyers asked secret court to ignore public court's decision on spying", *The Guardian*, 9 June (www.theguardian.com/world/2015/jun/09/obama-fisa-court-surveillance-phone-records).

Act aims at extending to citizens of designated countries (including EU member states) the right to challenge possible misuse of their data by the US government in US courts. The proposed Act would allow the Attorney General to extend US judicial redress protections to citizens of selected third countries. If eventually passed by Congress, the Act would address some of the key concerns expressed over the past few years by EU institutions with respect to US privacy laws. For example, former EU Vice-President and Commissioner for Justice Viviane Reding observed: "When Americans come to Europe and they think the authorities have not handled their case correctly, they can go to a European court. However an EU citizen cannot do the same in the US and go to an American court. There is no reciprocity; we do not have the basis for judicial redress … The US has recognised the importance of this request on several occasions – but they need to have a law. I have not yet seen it."[57] Also the new European Commission President Juncker wrote in his mission letter to Věra Jourová, the new Commissioner for Justice, Consumers and Gender Equality, that one of her tasks will be to "conclude negotiations on a comprehensive EU-US data protection agreement which provides justiciable rights for all EU citizens, regardless of where they reside, as well as reviewing the Safe Harbour arrangement".

Will these initiatives be enough to avoid the suspension of the Safe Harbour? As things stand, it is still unclear whether or not the US will implement the entirety of the EU's recommendations, such as empowering the FTC to conduct *ex-officio* investigations to assure that US companies are in compliance with their privacy policies and that any false claims would eventually be further investigated. At the end of 2014, when taking office, Ms Jourová already expressed strong doubts that Safe Harbour can be considered as really secure for EU citizens and called for a 'plan B'. Vice President Andrus Ansip was even more aggressive and specified that if there are no satisfying results from negotiations with the US, "the suspension of the agreement might then be the option".[58] Some commentators have reported that the negotiation pendulum is shifting between calls for interoperability of EU and US legislation; proposals to suspend the Safe Harbour and take it out of the TTIP, also due to the European Commission's uncertain mandate;[59] and more aggressive calls for 'data localisation' requirements, with localisation even being presented as a fundamental right. This is even more worrying since on the US side, drafts from the e-commerce section of TTIP include completely opposite stances: the principle of 'interoperability' of European and US data protection rules, and a ban on 'localisation.' In October 2014, the US negotiators placed a concrete text proposal on 'data flows' on the table. But the papers published in January 2015 by the European

[57] See Vivian Reding's speech at http://europa.eu/rapid/press-release_SPEECH-14-431_en.htm.

[58] See the initial hearing of Andrus Ansip in the European Parliament (www.europarl.europa.eu/hearings-2014/resources/library/media/20141022RES75838/20141022RES75838.pdf).

[59] The negotiation mandate for the European Commission instead refers to Article XIV of the General Agreement on Trade in Services (GATS) of the World Trade Organization. Article XIV contains a general exception clause stipulating that "nothing in the agreement may be construed to prevent the adoption or enforcement by any member of measures [...] necessary to secure compliance with laws or regulations [...] relating to [...] the protection of the privacy of individuals in relation to the processing and dissemination of personal data." The Commission's negotiation mandate states in Article 18: "The Agreement will not preclude the enforcement of exceptions on the supply of services justifiable under the relevant WTO rules (Articles XIV and XIVbis GATS)."Article XIV of GATS was indeed copied verbatim into a draft text of the TTIP agreement proposed by the Commission negotiators in July 2013 and leaked in February 2014.

Commission clearly state: "Data protection standards won't be part of TTIP negotiations. TTIP will make sure that the EU's data protection laws prevail over any commitments."[60]

6.3 What landing zones for data protection in the TTIP?

In an age of convergence, globalisation, and the data-driven economy, the US and the EU do not seem to be converging fast enough in their approaches to data protection. First, existing legislation confirms the existence of key differences in the main approaches followed by the two legal systems, with a clear focus on government intrusion into the private sphere in the US and significant emphasis on the relationship between data controllers and data subjects in the EU. Second, and relatedly, while in the United States privacy law focuses on redressing consumer harm and balancing privacy with efficient commercial transactions, in the EU privacy is considered as a fundamental right that prevails over competing interests (Hartzog and Solove 2014). Third, privacy protection is essentially triggered by the existence of 'personal data' or 'personally identifiable information' (PII): however, the definition of PII on the two sides of the Atlantic diverges significantly, with the US featuring a patchwork or partly inconsistent definitions and the EU relying on a single definition that broadly defines PII to encompass all information that is identifiable to a person.[61] Fourth, coverage of both personal *identified* and *identifiable* information seems to be more consistent in Europe than in the US: however, the EU seems too expansionist in its coverage of PII, whereas the US might err at the opposite extreme.

In addition, frictions between the US and EU authorities have mounted in the months following the Datagate scandal, such that even established cooperation and recognition frameworks such as the Safe Harbour regime are now being reconsidered. Calls for a European cloud or even clouds limited to national territory (e.g. in Germany) have become common in the debate over cloud privacy and security. The European Parliament has expressed its intention to reconsider the Safe Harbour as well as the Data Protection Umbrella Agreement that has been under discussion between the two parties since 2011. Reforms underway in the United States, including the US Freedom Act, do not seem to fully address the concerns expressed by the EU authorities, and the negotiations on the Safe Harbour seems still likely to face problems: on the one hand, EU authorities deem US privacy laws inadequate in terms of the level of protection they achieve for European citizens and increasingly consider data localisation as a fundamental right; on the other hand, US authorities seek to obtain a recognition of interoperability and a ban on data localisation in the TTIP negotiations. In short, the parties are almost as far from an agreement as they were a year ago, and despite some signs of good will the tensions are unlikely to be put to rest any time soon: on the contrary, the situation is even worsening as some EU member states are now taking action to create massive surveillance programmes, as in the case of France, which (after the terrorist attacks of January 2015) is considering the instruction of a *Loi de renseignement* (Intelligence Bill) that would go further than the US PATRIOT Act and the already annulled EU Data Retention Directive in

[60] http://trade.ec.europa.eu/doclib/docs/2015/january/tradoc_152999.2%20Services.pdf

[61] Hartzog & Solove (2014, p. 888) explain that there are three predominant approaches to defining personal information in the US: 1) the tautological approach, 2) the non-public approach and 3) the specific-types approach.

providing authorities with new technologies of mass surveillance of electronic communications.[62]

Needless to say, the persistence of divergent approaches can become an obstacle (or, at a minimum, a source of unnecessary compliance burdens) for companies wishing to provide Internet-based services on both sides of the Atlantic. This is especially the case for world-leading US-based Internet companies, which would profit enormously from a streamlining, update, and harmonisation of the definition of PII and, more generally, of the rules that apply to online data protection. To be sure, the Internet is challenging both legal regimes in a way that might end up requiring a thorough reform process. As of now, what seems likely is that the US will keep under-protecting privacy in the name of efficient commercial transactions (with a great responsibility being placed on the FTC to monitor abuses of bargaining power and other deceptive/abusive practices), whereas in the EU, Internet services might end up caught in the net of an overly formalistic, overly comprehensive legal framework, which leaves little room for trade-offs between privacy and welfare-enhancing customised service for data subjects.

Conclusions: What should the Digital TTIP achieve and what will it achieve?

Notwithstanding the strong political commitment shown by both the US and EU negotiators to speed up the conclusion of the TTIP agreement, the overall environment does not seem favourable to a comprehensive agreement in the digital sphere. Suffice it to recall that in a recent interview, President Barack Obama accused European corporations and regulators to be strategically hampering the position of US Internet companies.[63] The underlying reason, according to the American President, is that European companies "can't compete with us" and thus need to alter the level playing field to be able to survive. The reference is not only to the ongoing antitrust investigation into Google, but also to recent calls by the European Parliament to unbundle search engines (read: Google) from other commercial services, the current uprising of taxi drivers against Uber in many cities, the mounting debate on tax avoidance practices by several IT companies, the wave of 'Google taxes' imposed to remunerate publishers and the repeated calls to suspend the US-EU Safe Harbour agreement on data protection due to the alleged unreliability of US companies' privacy policies. Obama's statements triggered a blunt reaction: a European Commission's spokesperson called these comments "out of line".[64]

---

[62] These new technologies include so-called 'black boxes' or source code injected by French intelligence services on ISPs' infrastructure to detect suspicious user behaviour in real time. This would bring all (residents in France) under surveillance and expand monitoring to include private pictures, company trade secrets, medical records, etc. The authorities are expected shortly to propose a new register for suspected persons and new measures to record phone calls without authorisation from a judge, thus undermining data privacy protections.

[63] See "Obama attacks Europe over technology protectionism", by Murad Ahmed, Duncan Robinson and Richard Waters, *Financial Times*, 16 February 2015 (www.ft.com/cms/s/0/41d968d6-b5d2-11e4-b58d-00144feab7de.html#axzz3ejxpiSNf).

[64] Ibid.

Is Obama right or wrong? To be sure, much of the EU regulation that applies to the Internet is stricter than US regulation, but these rules apply regardless of nationality. In the EU, network operators have to share their networks even when they invest in high-speed broadband, while in the US such obligation was lifted a decade ago. In the EU, privacy is a fundamental right, whereas in the US it is treated as a tradable right. In the EU, antitrust follows a different approach than the US, and this usually results in stricter remedies imposed on companies with market power. Other fields, such as cybersecurity and consumer protection are more regulated in the EU than they are in the US. These rules have been applied more often to US companies since these companies have come to dominate the Internet ecosystem since the early days. In some cases, an aggravating factor was that EU rules were largely unfit for the Internet age, and this created significant problems when it came to their application to the Internet. That said, there is reason to believe that it is mostly the inadequate and obsolete features of EU law, rather than a design to hamper US companies, that inspired the Commission in these actions. Otherwise, important merger cases such as Google/DoubleClick, Google/ITA, Facebook/WhatsApp, Microsoft/Nokia, Microsoft/Skype and others would have been handled differently by the Brussels trustbusters.

The past months, however, have marked a change of direction. Many recent documents of the European Commission and European Parliament speak clearly of the need to revive industrial policy in a way that protects EU champions against the current domination of US Internet companies. The Commissioner for the digital agenda Günther Oettinger claims that EU telecom companies should become more profitable. Conferences are being organised in the Parliament with titles such as "How can we stop Internet giants?". Google and Facebook are constantly demonised in the public debate, not to mention Uber (but this would probably occur even if Uber were European) and Amazon (recently accused of unfair tax deals in, and with, Luxembourg). The Digital Single Market debate is mostly centred around industry consolidation and the creation of large mobile operators that would negotiate on a more equal footing with the Googles and the Apples. In Germany and France, pressure from content providers and publishers even led institutions to think that splitting Google could be reasonable. The European Parliament followed this trend by advocating such a structural remedy in the belief that "indexation, evaluation, presentation and ranking by search engines must be unbiased and transparent" (although an in-depth discussion of effects on users has never occurred to date). And most importantly, the European Commission is reportedly considering the extension of regulation from telecoms infrastructure to Internet platforms, in the name of so-called 'platform neutrality'. Such move would impose interoperability obligations on all leading platforms, in the attempt to create a neutral Internet. And again, it would likely damage consumers.

Getting out of this impasse and inverting the current trend of divergence requires an effort on both sides, and TTIP talks could become a viable setting to this end. The EU should understand that economic recovery would be hampered, not helped, by a revival of protectionism, and that the word "neutrality" is not a panacea for all the evils of the Internet, but rather a double-edged sword to be handled with care. Not surprisingly, but also not fully convincingly, the European Commission has taken great pains to reassure the United States that the DSM is not a protectionist strategy. The US should do its homework on data protection, settle the network neutrality debate with a convincing compromise, and avoid that the urge to claim US leadership in global Internet talks ends up bringing the Internet under an unprecedented, ill-advised wave of regulatory interventionism. Should the TTIP take the form of a 'living agreement,' as seems likely, then obvious starting points would be the easy-to-reach

agreements on e-labelling and e-accessibility, plus (if possible) an agreement to cooperate on standards related to cloud computing and the Internet of Things. In the coming years, however, it would be of utmost importance that such agreement encompasses network neutrality rules, data protection rules, intermediary liability, online copyright protection and related exceptions and limitations, and gradual convergence of competition law and policy in a field that is increasingly thirsty for legal certainty and streamlined, converging regulatory requirements on both sides of the Atlantic.

References

Akman, Pinar, (2009), "Searching for the Long-Lost Soul of Article 82", *Oxford Journal of Legal Studies*, Vol. 29, No. 2, pp. 267-303.

Bigo, Didier, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi, and Amandine Scherrer (2013). National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law. Brussels: European Parliament.

Bourreau, Marc, Pinar Doğan and Mathieu Manant (2010), "A Critical Review of the 'Ladder of Investment' Approach", *Telecommunications Policy*, Vol. 34, No. 11, 683–696.

Cline, Jay (2014), U.S. Takes the Gold in Doling out Privacy Fines. Computerworld 17 (February 17). http://www.computerworld.com/s/article/9246393/Jay_Cline_U.S._takes_the_gold_in_doling_out_privacy_fines?taxonomyId=84&pageNumber=3.

Conseil National du Numérique (2014), "Platform Neutrality: Building an open and sustainable digital environment", Opinion No. 2014-2, of the French Digital Council, Paris (www.cnnumerique.fr/wp-content/uploads/2014/06/PlatformNeutrality_VA.pdf).

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17 July 2000.

European Commission, Factsheets and EU textual proposals on parts 2 and 3 of the TTIP (http://trade.ec.europa.eu/doclib/press/index.cfm?id=1230).

European Commission (2012), European Commission. 2012b. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions—Unleashing the Potential of Cloud Computing in Europe, COM(2012) 529 final (September 27, 2012).

European Commission (2015), Communication on "A Digital Single Market Strategy for Europe", COM(2015) 192 final, Brussels, 6.5.2015.

Federal Communications Commission (FCC) (2002a), "Appropriate Framework for Broadband Access to the Internet over Wireline Facilities", Notice of Proposed Rulemaking, *Federal Communications Commission Record*, Vol. 17, No. 4, pp. 3019–3076.

_____ (2002b) "Inquiry Concerning High-Speed Access to the Internet over Cable and Other Facilities", Declaratory Ruling and Notice of Proposed Rulemaking, *Federal Communications Commission Record*, Vol. 17, No. 7, pp. 4798–4872.

_____ (2005a), "Madison River Communications, LLC", Order, *Federal Communications Commission Record*, Vol. 20, No. 6, pp. 4295–4300.

_____ (2005b), "Appropriate Framework for Broadband Access to the Internet over Wireline Facilities", Report and Order and Notice of Proposed Rulemaking, *Federal Communications Commission Record*, Vol. 20, No. 17, pp. 14853–14985.

_____ (2005c), "Appropriate Framework for Broadband Access to the Internet over Wireline Facilities", Policy Statement, *Federal Communications Commission Record*, Vol. 20, No. 17, pp. 14986–14988.

_____ (2006), "United Power Line Council's Petition for Declaratory Ruling Regarding the Classification of Broadband over Power Line Internet Access Service as an Information Service", Memorandum Opinion and Order, *Federal Communications Commission Record*, Vol. 21, No. 17, pp. 13281–13298.

_____ (2007), "Appropriate Regulatory Treatment for Broadband Access to the Internet over Wireless Networks", Declaratory Ruling, *Federal Communications Commission Record* Vol. 22, No. 8, pp. 5901–5934.

_____ (2010), "Preserving the Open Internet", Report and Order, *Federal Communications Commission Record*, Vol. 25, No. 21, pp. 17905–18098.

_____ (2014a), "Protecting and Promoting the Open Internet", Notice of Proposed Rulemaking, *Federal Communications Commission Record*, Vol. 29, No. 7, pp. 5561–5659.

_____ (2014b), "Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993", Seventeenth Report, *Federal Communications Commission Record*, Vol. 29, No. 19, pp. 15311–15478.

_____ (2015), "Protecting and Promoting the Open Internet", Report and Order on Remand, Declaratory Ruling, and Order (https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf).

Gerber, David (1994), "Constitutionalizing the Economy: German Neo-liberalism, Competition Law and the 'New' Europe", *American Journal of Comparative Law*, Vol. 42, pp. 25-84.

Hartzog, Woodrow and Daniel J. Solove (2014), "The FTC as data security regulator: *FTC v. Wyndham* and its implications", *BNA Privacy and Security Law Report* 13 (xx).

Hon, W. Kuan, Julia Hörnle, and Christopher Millard (2011a). The Problem of "Personal Data" in Cloud Computing: What Information Is Regulated?—The Cloud of Unknowing. International Data Privacy Law 1 (4): 211–228.

Hon, W. Kuan, Julia Hörnle, and Christopher Millard (2011b). Who Is Responsible for "Personal Data" in Cloud Computing? International Data Privacy Law 2 (1): 3–18.

Hon, W. Kuan, Julia Hörnle, and Christopher Millard (2012). Data Protection Jurisdic- tion and Cloud Computing—When Are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing. International Review of Law Comput- ers & Technology 26 (2–3): 129–164.

Pelkmans, Jacques, and Andrea Renda (2011), "Single eComms market? No such thing", *Communications & Strategies*, 2nd quarter.

Petit, Nicolas (2014), "Price Squeezes with Positive Margins in EU Competition Law: Economic and Legal Anatomy of a Zombie" (http://ssrn.com/abstract=2506521 or http://dx.doi.org/10.2139/ssrn.2506521).

Post, Robert C. (2001), "Three concepts of privacy," *Georgetown Law Journal,* Vol. 89 (6) 2087-2098.

Powell, Michael K. (2004), "Preserving Internet Freedom: Guiding Principles for the Industry", *Journal on Telecommunications and High Technology Law*, Vol. 3, No. 1, pp. 5–21.

Renda, Andrea (2005), "Telecom Services: a Transatlantic Perspective", in D.S. Hamilton and J.P. Quinlan (eds), *Deep Integration. How Transatlantic Markets are Leading Globalization*, CEPS Paperbacks, Chapter 11.

_____ (2007), "The Costs and Benefits of Transatlantic Convergence in Telecom Services, in Dan Hamilton and Joseph Quinlan (eds), *Sleeping Giant: Awakening the Transatlantic Services Economy*, Johns Hopkins University and Brookings Institution, Washington, D.C., November.

_____ (2009), "The review of the telecoms framework: a tale of the anti-commons, paper for the first report of the "Monitoring ICT European Regulation" initiative, NEREC, Madrid.

_____ (2010), *Competition-regulation Interface in Telecommunications. What's left of the Essential Facilities Doctrine*, Telecommunications Policy, Vol. 34, Issues 1-2, February-March, pp. 23-35.

_____ (2013), *Net Neutrality and Mandatory Network-Sharing: How to disconnect the continent*, CEPS Policy Briefs, 18 December, CEPS, Brussels (www.ceps.eu/system/files/PB309%20AR%20Net%20Neutrality_0.pdf).

_____ (2015a), *Antitrust, regulation and the "neutrality trap"*, CEPS Special Report No. 104, CEPS, Brussels, April.

_____ (forthcoming 2015b), "Cloud Privacy law in the United States and the European Union", in Christopher S. Yoo and Jean-Francois Blanchette (eds), *Regulating the Cloud: Policy for Computing Infrastructure*, Cambridge, MA: MIT Press, August.

Renda, Andrea et al. (2006), "Making Antitrust Damages Actions More Effective in Europe", Study for the European Commission, DG COMP, available online at http://ec.europa.eu/competition/antitrust/actionsdamages/files_white_paper/impact_study.pdf.

Renda, Andrea et al. (2015), Study on the implementation, application and effects of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society (InfoSoc) Directive and of its related instruments, Study for the European Parliament Research Service, forthcoming July 2015, to be published on the European Parliament's website.

Solove, Daniel J. (2006), A Taxonomy of Privacy. University of Pennsylvania Law Review 154 (3): 477–560.

Schwartz, (2013), EU Privacy and the Cloud: Consent and Jurisdiction under the Proposed Regulation. BNA Privacy and Security Law Report 12 (April 29): 1–3.

Schwartz and Daniel J. Solove (2013), Reconciling Personal Information in the United States and European Union. UC Berkeley Public Law Research Paper No. 2271442.

Whitman, James Q. (2004), "The Two Western Cultures of Privacy: Dignity versus Liberty" Faculty Scholarship Series. Paper 649, Yale Law School, Yale University, New Haven, CT (http://digitalcommons.law.yale.edu/fss_papers/649).

WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty, adopted in Geneva in December 20, 1996 (http://www.wipo.int/treaties).

Yoo, Christopher S. (2006), "Network Neutrality and the Economics of Congestion", *Georgetown Law Journal*, Vol. 94, No. 6, pp. 1847–1908.

_____ (2014), "US vs. European Broadband Deployment: What Do the Data Say?", Institute for Law and Economics Research Paper No. 14-35, University of Pennsylvania, Philadelphia, PA.

US Case Law

American Civil Liberties Union v. James Clapper, No. 13-3994 (S.D. New York December 28, 2013)

Brand X Internet Services et al., 545 U.S. 967 (2005).

Cascade Health Solutions v. PeaceHealth, 515 F.3d 883 (9th Cir. 2008).

Innovation Data Processing v. IBM, 585 F. Supp. 1470 (D.N.J. 1984).

LePage's Inc. v. 3M, 324 F.3d 141 (3d Cir. 2003) (en banc).

National Cable & Telecommunications Association v. Brand X Internet Services, 545 US 967 (2005).

Pacific Bell Telephone Co. v. Linkline Communications, Inc., 555 US 438 (2009).

Telex Corp. v. IBM, 367 F. Supp. 258 (N.D. Okla. 1973), *aff'd in relevant part & rev'd on other grounds*, 510 F.2d 894 (10th Cir. 1975).

Verizon Communications, Inc. v. Law Offices of Curtis V. Trinko, L.L.P., 540 US 398 (2004).

Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014).