European Parliament

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES

POLICY DEPARTMENT

Transatlantic Digital Economy and Data Protection: State-of-Play and Future Implications for the EU's External Policies

AFET

EN

2016

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES
POLICY DEPARTMENT

European Parliament

STUDY

Transatlantic Digital Economy and Data Protection: State-of-Play and Future Implications for the EU's External Policies

ABSTRACT

The internet has created a new global nervous system affecting all aspects of European society, politics and business; this will accelerate as we enter the era of the digitisation of everything. This digital transformation has enormous implications for the transatlantic relationship, especially in light of the differences that have developed concerning the appropriate balance between personal data protection, economic growth and national security. This study details how digital and data issues will be handled in the Transatlantic Trade and Investment Partnership; explains how this intersects with the new EU-US Privacy Shield Agreement and the broader implications of the judgment on Safe Harbour; and explores key issues in transatlantic law enforcement cooperation before highlighting a few broader foreign policy issues and laying forth some recommendations for the EU institutions.

EP/EXPO/B/AFET/FWC/2013-08/Lot3/01
July 2016 - PE 535.006

EN

This paper was requested by the European Parliament's Committee on Foreign Affairs.

English-language manuscript was completed on 01 July 2016.

Printed in Belgium.

Authors: Peter CHASE, Non-Resident Transatlantic Fellow, The German Marshall Fund of the United States, Belgium; Sudha DAVID-WILP, Deputy Director Berlin Office, Senior Transatlantic Fellow, The German Marshall Fund of the United States, Germany; Tim RIDOUT, Fellow, Wider Atlantic Program, The German Marshall Fund of the United States, U.S

Officials Responsible: Aydan BAHADIR, Elina VIILUP

Editorial Assistant: Liina BAHBOUT

Feedback of all kind is welcome. Please write to: aydan.bahadir@europarl.europa.eu

To obtain copies, please send a request to: poldep-expo@europarl.europa.eu

This paper will be published on the European Parliament's online database, 'Think tank'.

ISBN: 978-92-823-8660-6 (pdf)

doi:10.2861/173823 (pdf)

Catalogue number: QA-01-16-195-EN-N (pdf)

ISBN: 978-92-823-9848-7 (paper)

doi:10.2861/771804 (paper)

Catalogue number: QA-01-16-195-EN-C (paper)

Table of contents

Executive Summary

The internet and the *digitalization of everything* are powering a digital transformation, if not revolution, of the European and indeed global economy and society. Over 80 % of all Europeans have broad-band access and 90 % of European businesses are on the internet, up from 20 % in both cases little more than five years ago. This exponential growth is reflected as well in the United States and elsewhere, with some 4 billion people expected to be on the internet by 2020. New communications technologies, cheap but accurate sensors and enormous computing capabilities are now swiftly bringing *things* as well as people on-line, with some 26 billion things -- ranging from 'smart' clothing to medical devices to huge mining vehicles -- expected to contribute to an explosion of internet traffic over the next five years. This digitalization offers opportunities for radical new approaches to healthcare, transport, agriculture, energy and other sectors, which explains why so many new firms are 'born global.' Rather than referring to the 'digital economy,' we must now recognize that the economy is digital.

This transformation radically affects the concept of trade. Once measured almost exclusively in terms of the flow of goods, services -- which account for three-quarters of the European economy -- can increasingly be 'digitally delivered' across distances, and thus across borders. Nowhere is this more evident than in the highly integrated transatlantic economy, where digitally-delivered services trade reached some USD 250 billion in 2012. The on-going EU-US negotiations toward a Transatlantic Trade and Investment Partnership (TTIP) could have a significant impact on transatlantic digital trade, not just in such directly pertinent areas as e-commerce and data flows, but also with respect to trade in goods (where 'embedded services' are increasingly important), customs facilitation, services, investment and regulatory cooperation.

How the digital world is regulated -- especially with respect to the protection of personal data -- is thus hugely significant to transatlantic commercial relations. While TTIP itself is unlikely to directly address personal data other than by recognizing that both parties have the right to protect it, the regulatory framework that governs transfers of personal data across the Atlantic must be workable. The European Court of Justice ruling in October 2015 that the European Commission had not adequately considered the overall democratic framework for the protection of personal data in the United States when deciding, in 2000, that US firms that signed on to the Safe Harbour principles provided adequate protections, thus generated enormous efforts by the Commission and the US government to negotiate a new arrangement. The 'Privacy Shield' agreement announced in February 2016 and approved with slight modifications in July 2016 reflects both changes in US domestic law and practice (such as President Obama's 2014 Executive Order on intelligence agency activities and the passage of the Freedom and Judicial Redress Acts) and undertakings by the US Administration. Even if this transatlantic problem is resolved, however, the logic of the Court's ruling, when applied to other countries such as Russia and China, could affect the ability to transfer personal data to -- and thus the EU's commercial relations with -- those countries.

Just as the EU's commercial relations with the United States and the rest of the world will depend on the balance between privacy and economy reflected in Europe's regulation of data flows, the ability of our societies to ensure the security of our citizens will depend on finding new ways to address international law enforcement and national security cooperation in a digitalized world. This need to find the appropriate balance between security and privacy is especially important for the European Union and the United States, where a tradition of collaboration was affected by the revelations of mass surveillance by US intelligence agencies. In the United States, the priority given to security following the 9/11 attacks is increasingly being questioned, with a number of new laws adopted that curtail law enforcement and national security agency access to personal data held by companies. This could set the stage for increased transatlantic dialogue to rebuild trust in such areas as political oversight, law enforcement data

transfers (including through an updated EU-US Mutual Legal Assistance Treaty), and cooperation on cyber-security and encryption.

Beyond these commercial and security concerns, both the European Union and the United States are realizing that the internet is changing foreign policy more generally, including with respect to democracy promotion and all aspects of development. A robust dialogue about these issues necessitates a common understanding of digital and cyber issues writ large, as well as a concerted effort to work together in the international regulation of these field.

Given the leading role of the European Union and the United States in general, and specifically in the size of their digital relationship, all European Union institutions should think creatively about ways to enhance the transatlantic relationship in this domain, including through creation of a multifaceted Transatlantic Digital Dialogue, with an eye to building a Transatlantic Digital Marketplace; active consideration and oversight of laws that affected transatlantic digital flows; and deepened discussion on the critical law enforcement, cyber-security and national security issues that the two sides face in this digitalized world.

General Recommendations

- Recommendation 1: Restore clarity in the debate about digital transformation
- Recommendation 2: Affirm EU principles on promoting and protecting citizens' rights online
- Recommendation 3: Build certainty in the framework to transfer data across borders
- Recommendation 4: Strengthen the Transatlantic Digital Dialogue in all EU institutions, and establish an explicit goal of creating a Transatlantic Digital Marketplace
- Recommendation 5: Explicitly include the digital economy as part of trade and investment negotiations

Recommendations for the European Parliament

- Recommendation 6: Use the Transatlantic Legislators' Dialogue to enhance collaboration on rules for the digital age
- Recommendation 7: Assess the quality of 'democratic controls' over government access to personal data in the EU, the US and elsewhere
- Recommendation 8: Monitor the implementation of new digital legislation and its impact on transatlantic relations

Recommendations for the European Commission

- Recommendation 9: Upgrade the EU-US Information Society Dialogue and ensure coherence between policies adopted within the Commission and the US Administration
- Recommendation 10: Use this Dialogue and other established transatlantic channels to address and ensure coherence in the key digital law enforcement issues – general oversight, mutual legal assistance, and encryption and cybersecurity.
- Recommendation 11: Develop a cross-sectoral approach and a common vision for the digitalisation of the industry in Europe

Recommendations for the Council and for member states

- Recommendation 12: Swiftly transpose EU legislation on the digital economy and data privacy
- Recommendation 13: Pro-actively work with the Commission on transatlantic digital law enforcement issues
- Recommendation 14: Better engage EU citizens on transatlantic trust in digital issues

Recommendations for the European External Action Service

- Recommendation 15: Strengthen the EU- US Cyber Dialogue
- Recommendation 16: Include internet freedom and access to digital content and technologies as part of external policies toward developing and emerging countries.

Introduction

Digital technologies are transforming societies and economies across the globe. By connecting people, places and increasingly things with an unimagined rapidity, the internet is creating a new global nervous system that is at the core of all international exchanges. Much as the movement of goods and people drove economic and political relations over the course of the last century, the framework under which data moves globally will shape these same relations for years to come.

The European Union and the United States are at the heart of these developments. With the deep digital integration of the transatlantic space, the EU and the US are in a unique position to draw up the architecture and the rules for the new digital world. Yet both sides of the Atlantic are still struggling to grasp the changes digitalization is bringing. Frictions and tensions between proponents of privacy, security and the economy linger and create obstacles to the transatlantic partners' ability to tackle the challenges ahead. In order for the US and the EU to reap the full benefits of digital transformation, politicians, policymakers, businesses and other stakeholders need to work together on defining appropriate rules for the internet, guaranteeing the efficient flow of data across borders and stimulating growth and innovation while at the same time protecting fundamental rights.

In the EU and the US, defining the balance for protecting personal liberties in the digital age is the single most critical issue in public policy governing the internet. By connecting individuals to the rest of the world in an unprecedented way, the internet has disrupted traditional boundaries between the individual and the group in the economy and society, especially in terms of law enforcement and national security. Yet while these issues of the internet and the economy, law enforcement and national security are different and must be treated individually, the politicians and policy makers who will define this balance also need to keep the inter-relationship between them in mind. As is true in the physical realm, what the EU and the US do that affects digital trade will have a direct impact on how law enforcement authorities use data in their investigations, and the safeguards that are put in place to protect users, consumers and citizens alike.

Keeping the above in mind, this study seeks to examine how issues related to the transatlantic economy and data privacy may have an impact on the EU's foreign policy. Its purpose is to address the linkages between privacy, security, and the economy, not to draw a comprehensive list of data, digital or cyber legislation being discussed either in the EU or in the US. With internet users expected to reach 4 billion people worldwide by 2020[1], how to harness digital transformation for peace, prosperity and stability goes beyond maximizing the economic and societal benefits of digital technologies. In the transatlantic space in particular, conceptual differences on how to address these issues have led to more friction than convergence. As witnessed in recent years, these frictions – often technical – can quickly spill into the political sphere and directly influence the EU's foreign relations. Indeed, they can affect both the EU's role as a global economic power (commercial relations) and the security of its citizens and infrastructure (cybersecurity).

In Chapter 1, this report provides some background on the current state of digital transformation in the EU, the US and the world, providing context for the remainder of the study and drawing out some of the broader political, social and economic implications of this change.

[1] ITU, UNESCO, 'The State of Broadband 2015: Broadband as a Foundation for Sustainable Development,' Switzerland, Geneva, September 2015, p. 20, http://www.broadbandcommission.org/Documents/reports/bb-annualreport2015.pdf

Chapter 2 of the study focuses on the way in which the digitalisation of the EU and US economies is affecting transatlantic trade, and how the Transatlantic Trade and Investment Partnership (TTIP) might address digital issues to promote this.

The nexus between privacy and transatlantic trade is directly addressed in Chapter 3. With the need to restore trust between European and US citizens when it comes to the overall control of their online data, there are opportunities to create a new transatlantic equilibrium on digital issues.

The issue of privacy and security -- specifically with respect to law enforcement, counter-terrorism and cybersecurity -- is the subject of Chapter 4, while Chapter 5 introduces some of the broader foreign policy issues on which the EU and the US should consider collaborating.

Finally, Chapter 6 provides a set of specific recommendations to the European Parliament, the European Commission, the Council and member states and to the European External Action Service on how to move forward on the transatlantic digital economy and data privacy.

1 The European and Global Digital Transformation – Context and Implications

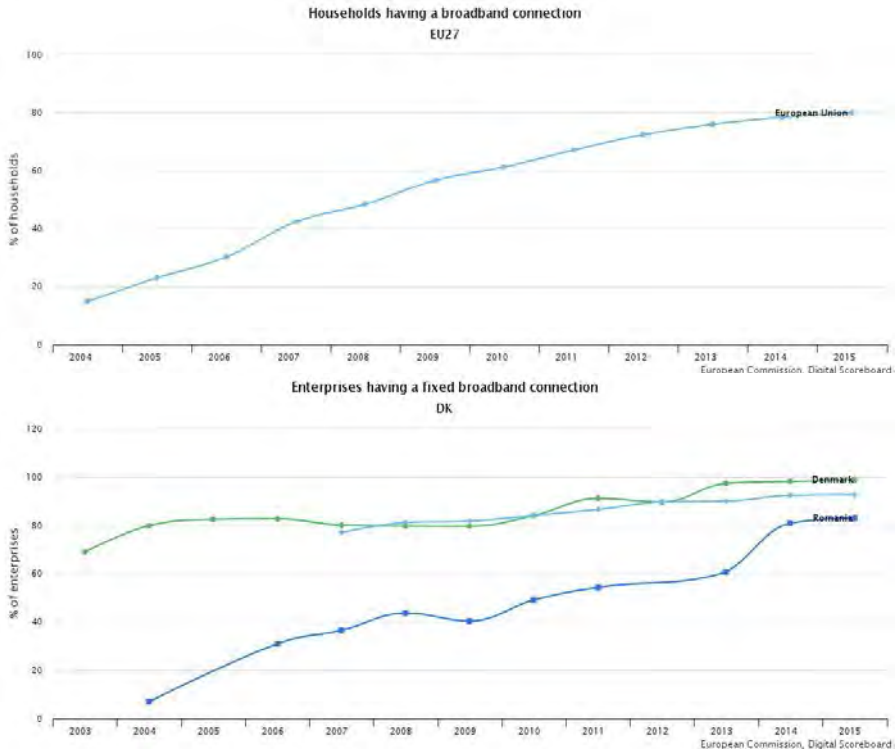
The world is going through a profound transformation as more people gain access to the internet. Understanding this digital transformation is critical to appreciating its impact on Europe's global context and foreign policy, and in particular its relations with the United States.

Europe:

The internet now pervades the lives of the vast majority of European citizens:

- Over 80 % of EU households have broadband connection, up from less than 20 % in 2004;
- Nearly 80 % of EU citizens have smart phones connected to the internet, up from less than 20 % in 2008; and
- Over 90 % of European businesses are online, with the least connected member state, Romania, quickly catching up to the most advanced, Denmark.

Figure 1 & 2: EU 27 Households having a broadband connection 2004 - 2015; Enterprises having a fixed broadband connection, Denmark - Romania comparison



Source: European Commission, Digital Scoreboard.

Not surprisingly, with the rapid growth of access to the internet by individuals and businesses, the amount of internet traffic in Europe is growing rapidly, and will continue to explode over the next five years, rising from 9.6 petabytes (PB, = 9.600.000 gigabytes) in 2014 to 24.7 PB in 2019[2].

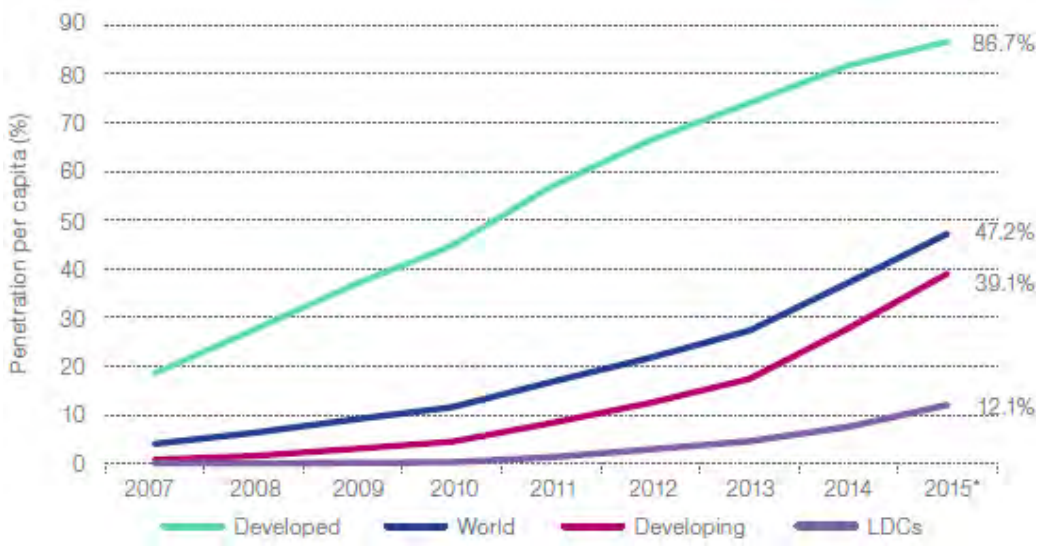
[2] Cisco, 'The Zettabyte Era - Trends and Analysis,' 23 June, 2015 Appendix A, Table 8. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html

Even those few in Europe who may not have a direct connection to the internet are affected by it –the news, business supply relations, discussions with family members away from home, and the political context in which they live are all affected by the inter-connectedness that the internet has brought to Europe.

The United States and the Rest of the World:

Europe, of course, is not alone in being brought online, for a similar story can be told of the US, virtually all developed OECD countries, and indeed a huge swath of the population in many developing economies – such as construction workers in Dakar and Kampala – helped in large part by the growth in mobile 'smart' phones that can access the internet:

Figure 3: Mobile Internet Subscription Penetration, by region and percent of population, 2007-2015



Source: ITU, UNESCO, The State of Broadband 2015.

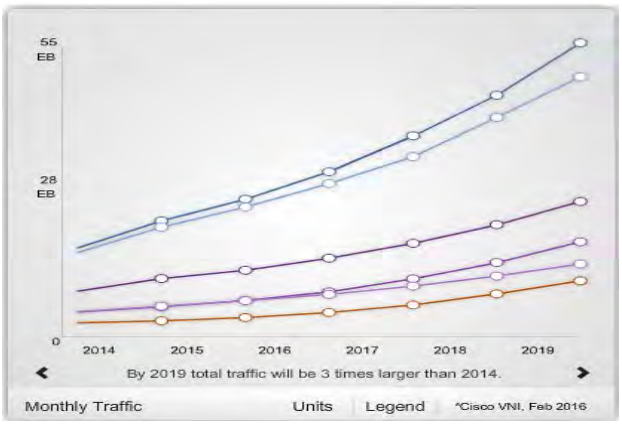
But where the internet first brought *people* together, this communications revolution is now being extended to *things*. Internet-connected electronics are being embedded in all sorts of objects and machinery – from numerical machine tools, to office buildings and bridges, to the clothing we wear. With the increased accuracy and low cost of sensors and radio frequency identification devices (RFID) that measure the location, movement, temperature and other aspects of these things, and super-abundant and super-fast computing (the computing power of 'smart' phones now exceed that used to put man on the moon), we are entering the era of the 'Internet of Things' (IoT), and the 'Big Data' these things – as well as the billions of connected people – can generate. Some 3.2 billion inanimate objects are now generating data as part of the IoT; this is projected to grow to 26 billion in just four years. Indeed, it is estimated that machine-to-machine internet traffic will grow at a 71 % compound annual growth rate between 2014 and 2019[3], powered in part by the sixth version of the internet protocol (IPv6), which increases the number of IP addresses to allow theoretically for 3.4×10^{38} inter-connected devices[4], and 'fifth generation' (5G) mobile transmission technology, which should significantly reduce spectrum use and energy requirements of mobile communications when it comes on-stream in 2020.

[3] Cisco, 'Visual Networking Index (VNI): Forecast and Methodology 2014-2019 White Paper', May 2015, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html

[4] R. Davies, Briefing: The Internet of Things: Opportunities and Challenges, European Parliament Research Service, May 2015, p. 2, http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf

Although machine-to-machine data connections do not use much bandwidth, all these factors together will lead to an explosion of internet traffic over the next five years. Cisco estimates that global internet traffic has increased more than fivefold in the past 5 years, and will increase nearly threefold over the next 5 years. Overall, internet traffic will grow at a compound annual growth rate of 23 percent from 2014 to 2019, surpassing the zettabyte (1 000 exabytes) threshold in 2016, and the two zettabyte threshold in 2019, or increasing from 6 gigabytes per capita in 2014 to 18 gigabytes in 2019. Effectively this means that global internet traffic in 2019 will be equivalent to 64 times the volume of the entire global internet in 2005[5].

Figure 4: 2014 - 2019 Bandwidth traffic by regions



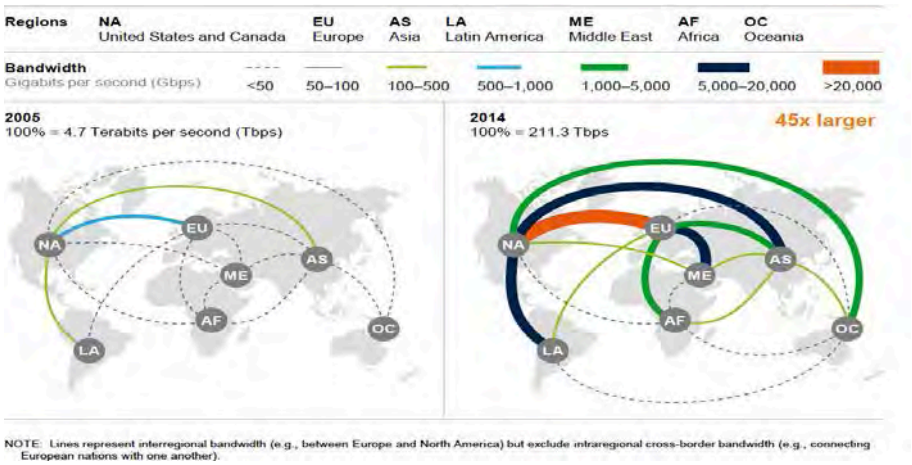
Asia Pacific
North America

Western Europe
Central and Eastern Europe
Latin America
Middle East and Africa

Source: Cisco, Visual Networking Index (VNI): Forecast and Methodology, 2014-2019.

Another analysis, by McKinsey Global Institute[6], has slightly different numbers but illustrates this growing global connectedness well:

Figure 5: Cross-border data flows by region



Source: McKinsey Global Institute, Digital Globalization: The New Era of Global Flows.

The new connectedness of people and increasingly of things is powering a digital transformation, if not a digital revolution, of our lives. Within countries, people are more connected to each other, to their

[5] Cisco, 'Visual Networking Index', op. cit.
[6] J. Manyika, et al, 'Digital Globalization: The New Era of Global Flows', McKinsey & Company, March 2016, p. 6, http://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows

communities and to their political leaders than ever before. Millions of individuals can be mobilized quickly, as Barack Obama demonstrated so well in his 2008 presidential victory, but also as the defeats of the Stop On-Line Piracy Act (SOPA) in the US Congress in 2011 and of the Anti-Counterfeit Trade Agreement (ACTA) in the European Parliament in 2012 showed. Bernie Sanders has over 4 million individuals contributing an average of USD 27 each to his campaign; over three million European citizens have signed a petition against the Transatlantic Trade and Investment Partnership (TTIP).

This is just the start. The international connectedness of people creates communities that are larger than many countries. As of the first quarter of 2016, Facebook had more active users (1.6 billion) than the population of China; it, YouTube, WhatsApp and WeChat all have more users than the 550 million people in the EU. These connections have societal consequences. National boundaries and polities begin to blur – the self-immolation of a Tunisian street vendor went viral and ignited the Arab Spring. Some governments, aware of the dangers of political 'contagion' the internet can bring, have developed huge bureaucratic structures to censor and control the internet.

As the internet increasingly brings people, things and the 'Big Data' they generate together, it creates enormous new opportunities, in healthcare (distance patient monitoring), education (distance learning), energy (smart meters), agriculture (plant-based targeted irrigation), environmental management (monitoring and forecasting air quality), smart cities (reducing traffic congestion through smart parking) and open government data[7]. And, of course, in online shopping – McKinsey estimates that by 2020 nearly a billion online customers will spend USD 1 trillion on cross-border online purchases[8].

All these services depend on generating and analysing vast quantities of data from a variety of sources, and not surprisingly business is leading the way. As a recent briefing note by the European Political Strategy Centre underscores, 'The internet and digital communications are general purpose technologies…. Against this backdrop, it is important to understand that there is no such thing as a 'digital economy' – the economy is digital. Far from being the exclusive domain of technology start-ups, every company, particularly in traditional industries, needs to prepare for digitisation[9].' And further, 'The consumer and user is ever more central to the new economy, by virtue of being more active and responsive, hence shaping the manufacturing value chain and leading the way towards tailor-made, 'personalised production on demand' and the emergence of hyper-connected services. If the industrial age was marked by standardisation, the digital era is about customisation. These tectonic shifts go hand in hand with other developments of seismic proportions: the blurring distinction between products and services; …; and the growing importance of investments in intangibles – such as software or design – which increasingly outstrip investments in tangibles – such as machines or buildings – in the leading economies[10].'

These considerations help explain the McKinsey Global Institute observation that more than 80 % of the tech-based start-ups they surveyed are 'born global,' with foreign customers, financing and suppliers from day one; that they use platforms like Facebook, Amazon, eBay, Etsy[11] and Alibaba to find customers and suppliers abroad; and that access to the digital marketplace is likely to benefit businesses on the 'periphery' of global trade relatively more[12]. But they also explain the disruptive patterns the internet

[7] P. MacDonnell, D. Castro, 'Europe Should Embrace the Data Revolution,' Center for Data Innovation, 29 February, 2016, http://www2.datainnovation.org/2016-europe-embrace-data-revolution.pdf; see also, Davies, 'The Internet of Things' op. cit.
[8] Manyika et al, 'Digital Globalization', op cit. p. 34.
[9] European Political Strategy Center, 'Strategic Note - The Integration of Products and Services - Taking the Single Market into the 21st Century,' Issue 7, 6 October, 2015, http://ec.europa.eu/epsc/pdf/publications/strategic_note_issue_7.pdf
[10] EPSC, 'The Integration of Products and Services'.
[11] Etsy is a US-based online platform for artists and crafters, which now has 1.6 million active sellers selling USD 2.4 billion to 25 million buyers in 2015; 30 % of these sales were international. See https://www.etsy.com/
[12] Manyika et al, 'Digital Globalization', op cit.

brings even to large established firms with new business models, in healthcare, transport, finance, and increasingly even major manufacturing.

The service sector, where the EU is the world's largest exporter, is perhaps the most affected by this. When the General Agreement on Trade in Services (GATS) was concluded as part of the new World Trade Organization (WTO) 20 years ago, services other than transport and logistics were largely considered 'non-tradable' – cross-border trade in services was almost an after-thought compared to the three other 'modes of delivery' – movement of consumers, movement of providers and establishment. This has changed dramatically, as the internet allows for the distant provision of professional (legal, medical, educational) and many other business services[13]. As a result, 'trade in digitally-deliverable services has more than doubled over the past decade, reaching USD 2.4 trillion in 2014. This amounts to 50 percent of total service exports.'[14] Not surprisingly, for major trading regions like the EU that are strong in services as well goods exports, being globally connected through the internet is now essential for economic growth.

Implications for the EU's External Action

- All policies, including external, need to be thought of in the context of the global explosion of connectedness and data;
- The EU institutions do a good job of communicating to the European public on the internet, but must always be aware that such communication also reaches the global public;
- Policies that promote internet communications in developing countries can have a powerful effect on empowering individuals;
- The competition for getting messages to individuals, however, is increasingly fierce, such that 'traditional' approaches and messages are increasingly challenged;
- Economic power will increasingly be determined by the ability of individuals and firms to adapt to and adopt the technologies of the internet.

2 Digital Trade and the Transatlantic Trade and Investment Partnership

2.1 Transatlantic Digital Trade

The transatlantic economies are highly integrated. Commercial exchanges in terms of goods and services trade between the European Union and the United States amount to nearly EUR 1 trillion annually. But more importantly, the EU and the US have a unique investment-based relationship, with US and European firms each having invested over EUR 1.7 *trillion* in the partner economy on the other side of the ocean[15]. These investments generate annual sales of nearly EUR 5 trillion and directly employ over eight million people in both economies, with an estimated 6 million more directly engaged in selling to them.

Both the US and the EU are deeply connected to the internet, and as a result the largest inter-continental internet data flows are across the Atlantic. These data flows are now the backbone of the transatlantic

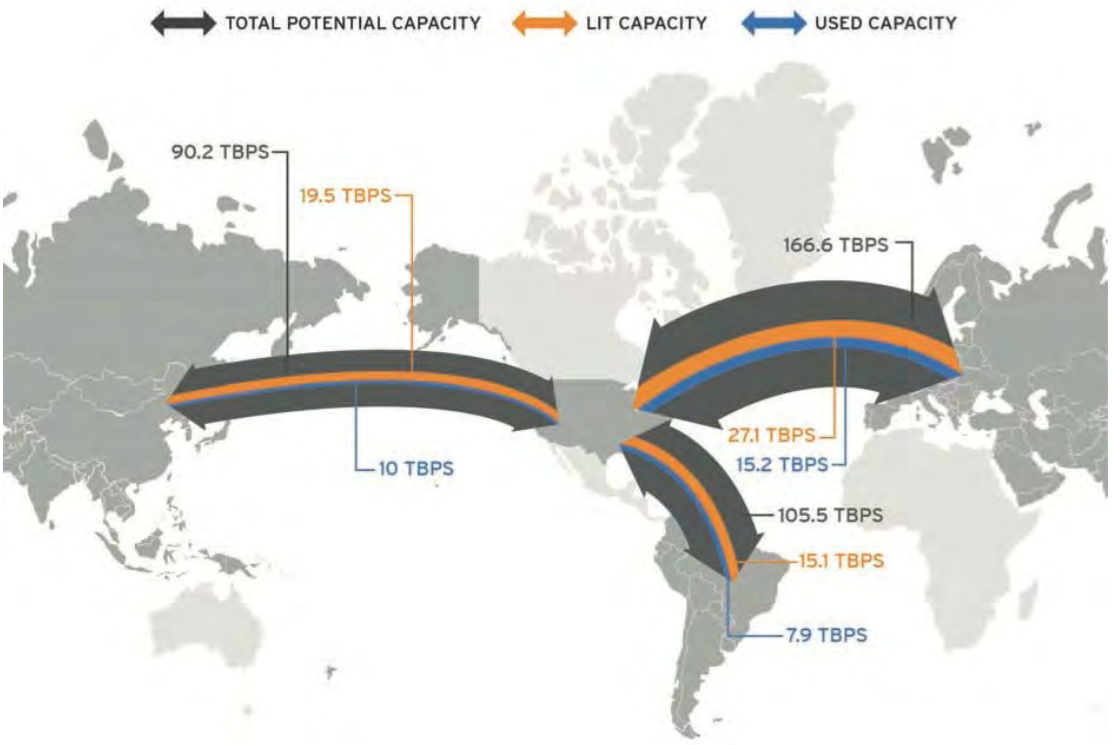
[13] Jensen Bradford of the Petersen Institute for International Economics was one of the first to develop this concept; see, e.g., B. Jensen, L. Kletzer 'Tradable Services: Understanding the Scope and Impact of Services Outsourcing,' Peterson Institute for International Economics Working Paper 5-9, September 2005, https://piie.com/publications/wp/wp05-9.pdf

[14] Manyika et al, 'Digital Globalization', op cit, page 28.

[15] European Commission, 'Countries and regions - United States,' http://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states/

economy, both for direct e-commerce purchases of goods and services and to facilitate virtually all business relations between the US and EU.

Figure 6: Submarine Cable Bandwidth (in terabits per second, or TBps)



Source: Telegeography 2014.

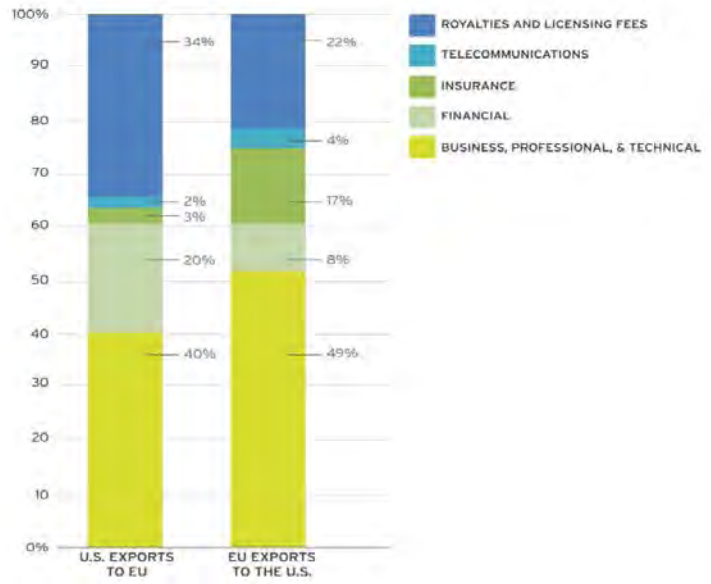
The most direct relationship between the internet and trade is e-commerce: the purchase and sale of goods and services, physical or digital, over the internet. Good statistics on the precise volume of transatlantic e-commerce trade are, however, difficult to come by. In its enormous two-part study on the internet and trade in the USA, the US International Trade Commission (USITC) estimated that 'digitally intensive' US firms (which include a wide range of traditional manufacturing) had online sales of USD 935.2 billion in 2012; of this amount, USD 222.9 billion was exported. Only 30 percent of the total sales were 'digital' products delivered online (as opposed to physical goods from the manufacturing, wholesale and retail trade sectors), while some 40 % or USD 90.6 billion of the exports were digitally-delivered. Online purchases were USD 472 billion in 2012 (USD 422 billion delivered as physical goods), while online imports accounted for USD 106.2 billion of that figure, again, with the vast majority as physical goods. The USITC survey results clearly show that Europe was a major trading partner for these internet purchases and sales, with nearly half of all companies indicating an online trading relationship with the EU[16].

Looking at global trade in goods ordered over the internet, McKinsey Global Institute estimates this reached USD2.2 trillion in 2015, or 12 percent of total goods trade, both business-to-consumer (B2C) and business-to-business (B2B)[17]. It did not separate out transatlantic e-commerce trade in goods, but a substantial portion of this global figure is undoubtedly between the EU and the US.

[16] US International Trade Commission, 'Digital Trade in the U.S. and Global Economies, Part 2,' Publication Number: 4485 Investigation Number: 332-540, August 2014, https://www.usitc.gov/publications/332/pub4485.pdf
[17] Manyika et al, 'Digital Globalization', op cit. p. 34.

While getting exact data for transatlantic e-commerce is difficult, as indicated above, the internet facilitates trade in services in particular. This is especially relevant in the transatlantic context, as services generate approximately 70 % of GDP in both the EU and the US – which is one reason services trade has been called the 'Sleeping Giant' of the transatlantic economy[18]. Joshua Meltzer of the Brookings Institution estimates that in 2012, the EU's global exports of digitally-deliverable services were USD 465 billion, of which some USD 86.3 billion were imported by the USA (60 percent of the EU's services exports to the US); for the US, global exports of digitally-deliverable services were USD 365 billion in 2012, of which some USD 140.6 billion were imported by the EU.

Figure 7: US EU Digitally Deliverable Services Trade by Sector, 2012[19]



Source: US Bureau of Economic Analysis.

It is important to stress here that the import of these digitally-deliverable services is also critical to the export performances of the European Union and the United States. Meltzer estimates that in 2012, 53 % of the digitally-deliverable services that the EU imported from the USA, or USD 22.3 billion, added value to the EU's exports of goods and services in that year[20].

2.2 TTIP and Transatlantic Digital Trade

The purpose of the Transatlantic Trade and Investment Partnership, as its name implies, is to facilitate trade and investment flows between the two partners to spur economic growth in both[21]. While the two already have an unparalleled commercial relationship, TTIP would be a contract between the European Union and the United States covering things they – as governments – can do to make it even better.

Launched in June 2013, the TTIP negotiations just completed their 14th round in three years in Brussels in mid-July. The talks languished throughout 2014 over an unnecessary miscommunication about tariff

[18] D. Hamilton, J. Quinlan, *Sleeping Giant: Awakening the Transatlantic Services Economy*, Washington, D.C.: Center for Transatlantic Relations, Paul H. Nitze School of Advanced International Studies, Johns Hopkins University, November 2007.
[19] J. Meltzer, 'The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment,' Brookings Institution, Global Economy and Development Center, Working Paper 79, October 2014, http://www.brookings.edu/~/media/research/files/papers/2014/10/internet-transatlantic-data-flows-meltzer/internet-transatlantic-data-flows-version-2.pdf
[20] Meltzer, 'Internet and Transatlantic Data Flows', p.17.
[21] European Commission, 'Statement by President Barroso on the EU-US trade agreement with U.S. President Barack Obama, the President of the European Council Herman Van Rompuy and UK Prime Minister David Cameron,' 17 June, 2013, http://europa.eu/rapid/press-release_SPEECH-13-544_en.htm

offers early in the year, immense concerns in Europe over 'investor-state dispute settlement,' the continued political fall-out from the revelations of US intelligence services 'mining' Europeans' personal data held by US internet firms, and the departure of the Barroso Commission at the end of the year. With the advent of the Juncker Commission, however, the talks regained some momentum and the two sides have pledged to try to complete the negotiations on the basic text of the trade provisions in TTIP by the end of President Obama's term in January 2017 – a pledge Mr. Obama underscored at the Hannover Fair in April 2016[22].

Achieving this will be difficult, but it is possible. If done, the agreement will still need to undergo 12-18 months of translation and legal review before the Commission can ask the Council for authority to sign (perhaps early 2018), get unanimous Council approval and then submit the text to the European Parliament for its consent (perhaps by the end of 2018). During this time, work on the regulatory cooperation issues, which will not be completed by the end of 2016, could continue. With the change in US Administration and key European elections in 2017, if this ambitious timeline cannot be met, TTIP could well be delayed significantly.

While some of the TTIP provisions (on e-commerce and electronic data flows) will deal explicitly with the digital aspect of the transatlantic relationship, the discussion above about the importance of digital technologies in all aspects of trade implies that many other parts of the agreement will influence or be affected by it, including provisions dealing with trade in goods (ICT equipment), customs facilitation, trade in services, investment, procurement, regulatory issues, and a few of the areas under the 'rules' part of the agreement.

E-Commerce and Data Flows

The EU and the USA share many values and interests in promoting the internet, and indeed in April 2011 adopted a Joint Statement on 'Trade Principles for Information and Communications Technologies Services' that underscores their common commitment to transparency, open networks and network access, free cross-border data flows, personal data protection, avoiding data localisation requirements, limiting foreign ownership restrictions, calling for independent regulatory authorities, liberal licensing and authorization processes, and promoting interconnection[23]. Reflecting these shared principles, the EU and US in general have taken very similar approaches to the issue of e-commerce in trade, as in their respective agreements with Korea.

During the year the 'High Level Working Group on Jobs and Growth' spent exploring whether to launch bilateral trade negotiations, digital issues were never flagged as contentious. Indeed, e-commerce and electronic data flows are not mentioned specifically in the High Level Working Group's final report[24], nor do these issues figure in the Council's June 2013 negotiating directives governing the Commission's objectives in TTIP[25]. On the other side of the ocean, the US Trade Representative's office indicated in its

[22] White House, 'Remarks by President Obama at the Hannover Messe Trade Show Opening,' 24 April, 2016, https://www.whitehouse.gov/the-press-office/2016/04/24/remarks-president-obama-hannover-messe-trade-show-opening

[23] European Commission, 'European Union-United States Trade Principles for Information and Communication Technology Services', 4 April, 2011, http://trade.ec.europa.eu/doclib/docs/2011/april/tradoc_147780.pdf. This generally positive collaboration continues outside the TTIP context; see for instance European Commission, 'Joint Statement for the 2015 (13th) EU-U.S. Information Society Dialogue',14 April, 2015, https://ec.europa.eu/digital-single-market/en/news/joint-statement-2015-eu-us-information-society-dialogue

[24] European Commission, 'Final Report of the High Level Working Group on Jobs and Growth', 11 February, 2013. http://trade.ec.europa.eu/doclib/docs/2013/february/tradoc_150519.pdf

[25] European Council, 'Directives for the negotiation on the Transatlantic Trade and Investment Partnership between the European Union and the United States of America,' Approved by the Foreign Affairs Council (Trade) on 14 June, 9 October, 2014, http://data.consilium.europa.eu/doc/document/ST-11103-2013-DCL-1/en/pdf

March 20, 2013, letter to Congress notifying it of the administration's intent to launch the TTIP negotiations that among the objectives it hoped to attain were:

'Electronic Commerce and Information and Technology Services

- Seek to develop appropriate provisions to facilitate the use of electronic commerce to support goods and services trade, including through commitments not to impose customs duties on digital products or unjustifiably discriminate among products delivered electronically;
- Seek to include provisions that facilitate the movement of cross-border data flows[26].'

At the time, the general feeling was that issues concerning e-commerce and data flows should not have been contentious between the EU and the United States.

The revelations concerning the National Security Agency's 'PRISM' program to access personal data held by US internet companies, published literally days before the formal launch of the talks in June 2013, completely changed the political context, however, leading to calls in Europe for terminating the EU-US 'Safe Harbour' program, imposing stricter data protection requirements through the EU's new General Data Protection Regulation, regulating internet platforms, and excluding data protection from TTIP altogether.

These new political sensitivities created an impasse in the TTIP negotiations on e-commerce and digital trade. Although the Commission's October 2015 'Trade for All' strategy includes an entire section on 'Facilitating Digital Trade[27],' the EU did not want to discuss the broader issue of data flows in TTIP absent agreement on a new data protection arrangement, and offered text only on e-commerce[28]. The text stipulates that customs duties will not be imposed on electronic transmissions as they shall be considered trade in services; affirms in principle that the provision of services electronically should not require authorization; allows for electronic contracts as well as electronic trust and authentication services; protects consumers against spam; and encourages regulatory cooperation on e-commerce issues. The text also includes an exception for measures that protect personal data (see Chapter 3).

Goaded by an industry that was unsettled about the tenor of the political debate in Europe post-Snowden, the US put forward text modelled on the Trans-Pacific Partnership (TPP) agreement, signed by the US and 11 other countries in the Pacific basin in February 2016. It also refused to discuss the EU's e-commerce provisions unless the EU took up data flows as well, arguing that protecting e-commerce without protecting data flows makes no sense.

The US text is not public, but the TPP agreement, among other things:

- Secures commitments not to impose customs duties on digital products and content transmitted electronically;
- Ensures non-discriminatory treatment of digital products transmitted electronically, and guarantees that these products will not face government-sanctioned discrimination based on the nationality or territory in which the product is produced;

[26] US Trade Representative, 'Letter from Ambassador Demetrios Marantis, Acting U.S. Trade Representative, to Congress,' 20 March, 2013, https://ustr.gov/sites/default/files/03202013%20TTIP%20Notification%20Letter.PDF. The letter also underscores that the Administration will "take into account other important U.S. objectives, including but not limited to the protection of health, safety, the environment, essential security and consumer interests."

[27] European Commission, 'Trade for All -- Toward a More Responsible Trade and Investment Policy,' October 2015; see especially Section 2.1.2, http://trade.ec.europa.eu/doclib/docs/2015/october/tradoc_153846.pdf

[28] European Commission, 'Transatlantic Trade and Investment Partnership: Trade in Services, Investment and E-Commerce,' pages 47-50, 31 July, 2015, http://trade.ec.europa.eu/doclib/docs/2015/july/tradoc_153669.pdf

- Provides for adoption of Electronic Authentication and Electronic Signatures;
- Establishes requirements that support a single, global internet, including free cross-border data flows, consistent with Article 14 of the WTO GATS;
- Requires non-discriminatory treatment for service companies of other TPP countries, and prohibits quantitative limits on market access, or requirements to use a specific type of joint venture or corporate form;
- Creates rules against localisation requirements that force businesses to place computer infrastructure, manufacturing or service facilities in each market in which they seek to operate, rather than allowing them to offer goods or services from network centres in sites that make better business sense;
- Includes measures against unsolicited commercial electronic messages (SPAM);
- Calls for close cooperation among parties to help businesses overcome obstacles and take advantage of e-commerce and promotes participation and transparency in the development of laws and regulations affecting the internet, including opportunities for public comment;
- Encourages cooperation on cybersecurity matters; and
- Ensures that no party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory[29].

While there are uncertainties on whether the provisions of TPP are replicable in TTIP, European industry sees them as a step forward in promoting international rules for the digital economy[30].

It now looks like this impasse is beginning to break, given the progress in February 2016 on a replacement to the Safe Harbour agreement (discussed in Chapter 3). This permitted some discussion during the April round of the e-commerce provisions that are common to the two sides[31]. And there is some talk among negotiators that the EU is considering offering a chapter on digital trade, which would reflect the broader ideas in the Trade for All Strategy noted above. That said, negotiating tactics could also preclude movement in the immediate future, since the EU is aware that the US is very interested in progress on this issue, but does not appear to be willing to make progress in issues of concern to Brussels.

Other Issues

Such tactical moves have a far wider import, however, since digital trade is so critical to the EU and US economic relationship, and therefore affects many other TTIP provisions:

Trade in Goods: Tariffs on virtually all major ICT products either have been or are being eliminated under the WTO's Information and Technology Agreement (ITA), originally concluded in 1996 and then expanded by an additional 201 products in July 2015[32]. But TTIP is also meant to eliminate duties on virtually all other

[29] DIGITALEUROPE, 'Assessment of the Trans-Pacific Partnership Provisions - Our recommendations for the Transatlantic Trade and Investment Partnership (TTIP) and the Trade in Services Agreement (TiSA),' January 2016, http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&entryID=1090&PortalId=0&TabId=353

[30] Ibid.

[31] European Commission, 'Report for the 13th Round of Negotiations for the Transatlantic Trade and Investment Partnership' New York, 25-29 April 2016, page 6, http://trade.ec.europa.eu/doclib/docs/2016/may/tradoc_154581.pdf

[32] See World Trade Organization, 'Information and Technology Agreement -- An Explanation' https://www.wto.org/english/tratop_e/inftec_e/itaintro_e.htm. The first ITA agreement covers products trade in which was USD 1.6 trillion in 2013; trade in products covered by the 2015 agreement amounted to USD 1.3 trillion that year.

products, including many – jewellery and apparel, for instance – where SMEs in particular could benefit from internet sales to American consumers. TTIP should also promote such trade by, for instance, facilitating returns as well as working on the e-authentication and e-trust services noted in the Commission's report above.

Customs Facilitation: One of the key aims of TTIP is to create a single electronic platform for EU and US firms so that an exporter's documents are provided automatically to all the relevant agencies on the importing side; some also hope this section will significantly increase the duty-free allowance for small parcels (which was just raised to USD 850 in the USA, but remains at EUR 28 in the EU) and perhaps simplify or even eliminate VAT payments for such small shipments. Again, this would have a direct impact on SMEs using the internet to export directly to U.S. consumers.

Trade in Services: As discussed above, cross-border trade in services has been significantly facilitated by the internet. Although in general both the EU and the US seek to liberalize this area, they differ significantly in approach: the US believes the most effective approach is for the two sides to grant service providers of the other party non-discriminatory treatment in all areas where the party doesn't take an explicit exception (the 'negative list' approach used by the EU in its trade agreement with Canada), while the EU suggests that entry into the market should be positively listed, with national treatment the general rule after that (a 'hybrid' approach being used in the services trade talks in Geneva). The negative list approach, among other things, would more easily allow for novel ways for delivering services, an approach the US advocates. In addition, the US wants to 'grandfather' any limitations state and other local governments might have, while the EU wants these exceptions to be spelled out. Many of the other obstacles to services trade are more regulatory than limitations on cross-border market access; these are discussed further below.

Investment: As noted above, the unique investment-based relationship between the EU and the United States powers trade between them. These investments rely on transatlantic data flows, not just for communications between headquarters and subsidiaries, but also operationally as the internet allows centralized administrative processing. Further, establishing a firm in another country is traditionally the most important way to 'export' services[33], although trade and investment are fundamentally different operations with fundamentally different rules. While investment in manufacturing is quite free on both sides of the Atlantic, in the services sector, the US has a number of significant limitations on foreign investment, including a 25 % foreign ownership requirement on some basic telecommunications providers (broadcasters, common carriers/transmitters), which the EU would like liberalized. The US Federal Communications Commission is reportedly considering loosening these restrictions[34].

Regulatory Issues: Much of the expected economic gains from TTIP are expected to come from the regulatory provisions in the agreement. In addition to speaking generally about commonly held principles and practices for good regulation, TTIP will focus on regulatory cooperation in areas that affect the trade of goods and services between the EU and the US (although regulatory cooperation is unlikely to touch 'purely' domestic regulation, such as water and air quality standards, labour conditions, etc.)[35]. This would include ICT standards, e-accessibility, e-health, e-accessibility and the like[36], as well as

[33] "Mode 3" in the parlance of the WTO's General Agreement on Trade in Services.
[34] M. O'Reilly, FCC Commissioner, 'Affirmatively Expand Permissible Foreign Ownership,' Federal Communications Commission, 3 March, 2015, https://www.fcc.gov/news-events/blog/2015/03/03/affirmatively-expand-permissible-foreign-ownership
[35] See e.g., P. Chase, J. Pelkmans, 'This Time It's Different: Turbo-charging Regulatory Cooperation in TTIP', Centre for European Policy Studies, Paper No 7 in the CEPS-CTR project 'TTIP in the Balance' and CEPS Special Report No 110, 4 June, 2015, https://www.ceps.eu/publications/time-it's-different-turbo-charging-regulatory-cooperation-ttip
[36] For a detailed description of the regulatory issues European and US industry jointly believe TTIP should cover, see DIGITALEUROPE, Information Technology Industry Council, 'ICT Industry Recommendations for Regulatory Cooperation in the

regulations governing cross-border trade in digitally-delivered services, such as professional services. In these areas, the relevant regulators on both sides will attempt to see whether the level of protection they demand for these goods and services is sufficiently equivalent to allow 'mutual recognition' of each sides standards rather than to make changes in the level of protection required under their domestic law. In this sense, it is unlikely that TTIP itself will address many of the broader digital issues such as programs relating to broadband development, net neutrality, anti-trust or platform regulation per se[37].

Implications for the EU's external relations

- Increased data flows between the EU and the US reinforce transatlantic economic integration, but such growing interdependence brings challenges as well as benefits, especially in the different approaches the two sides may take in regulating the internet.
- Uncoordinated approaches to the digital economy and data privacy may have negative repercussions on the transatlantic economy as a whole.
- Issues under discussion in the somewhat adversarial context of a trade negotiation can sometimes be better addressed in the more collaborative context of regulator-regulator discussions.
- A comprehensive and quantitative analysis of the contribution of digital transformation to the transatlantic economy could contribute to rebalancing global economic competitiveness in light of new technological realities.

3 Data Protection and Transatlantic Relations - the Commercial Dimension

3.1 Personal Data, Data Protection, Digital Trade and TTIP

The transatlantic debate over data protection has clearly affected the TTIP negotiations, although TTIP as a bilateral trade agreement will not affect the levels of protection for personal data in either the European Union or the United States.

Laws and regulations governing the protection of personal data of course can affect digital trade when they govern the transfer of personal data into or out of a jurisdiction, simply because so many internet-based communications – from hotel bookings to email – may involve the transmission of personally-identifiable information (depending on how broadly that term is defined).

That said, it is broadly understood in trade law that countries may adopt laws protecting personal data. The 1995 WTO General Agreement on Trade in Services (GATS) stipulates in Article XIV that '…nothing in this agreement shall be construed to prevent the adoption or enforcement by any Member of measures: … (c) necessary to secure compliance with laws and regulations …including those relating to: … (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; ….'[38] This general approach is

Transatlantic Trade and Investment Partnership', 2 February, 2015, http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&entryID=901&PortalId=0&TabId=353

[37] A. Renda, C. Yoo, 'Telecommunications and Internet Services: The Digital Side of TTIP', Centre for European Policy Studies and the Center for Transatlantic Relations, the Paul Nitze School of Advanced International Studies, Johns Hopkins University, Paper No 8 in the CEPS-CTR Project 'TTIP in the Balance' and CEPS Special Report No 112, July 2015, https://www.ceps.eu/publications/telecommunications-and-internet-services-digital-side-ttip

[38] World Trade Organization, 'Uruguay Round Agreement - General Agreement on Trade in Services', Article XIV, 1995, https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm

echoed in the 2011 EU-US Joint Statement on Trade Principles for Information and Technology Services, which indicates that the principles '…are also without prejudice to the policy objectives and legislation of the European Union and the United States in areas such as the protection of intellectual property, the protection of privacy and of the confidentiality of personal and commercial data, and the enhancement of cultural diversity (including through public funding and assistance)[39].' The United States also subscribed to this general approach of giving an exception for laws governing personal data protection in the Trans-Pacific Partnership Agreement, by explicitly incorporating GATS Article XIV (c), cited above, on data protection into the TPP agreement[40]. As the EU Trade Negotiator, Mr. Garcia-Bercero, averred in 2nd May remarks to the press[41], TTIP will also have a General Exceptions Chapter which will take a similar approach.

Some question whether this type of general exception is sufficient to ensure that trade law cannot compel changes in a country's data protection laws. To use the exception as a defence against a complaint by a partner under a trade agreement, a party must show that the data protection measures are tailored to the problem of protecting data, that they are necessary to achieve the purpose, that they are not a disguised restriction on trade, and that they 'do not constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail.' In the 44 cases where the general exceptions articles have been invoked as a defence, it has succeeded only once[42].

The point here, however, is that TTIP itself will not deal directly with data protection but will include an exceptions provision allowing measures to be taken to protect personal data. EU negotiators are confident that the EU laws will meet the scope, necessity and proportionality tests, as they would also need to do under the EU Treaties.

3.2 EU Personal Data Protection Law and Digital Trade

Europe has a long tradition of prioritizing the protection of privacy and personal data in the commercial realm, dating to the Council of Europe's 1953 European Convention on Human Rights (Article 8) and its 1981 Convention 108 on the 'Protection of Individuals with regard to the Automatic Processing of Personal Data.' At the EU level, the first major piece of legislation in this field was the 1995 Data Protection Directive (95/46)[43], followed by the Directive on Privacy and Electronic Communications (2002/58), and, most recently, the General Data Protection Regulation (2016/679)[44], published on 4th May, 2016, entering into force on 24 May, 2016, and formally applying as of 25 May, 2018.

[39] European Commission, 'EU-U.S. Joint Statement on Trade Principles for Information and Communications Technologies Services,' preamble, April 4, 2011, http://trade.ec.europa.eu/doclib/docs/2011/april/tradoc_147780.pdf. The general sentiment was also echoed by the EU and the United States (as well as France, Germany, Italy and the United Kingdom) in the April 29 'Joint Declaration by G-7 ICT Ministers', see point 18, where the parties pledge to "promote effective privacy and data protection across jurisdictions to meet high standards of privacy and data protection." http://www.mise.gov.it/images/stories/documenti/02_The_Declaration.pdf

[40] US Trade Representative, 'Trans-Pacific Partnership Agreement, Chapter 29, Exceptions and General Provisions', Section A, Exceptions; Article 29.1, General Exceptions, paragraph 3, https://ustr.gov/sites/default/files/TPP-Final-Text-Exceptions-and-General-Provisions.pdf

[41] European Commission, Statements by Ignacio Garcia-Bercero, 'EC technical briefing on-the-record on the 13th TTIP negotiations round debriefing,' 2 May, 2016, http://ec.europa.eu/avservices/video/player.cfm?sitelang=en&ref=I120640

[42] Public Citizen, 'Only One of 44 Attempts to Use the GATT Article XX/GATS Article XIV "General Exception" has Ever Succeeded: Replicating the WTO Exception Construct will not Provide for an Effective TPP General Exception', August 2015 https://www.citizen.org/documents/general-exception.pdf. Note that only one of these cases involved GATS Article XIV exceptions, and that was related to restrictions of on-line gambling services rather than data protection.

[43] EUR-Lex, 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.' 24 October, 1995, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=EN

[44] European Commission, 'Regulation 2016/679 of the European Parliament and of the Council of 27 April, 2016, on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and

Both the 1995 Data Protection Directive and the new 2016 General Data Protection Regulation (GDPR) establish stringent requirements on companies that control and/or process personally identifiable information within the EU, but this paper focuses only on those provisions that cover the transfer of personal data outside the EU, thus having a direct bearing on digital trade.

The two pieces of legislation are similar with respect to export of personal data (imported data must of course be treated in accordance with local laws), in particular in requiring that personal data of EU citizens and residents can only be transferred to jurisdictions that provide 'adequate' protection for such data. The legal and political context, however, has changed dramatically during the 21 years intervening between them, especially when it comes to government access to data for law enforcement and national security purposes.

The Data Protection Directive was adopted shortly after the entry into force of the 1992 Maastricht Treaty, which created the European Union and gave it – not the European Communities – some competence over encouraging coordination among the member states on certain law enforcement and foreign policy issues (the so-called Second and Third 'pillars' of the Treaty). Thus, while the preamble of the Data Protection Directive refers to the importance of protecting fundamental rights and freedoms, and refers in this connection to the Council of Europe's European Convention for the Protection of Human Rights and Fundamental Freedoms, it goes on to say in Article 3(2) that,

> '2. This Directive shall not apply to the processing of personal data:
>
> – in the course of an activity *which falls outside the scope of Community law (emphasis added)*, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law…'

This explicit exclusion of law enforcement and national security matters from the underlying law understandably governed the approach the Commission took with respect to transfers of personal data outside the EU.

In terms of transfers to third countries, Directive 95/46 is clear, saying in preambular paragraph 57, 'Whereas, on the other hand, the *transfer* of personal data to a third country which does not ensure an adequate level of protection *must be prohibited*' *(emphasis added).*

The Directive goes on to include two articles that clarify the application of this prohibition: Article 25, which allows the Commission to find that a country provides 'adequate protection,' and Article 26, which stipulates that where an adequate level of protection does not apply, a member state may allow the transfer of personal data when it takes place because the individual concerned has 'unambiguously' consented to the transfer, when the transfer is done in accordance with a contract, where a firm has undertaken sufficient guarantees to protect the data (generally through binding corporate rules), and where contract clauses provide adequate certainty with respect to the onward processing of the data[45].

In the twenty years since the Data Protection Directive was adopted, the Commission has determined under Article 25 that only five countries outside Europe have 'adequate' levels of protection: Argentina,

Repealing Directive 95/46/EC (General Data Protection Regulation)' 27 April, 2016, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[45] EUR-Lex, 'Data Protection Directive 95/46/EC', 24 October 1995, Articles 25 and 26, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=EN

Canada, Israel, New Zealand and Uruguay[46]. The United States is included in this list, but *only* to the extent that the firm involved in the transfer of the data adheres to the requirements of the Safe Harbour program.

3.3 Safe Harbour, and Its Adequacy

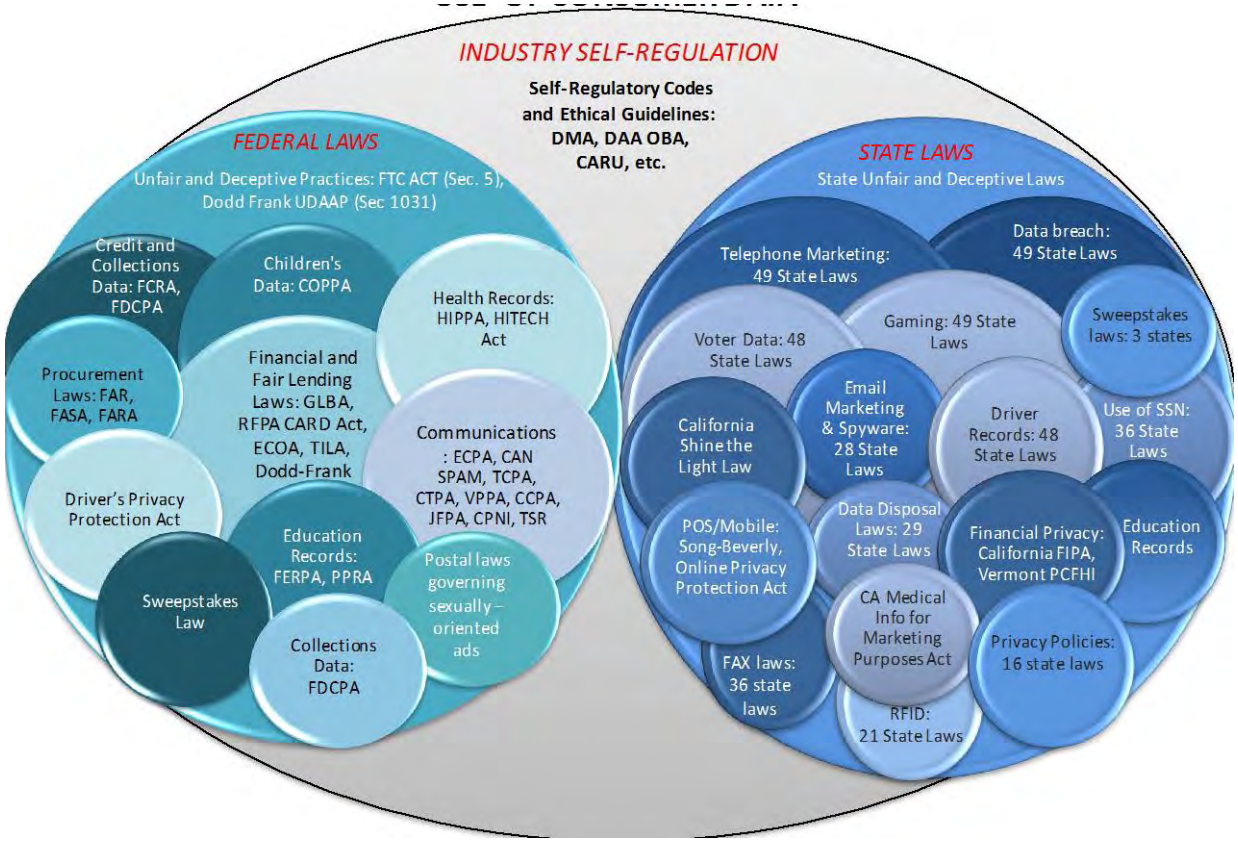
It took nearly five years for the EU and the United States to agree upon Safe Harbour in 2000 as a mechanism under which firms could transfer personal data from the EU to the United States in compliance with the Data Protection Directive.

The principal problem from the EU perspective was that the US lacks a generally-applicable law which regulates the way in which firms are allowed to process the personal data they possess. As a general matter, the US Constitution, subsequent law and Supreme Court jurisprudence focuses on limiting the extent to which governmental and law enforcement authorities can intrude into private space. Beyond that, the government has adopted a number of laws that restrict what private sector actors *in specific sectors* are permitted to do with personal data they collect, in particular with respect to finance, healthcare, students and under-aged persons. Similar laws have been enacted at the state level in many parts of the USA, leading to a colourful, if confusing, picture of privacy law in the United States as of mid-2013 (see Figure 8 below).

Thus, while in some areas (finance, health, etc.) data protection rules are more stringent in the United States than in the European Union, with potential criminal sanctions in the event of unauthorized disclosure or abuse of personal data, there is no general requirement that data controllers and/or processors obtain unambiguous personal consent from individuals with respect to the use of their data in sectors that do not have specific laws.

[46] European Commission, 'Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries,' http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

Figure 8: Laws and Regulations Governing Commercial Use of Consumer Data



Source: Experian

In this sense, it was impossible for the European Commission to find that the United States provided 'adequate' protection for personal data in the meaning of Directive 95/46.

Safe Harbour was a creative solution to this conundrum, given the importance of the immense flows of data taking place between the US and the EU. Under Safe Harbour, firms would agree to uphold seven principles – on notice (that data is being collected and how it will be used), choice (the ability to opt-out, including on onward transfers), onward transfer (only to other organizations accepting similar constraints), security (of the data collected), data integrity (relevance and reliability of the data for purpose), access (the right to correct data being held) and enforcement[47]. The Federal Trade Commission (FTC), which is responsible for ensuring truth in advertising, was the authority responsible for enforcing these self-certification pledges.

While some 4 500 firms (including numerous European firms with operations in the United States) pledged to adhere to the Safe Harbour principles, and were thus considered to provide 'adequate' safeguards with respect to the protection of personal data in compliance with Directive 95/46, Safe Harbour itself was never 'adequate' to cover all transfers of personal data to the USA. Among other things, the jurisdiction of the FTC did not extend to financial service firms, which instead had to adopt

[47] EUR-Lex,'2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.),' 26 July, 2000, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000D0520&from=en

'binding corporate rules'[48] ensuring that they would globally adhere to protections of the personal data of Europeans when such data was exported outside the jurisdiction of the EU. Beyond that, some 100 000 firms export from the USA to Europe[49], while untold hundreds of thousands (especially SMEs) more do business with individuals and firms in the EU (including when they visit the US). None of these were covered by Safe Harbour, and may or may not have been subject to 'standard contract clauses' governing the use of personal data collected in the conduct of their business.

3.4 The ECJ Decision on Safe Harbour

On October 6, 2015, the European Court of Justice (ECJ) annulled the Commission's 2000 decision on Safe Harbour, finding that individuals – such as the Austrian law student Max Schrems – had the right to question whether a third country provided adequate protections for personal data transferred there; that member state Data Protection Authorities (DPAs, in this case, Ireland's) had an obligation to assess the adequacy of third country protections; that whatever the DPA's finding, only the ECJ had the power to annul a Commission decision; and that in the case of Safe Harbour, the Commission's 2000 Decision had not taken into account whether the third country concerned (here, the United States) had in place adequate controls to ensure that government access to data collected by private firms would be necessary and proportionate. In this last respect, the ECJ judgement refers regularly to reading the Data Protection Directive 'in light of' the European Charter of Fundament Rights[50].

While the ECJ did not rule specifically about whether the United States provided adequate protections, it reiterates three times the sentiment expressed in the Data Protection Directive that transfers to third countries that do not provide such protections 'must be prohibited.' It underscores that 'the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter[51].' It notes that Safe Harbour only applies to firms, that exemptions limit the Safe Harbour principles 'to the extent necessary to meet national security, public interest, or law enforcement requirements,' and that the Commission did not consider whether there are any legal limitations on the ability of the state to 'interfere' with the fundamental freedoms of people. It further affirms that 'legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court's settled case-law, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data[52].'

The EU Data Protection Authorities (Working Party 29), in their statement of October 16 following the ECJ judgement, clarified further that, 'transfers to third countries where the powers of state authorities to

[48] As of 8 May, 2016, 83 firms are recognized as having adopted binding corporate rules for their global operations; of these, ten are financial services firms operating on both sides of the Atlantic, http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm

[49] N. Soroka, 'U.S. Trading Companies, 2012,' US Department of Commerce, November 2014, http://www.trade.gov/mas/ian/build/groups/public/@tg_ian/documents/webcontent/tg_ian_004048.pdf

[50] InfoCuria, 'Judgement of the Court (Grand Chamber), Case C-362/14, in re Maximillian Schrems v. Data Protection Commissioner,' 6 October, 2015. The judgement is worth reading in its entirety, http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EN

[51] InfoCuria, 'Case C-362/14,' op.cit. especially paragraphs 68-74.

[52] InfoCuria, 'Case C-362/14,' op. cit. see in particular paragraphs 79-98.

access information go beyond what is necessary in a democratic society will not be considered as safe destinations for transfers[53].'

Neither the ECJ judgement nor the DPA statement mentions that the Personal Data Protection Directive explicitly excludes law enforcement and national security from its scope, nor do they acknowledge that the European Charter of Fundamental Rights was not a part of EU law when Safe Harbour was concluded. The ECJ does, however, indicate that the Commission has an obligation to 'check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified….' And it notes further that 'when the validity of a Commission decision adopted pursuant to Article 25(6) of Directive 95/46 is examined, account must also be taken of the circumstances that have arisen after that decision's adoption[54].'

3.5 Privacy Shield, and the GDPR

The European Commission and US government authorities, notably the Department of Commerce and the Federal Trade Commission, had already been negotiating an update to the Safe Harbour agreement in the aftermath of the strong European reaction to the NSA revelations; those negotiations became even more intense following the ECJ's judgement and the opinion of the Data Protection Authorities, which essentially gave them until January 31, 2016 to conclude a new deal.

That deal, the EU-US Privacy Shield, was presented to the public on February 29, 2016[55]. The Privacy Shield arrangement places even more stringent obligations on firms that transfer personal data to the USA than under Safe Harbour, incorporates specific pledges by the US government with respect to government agency (intelligence and law enforcement) access to such data, and provides EU citizens additional sources of recourse and redress should they feel the data transferred to the USA is abused.

Privacy Shield, like Safe Harbour, is based on self-certification by firms that they will comply with key privacy principles, including:

- the Notice Principle, under which firms must inform individuals on key elements regarding the processing of their data;
- the Choice Principle under which individuals may object to the transfer of their data to third parties or any 'materially different' use of that data;
- the Security Principle, under which firms must take appropriate safeguards to keep the data they hold safe;
- the Data Integrity and Purpose Limitation Principle, where a company may not process personal data in a way incompatible with the purpose for which it was originally collected or subsequently authorized by the individual;
- the Access Principle, which ensures an individual can always get information on how his data is being used by a firm, and allows that person to correct, amend or delete personal information where it is inaccurate or has been processed in violation of the Privacy Principles;

[53] European Commission, 'Statement of the Article 29 Working Party,' 16 October, 2015, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf
[54] InfoCuria, 'Case C-362/14,'op. cit. paragraphs 76, 77.
[55] European Commission, 'COMMISSION IMPLEMENTING DECISION pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.' http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf

- the Accountability for Onward Transfer Principle, where a firm must ensure that any other party granted access to the data in accordance with the Notice and Choice Principles is subject to all the limitations in the agreement; and
- the Recourse, Enforcement and Liability Principle which requires a firm to put in place effective redress mechanisms to ensure enforcement of the Principles.

Firms will need to annually re-certify compliance with these principles and the U.S. Department of Commerce, as part of the Privacy Shield Agreement, undertakes to actively monitor compliance and to remove firms from the list that do not comply, including by working with EU DPAs. In addition to this oversight and enforcement through the Federal Trade Commission and Department of Transportation, EU citizens have a number of avenues for enforcing their rights, including through direct complaints monitored by the Department, referral to an independent dispute resolution body approved by the Department and if necessary facilitation by the Department. Further the FTC and Department of Transportation have agreed to give priority consideration to undertake enforcement action in response to complaints by the Department or EU DPAs.

And, as noted above and discussed in more detail below, the Agreement also incorporates letters from the Director of National Intelligence, the Department of Justice, and the Secretary of State with respect to government access to personal data of Europeans, with the latter importantly establishing an Ombudsman who will be able to respond to complaints about possible abuse of personal data by national security or law enforcement agencies.

In presenting the new agreement, the European Commission also proposed issuing a new 'adequacy' determination for companies that participate in Privacy Shield, as it believed that all these provisions in the agreement meet the concerns of the European Court of Justice decision as well as the requirements of the new General Data Protection Regulation. The EU Data Protection Authorities, in their 13 April, 2016 opinion[56] on Privacy Shield, 'welcomed the significant improvements' in it over the previous Safe Harbour agreement, but indicated that, on the commercial side, it is in many respects confusing; does not adequately address the issue of data retention; and is too vague with respect to onward transfers to third countries. With respect to governmental access to data, although the DPAs admit that Privacy Shield 'extensively' addresses this subject, they continue to believe it does not provide sufficient guarantees against 'massive and indiscriminate collection of personal data,' which 'can never be considered as proportionate and strictly necessary in a democratic society.'

Many of the DPAs' concerns were echoed in a European Parliament resolution of 26 May, 2016, which inter alia welcomes the significant improvements in Privacy Shield over Safe Harbour, but expresses concern over the US government's continued ability to collect and access bulk data, considers that the Ombudsman function in the State Department is not sufficiently strong to resolve EU citizen complaints about such activity, and notes that the redress mechanisms are too complicated[57].

The Commission and its US counterparts discussed these issues and adopted some modifications to the original Privacy Shield agreement that spell out conditions to ensure US agencies can only access data through 'targeted and focused' requests; ensure the Ombudsman is independent of the national security authorities; provide more explicit data retention terms; and clarify issues related to transfers to third

[56] European Commission, Article 29 Data Protection Working Party, 'Opinion 01/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision,' 16/EN, WP 238, 13 April, 2016, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

[57] European Parliament, 'European Parliament Resolution of 26 May 2016 on Transatlantic Data Flows,' 26 May, 2016. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0233+0+DOC+XML+V0//EN&language=EN

countries. These changes led to an adequacy decision[58] on 12 July, 2016, just as the 14th TTIP round began.

It remains widely presumed, however, that this Commission decision on Privacy Shield will be contested, not just under the previous Data Protection Directive, but also under the General Data Protection Regulation, which, while stronger than 95/46, in many respects carries forward its provisions on the transfer of data to third countries[59]. And today it is clear that the European Charter of Fundamental Rights is firmly established in EU law (although the new General Personal Data Protection Directive rather than the GDPR itself governs law enforcement and national security authorities' access to personal data).

3.6 Implications for Data Transfers from the European Union, and Its Connection to the Digital World

While considerable attention has been focused on the ECJ's decision annulling the Safe Harbour Agreement and on the subsequent Privacy Shield proposal, in many respects this misses the broader and more important issue – how can and should the European Union ensure that it is connected to the digital world, given that many countries beyond the United States may not provide 'adequate' guarantees for the fundamental rights of European citizens?

In its judgement, the ECJ made clear that an Article 25 adequacy decision by the European Commission must take into account – now in light of the European Charter of Fundamental Rights, which became a part of EU law in 2009 with the Lisbon Treaty – the underlying democratic controls in a country over law enforcement and national security agency access to data. It did not comment about whether these democratic controls should also apply with respect to the further derogations in Article 26, including individual consent, binding corporate rules and model contract clauses, but the logic of the ruling – the right to privacy free from intrusion of the government – would clearly seem to imply that it should. And indeed, some Data Protection Authorities (now empowered by the ECJ ruling to make their individual assessments) have stated that they believe this is the case[60].

If forced in a subsequent case to determine whether the United States has adequate democratic controls over the ability of government national security and law enforcement authorities to access personal data, the ECJ would need to take a number of developments since the revelations about the PRISM program into account, including[61]:

- President Obama's Issuance of Presidential Policy Directive 28, significantly restricting the activities of US intelligence agencies' ability to access personal data[62];

[58] European Commission, 'European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows,' 12 July, 2016. http://europa.eu/rapid/press-release_IP-16-2461_en.htm

[59] Numerous analyses have been written about the third country transfer provisions of the GDPR; see, for example, L. Power, 'Getting to Know the GDPR, Part 9 - Data Transfer Restrictions are Here to Stay, but so are BCR,' Field Fischer Privacy, Security and Information Blog, 24 February, 2016, http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-gdpr-part-9-data-transfer-restrictions-are-here-to-stay-but-so-are-bcr/

[60] See, e.g., Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein (Independent Centre for Privacy Protection Schleswig-Holstein), 'Positionspapier des ULD zum Urteil des Gerichtshofs der Europäischen Union vom 6 Oktober 2015, C-362/14,' 14 October, 2015, https://www.datenschutzzentrum.de/uploads/internationales/20151014_ULD-Positionspapier-zum-EuGH-Urteil.pdf

[61] For a much more detailed description of the following, see P. Swire, 'U.S. Surveillance Law, Safe Harbor and Reforms since 2013,' 17 December, 2015, https://fpf.org/wp-content/uploads/2015/12/White-Paper-Swire-US-EU-Surveillance.pdf; as well as B. Jacques, et al, 'Essentially Equivalent: A Comparison of the Legal Orders for Privacy and Data Protection in the United States and the European Union,' Sidley Austin LLP, 25 January, 2016, http://www.sidley.com/~/media/publications/essentially-equivalent---final.pdf

[62] White House, 'Presidential Policy Directive/PPD-28,' 17 January 2014, https://www.whitehouse.gov/sites/default/files/docs/2014sigint_mem_ppd_rel.pdf

- The December 2013 Report of the President's Review Group on Intelligence and Communications Technologies[63];
- The reports of the Privacy and Civil Liberties Oversight Board (PCLOB)[64];
- The increased funding of the PCLOB, which now has 32 staff in addition to its five board members;
- Significant limitations on bulk data collection enacted with the 2015 Freedom Act (amending the 2001 Patriot Act), and implementing greater judicial review of access to telephone records collected under Section 215;
- Declassification and publication of orders by the Foreign Intelligence Surveillance Court (FISC);
- Appointment of experts to advise the FISC on privacy and civil liberties;
- Expanded transparency of companies subject to national security orders[65];
- Greater reporting requirements required of the US government on its surveillance activities; and
- Passage of the Judicial Redress Act, which grants European citizens the same rights to contest in US courts alleged abuse of their personal information by the US government.

Many of these changes are discussed at length by the Commission in its Communication on the Privacy Shield as the reason that it believes that the United States provides adequate protections from unwarranted intrusion by the government on data held by firms -- even if some DPAs disagree. But whether these and many more steps by the US government assure the ECJ that indeed the United States has 'adequate' democratic protections over the government's ability to access the data of European citizens transferred to the United States remains to be seen. If, in the ECJ's judgement, the United States passes muster, then Privacy Shield, individual consent, Binding Corporate Rules and Model Contract Clauses governing transfers of personal data to the USA should all be permitted. If the ECJ finds the U.S. inadequate in these respects, then Privacy Shield would be annulled again. But further, the ECJ could well be compelled to rule whether the absence of adequate controls on governmental action also precluded the use of the other exceptions, which could mean that all transfers of personal data to the United States would be prohibited.

That of course would have a dramatic effect on transatlantic trade. But even if the U.S. is found adequate with respect to democratic controls, this would not solve the broader EU problem, for the personal data of European citizens is daily transferred to hundreds of other jurisdictions around the world. Some of these the European Commission has determined to provide adequate protections (as noted above, Argentina, Canada, Israel, New Zealand and Uruguay), but all of these determinations were made without regard to the European Charter of Fundamental Rights, and all of them can now be questioned by any individual and/or any DPA. This could prove difficult for countries such as Russia and China, as the former

[63] White House, 'Liberty and Security in a Changing World - Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies,' 12 December, 2013, https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

[64] See, e.g., Privacy and Civil Liberties Oversight Board, 'Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court,' 23 January, 2014, https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf; Privacy and Civil Liberties Oversight Board, 'Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act,' 2 July, 2014, https://www.pclob.gov/library/702-Report.pdf

[65] The statistics show far more targeted activity than the speculation in the popular press. Of the six categories reported, the highest percentage of users affected is for content requests to Google, a maximum of .0014 %, or about 1 in 100.000.

has been found by the European Court of Human Rights[66] to regularly access personal data transmitted to it, while the latter has been documented in a 2015 report to the European Parliament's Civil Liberties Committee as having inadequate protections even before considering questions of governmental access[67].

As the report on China just referred to goes on to state, however, it would be 'impractical' to prohibit data flows to China, given the immense economic and social relationship between the European Union and that country. This is undoubtedly more generally true, especially given that the value of Big Data and the Internet of Things both rely on their global reach, and making connections between data points that may not have been initially envisioned when the data was collected.

Implications for the EU's External Relations

- The ECJ's judgement bringing the European Charter of Fundamental Rights into the third country assessments under the Data Protection Directive 95/46 has significant implications with respect to the transfer of personal data from Europe to the rest of the world.
- This issue has increased in magnitude with the 2009 Lisbon Treaty incorporation of the European Charter of Fundamental Rights into EU law.
- The United States has responded to the Snowden revelations with significant steps to ensure that personal data transmitted from Europe is protected, both by companies under the new Privacy Shield regime and from government intrusion, but these steps will remain insecure until the European Court of Justice has examined them.
- If approved, the Privacy Shield could become a template for the EU for future agreements on the transfer of data abroad. A failure by the EU and the US to move ahead with the Privacy Shield, on the other hand, will have direct consequences on the transatlantic economy and may risk derailing talks over a transatlantic trade and investment partnership (TTIP).
- Given the transnational nature of digital data flows, the EU's high standards on data privacy could serve to put pressure on other countries to raise their standards but they could also hamper business and damage relations with countries that feel the standards are too high for their own countries.
- Other countries may or may not achieve the level of protection of personal data now being required of them, under existing law interpreted in light of the European Charter on Fundamental Rights or under the new General Data Protection Regulation. This legally could mean that the personal data of European citizens may not be transferred to these countries.
- This uncertainty could have a disruptive influence on the EU's ability to build its internet connectedness to the rest of the world if an appropriate balance between personal data protection and the ability of governments to interfere with such data cannot be found.

[66] See, e.g., European Court of Human Rights, 'Arbitrary and Abusive Secret Surveillance of Mobile Telephone Communications in Russia,' Roman Zakharov v Russia, 4 December, 2015, http://hudoc.echr.coe.int/eng?i=001-159324#{"itemid":["001-159324"]}

[67] P. Hert, V. Papakonstantinou, 'The Data Protection Regime in China,' European Parliament, Directorate for Internal Policies, Policy Department C: Citizens' rights and Constitutional Affairs, study commissioned at the request of the LIBE Committee, October 2015, http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf

4 The Transatlantic Digital Transformation, Law Enforcement and National Security

The United States and the European Union have been working for over a decade to strengthen collaboration on law enforcement and national security issues since these issues began to enter into the EU's remit with the Maastricht Treaty. They have had some notable successes, including the 2001 Europol-US agreement (and a supplement a year later)[68], the EU-US Mutual Legal Assistance Agreement on Criminal Matters[69] and the EU-US Extradition Agreement[70], both signed in 2003[71], and the Eurojust-US Agreement of 2006[72].

But this has not always come easily, and one of the most contentious issues has been law enforcement data sharing in the digital context. Indeed, one of the first actions taken by the European Parliament following the entry into force of the Lisbon Treaty in December 2009 was to reject the EU-US Terrorism Financing Tracking Program (TFTP) agreement, which set conditions on the U.S. Treasury Department's ability to access the SWIFT interbank transfer network in its efforts to fight terrorism and organized crime. Only with fairly extensive recrafting and intensive discussions with Members of European Parliament was the agreement finally accepted and concluded in 2012. A similar debate had taken place over an agreement on exchanges of Passenger Name Records, which had been provisionally applied since 2007 but which, at the insistence of the European Parliament, was re-negotiated and only came into force in 2012[73].

The concerns related to US government access to the personal data of Europeans for law enforcement and counter-terrorism/national security purposes had thus been around for a long time before the 2013 revelations about the NSA's PRISM program and other US government espionage activities in Europe. These concerns reflect in part different emphases about the role of government in protecting the safety of citizens, an emphasis which shifted dramatically in the United States after the September 2001 attacks on the World Trade Center towers in New York and on the Pentagon in Washington. But to some extent they also reflect institutional structures in the EU, where security and law enforcement responsibilities continue to lie with the member states[74].

A robust debate between the transatlantic partners over the appropriate balance between national security/law enforcement and privacy has become even more critical in the past two years, especially given the terrorist attacks in Paris in January and November 2015 and in Brussels in March 2016. Although Europe is no stranger to terrorist attacks, these have traditionally been more 'home grown;' recent attacks

[68] See pdf files of the agreements, available at Europol, 'External Relations, Operational Agreements with Non-EU States,' https://www.europol.europa.eu/content/page/external-cooperation-31

[69] European Commission, 'EU-U.S. Mutual Legal Assistance Agreement,' 6 June, 2003, http://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?redirect=true&treatyId=5441

[70] European Commission, 'Agreement on extradition between the European Union and the United States of America,' 25 June, 2003, http://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?step=0&redirect=true&treatyId=5461

[71] Indeed, in part to honour some of these achievements, a room in the Berlaymont has been named in honour of Mark Richards, the first Department of Justice Attaché to the U.S. Mission to the European Union.

[72] Eurojust, 'Agreement between Eurojust and the United States of America,' 6 November, 2006, http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/agreements/Agreement%20Eurojust-USA%20(2006)/Eurojust-USA-2006-11-06-EN.pdf

[73] European Council, 'Council Adopts new EU-US Agreement on Passenger Name Records,' 26 April, 2012, http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/129806.pdf

[74] See, e.g., C. Mortera-Martinez, 'Big Data, Big Brother: How to Secure Europeans' Safety and Privacy,' Center for European Reform, Open Society Foundation, December 2015, http://www.cer.org.uk/sites/default/files/pb_CMM_bigbrother_4dec15.pdf

have created an even more immediate sense of vulnerability. A number of EU member states are reforming the surveillance ability of their intelligence services in response. On 24 June, 2015, the French Parliament adopted a very controversial 'Patriot Act', granting intelligence agencies greater powers to collect, retain and access personal data, while in Germany, a reform of the intelligence services is expected to be adopted in the first half of 2016, reviewing and very likely restricting the collection and access of data by the Federal Intelligence Service (BND). Cooperation between the BND and the NSA is also said to have been already reduced[75]. In November 2015, while outlining a new National Cyber Security Plan for the UK to be published in 2016, the Chancellor of the Exchequer George Osborne argued that 'any new regulation will need to be carefully done – light enough and supple enough that it can keep up with the threat, so it encourages growth and innovation rather than suffocates it[76].'

And to some extent it was the Paris attacks that helped spur agreement on the EU's own Passenger Name Records law, as a deal was struck in December 2015 which included the possibility for Member States to include 'intra-EU' flights in the domestic implementation of the directive, a five years period of retention with a first six-months period of 'unmasked' data, and a range of new safeguards on the protection of data[77]. The PNR legislation was adopted in April 2016, in tandem with the General Data Protection Regulation and the Law Enforcement Data Protection Directive.

The challenge of digital transformation for Europe and US alike is clearly identified: how to ensure that the digitisation of economies and societies provides the appropriate guarantees for greater national and economic security. While these debates are in the first instance domestic and internal, they are also an important aspect of the bilateral relationship between the two.

4.1 The US Debate

In this connection, it is critical to bear in mind that a fierce debate rages in the United States about the appropriate balance between the use of digital technologies to protect US citizens and the concern about possible infringements on personal rights and freedoms that can come from this. The NSA's data gathering activities were widely seen as having over-stepped the bounds – indeed, the original co-sponsors of the Patriot Act under which the NSA was operating (the then respective chairmen of the Senate and House Judiciary Committees, Senator Patrick Leahy and Representative Jim Sensenbrenner) led the charge to amend that act with the Freedom Act, adopted in June 2015.

Similarly, US internet companies are fighting strenuously against perceived over-reach by the US government that they believe could undermine customers' trust in them. Microsoft is appealing a court order of the Second Circuit Court of Appeals against the US government's request for customer data stored by the company in Ireland. The request is part of a federal investigation on drug trafficking and raises the question whether US law enforcement authorities can use a search warrant to force a US- based company to provide access to data stored in Europe[78]. Beyond the question about the legality of the warrant, the case points to some of the most sensitive aspects of digital transformation.

[75] K. Connolly, 'German secret service BND reduces cooperation with NSA,' The Guardian, 7 May, 2015, http://www.theguardian.com/world/2015/may/07/german-secret-service-bnd-restricts-cooperation-nsa-us-online-surveillance-spy

[76] Government of the United Kingdom, 'Chancellor's speech to GCHQ on cyber security,' 17 November, 2015, https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

[77] European Parliament, 'EU Passenger Name Record (PNR) proposal: an overview,' 14 December, 2015, http://www.europarl.europa.eu/news/en/news-room/20150123BKG12902/EU-Passenger-Name-Record-(PNR)-proposal-an-overview

[78] S. Carswell, 'Microsoft warns of risks to Irish operation in US search warrant case,' *The Irish Times*, 25 February, 2016, http://www.irishtimes.com/business/microsoft-warns-of-risks-to-irish-operation-in-us-search-warrant-case-1.2548718

On 16 February, 2016, Tim Cook, CEO of Apple, published an online message to customers informing them of the Federal Bureau of Investigation's (FBI) request to Apple to build a backdoor to an iPhone recovered during the investigation of an act of terrorism in San Bernardino, California[79]. This software would give access to the iPhone's content, something perceived by Apple as a dangerous precedent threatening personal data protection. Apple has received the support of most of the tech community[80].

As noted in Chapter 3 above, the 2013 NSA revelations directly led to numerous steps by the Obama administration and by the US Congress to rectify the balance between data protection and national security and law enforcement. President Obama's Presidential Policy Directive 28, issued within half a year of the revelations, was a major step in this regard. The Freedom Act importantly codified major changes into law, including strengthened judicial oversight for FBI access to personal data held by companies; the need for a more precisely defined 'specific selection terms' to be used in searching for data; stricter time limits for accessing data and for its erasure; more detailed 'minimization' requirements to ensure destruction of data obtained incidentally; stricter transparency and supervision requirements; additional, narrower criteria on meta-data searches; and privacy procedures to ensure that data collected will not be inappropriately disclosed[81].

In addition to the Freedom Act and the Judicial Redress Act, the US Congress is also considering other critical pieces of legislation. The Email Privacy Act[82] amends the Electronic Communications Privacy Act (ECPA) of 1986[83] by clearly requiring a warrant to access stored electronic communications all the time. Current law allows for warrantless search of stored electronic communications older than 180 days, which seemed reasonable in 1986 when people did not store troves of communications indefinitely as they do with web-based email services. The bill passed the House unanimously on 27 April, 2016 and heads to the Senate, where it may face amendments and tougher scrutiny. Second, the Microsoft Ireland case mentioned above has highlighted the need to improve international legal frameworks that govern the transfer of electronic data across borders through due process when the harm being investigated has transnational impact – known as extraterritorial access to data. The pending Law Enforcement Access to Data Stored Abroad (LEADS) Act[84] would amend ECPA to improve the efficiency and transparency of the MLAT process while also clarifying that US law enforcement may obtain a warrant for any electronic communication physically stored within US territory or if the account-holder is a US person, regardless of where it is stored. Both the LEADS Act and Email Privacy Act would help update and clarify the US legal framework.

[79] T. Cook, 'A Message to Our Customers,' Apple, 16 February, 2016, http://www.apple.com/customer-letter/

[80] Microsoft, 'Brief of Amici Curiae Amazon.com, Box, Cisco Systems, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest, Pintrest, Slack, Snapchat, Whatsapp and Yahoo in support of Apple, Inc.' ED No CM 16-10 (SP), 22 March, 2016, http://mscorpmedia.azureedge.net/mscorpmedia/2016/03/smith_post.pdf

[81] F. Boehm, 'A Comparison between US and EU Data Protection Legislation for Law Enforcement Purposes,' European Parliament, Directorate for Internal Policies, Policy Department C: Citizens' rights and Constitutional Affairs, study commissioned at the request of the LIBE Committee, September 2015; see especially Section 3.4, http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf

[82] US Congress, 'H.R.699 - Email Privacy Act,' 2 April, 2015, https://www.congress.gov/bill/114th-congress/house-bill/699

[83] The ECPA is the primary source of law governing electronic privacy, and it is seen by many as outdated. It contains three parts. The first outlaws unauthorized interception of wire, oral, or electronic communications and also provides a framework for lawful interception with judicial oversight, which was itself an amendment of the Omnibus Crime Control and Safe Streets Act of 1968. The second part is known as the Stored Communications Act, focusing on privacy of stored communications such as email. The third part focuses on government procedures for pen registers as well as on trap and trace devices. ECPA has been amended several times, most prominently by the Communications Assistance for Law Enforcement Act of 1994 (CALEA), the USA PATRIOT Act of 2001, the USA PATRIOT Improvement and Reauthorization Act of 2006, and the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008.

[84] US Congress, 'H.R.1174 - Law Enforcement Access to Data Stored Abroad Act,' 27 February, 2015, https://www.congress.gov/bill/114th-congress/house-bill/1174

4.2 Creating a Transatlantic Dialogue to Re-Build Trust

Whether these changes to US law and practice governing law enforcement and national security access to personal data and the strictures imposed on commercial use of personal data by the new Privacy Shield agreement are sufficient to (re-)establish at least legally the 'essential equivalency' of the US and EU regimes on data protection, as a group of eminent European and US lawyers contend[85], will probably only be determined should the European Court of Justice deliver an opinion on this after reviewing the adequacy of the Privacy Shield arrangements.

But to some extent this debate over the 'equivalence' and 'adequacy' of the US legal regime misses the broader point – the need for a strengthened political dialogue between the United States and the European Union on the issue of the appropriate balance between data protection and law enforcement/national security. Such a dialogue, if done properly, can help restore political trust between the transatlantic partners, both at the governmental level and indirectly at the commercial and citizen level.

Such a dialogue could cover three suites of issues, including the general one of political oversight of law enforcement and national security activity; the operational one of new mechanisms for extraterritorial access to data through a mutual legal assistance framework appropriate to the digital age; and a practical one on cybersecurity and encryption standards[86].

4.2.1 Oversight

Perhaps somewhat ironically, the recent steps to ensure greater oversight of the activities of law enforcement and national security agencies in the USA has led some experts to conclude that 'contrary to popular representation, US laws on oversight of surveillance contain myriad constraints on the security services … (that are) more comprehensive than similar laws[87]' in many EU member states, and probably than in the EU itself. Especially as some member states go further to strengthen their ability to detect and prevent possible terrorist attacks in Europe[88], more in-depth discussions among relevant US and EU politicians about how to establish actual oversight (as opposed to theoretical compliance by virtue of obligations undertaken pursuant to the European Charter of Fundamental Rights and the European Convention of Human Rights) could prove useful.

Such a dialogue could include discussions about possible updates to the 1981 ECHR Convention 108 on automated data processing; mechanisms for permanent, independent oversight such as the Privacy and Civil Liberties Oversight Board; the incorporation of adversarial counsel to ensure independent views are heard; publication of all non-classified elements of authorizing decisions and oversight reports of agency activity; defining public standards for the rights of non-citizens; and judicial or quasi-judicial review of all surveillance requests.

[85] Jacques et al, 'Privacy and Data Protection,' op. cit.

[86] Many of the ideas noted here are derived from the recommendations of a U.S.-German panel of experts 'Transatlantic Digital Dialogue: Rebuilding Trust through Cooperative Reform,' convened by The German Marshall Fund of the United States as well as the Stiftung fuer Neue Verantwortung, 5 November, 2015 http://www.gmfus.org/publications/transatlantic-digital-dialogue-rebuilding-trust-through-cooperative-reform; as well as those of a broader expert panel under former Swedish Prime Minister Carl Bildt and former U.S. Ambassador to the European Union, William Kennard, convened by the Atlantic Council, 'Building a Transatlantic Digital Marketplace: Twenty Steps to 2020,' April 2016, http://www.atlanticcouncil.org/images/publications/Building_a_Transatlantic_Digital_Marketplace_web_0406.pdf

[87] Ben Scott, 'Transatlantic Digital Dialogue,' op. cit. p. 6.

[88] See, e.g. European Union Agency for Fundamental Rights, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU,' 18 November, 2015, http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services

4.2.2 Law Enforcement Data Transfers

The European Union and the United States had been discussing 'principles' governing law enforcement agency cooperation and data transfers for years before the NSA revelations and concerns about Safe Harbour prompted them to intensify their negotiations and eventually conclude, on 8 September 2015, the so-called 'Umbrella Agreement' governing the exchange of personal data in the context of law enforcement cooperation[89].

This 14-page agreement, which was signed[90] on 2 June 2016, following the adoption of the Judicial Redress Act, sets framework understandings about how personal data obtained through law enforcement procedures will be transmitted, processed, transferred to other authorities, secured, retained, amended and the like, but it does not establish an actual mechanism for data transfers; those derive from more operational agreements between relevant EU and member state authorities with their US counterparts[91].

One of the most important mechanisms for exchanges of personal information in law enforcement proceedings are the Mutual Legal Assistance Treaties. These are in general woefully inadequate for the digital age, which is the main reason the Department of Justice is arguing so strenuously against Microsoft's contention that it needs to go through the MLAT process to access data the company holds in its servers in Ireland -- it contends that in the digital world electronic evidence could be too easily transferred to jurisdictions where law enforcement authorities could not access it. At the same time, in the case of foreign countries seeking the content of communications stored in the USA, the US Department of Justice and many US companies have interpreted the ECPA as prohibiting disclosure of electronic communications to a foreign government without a warrant issued by a US judge based on probable cause[92]. This means that foreign government access to certain data stored in the United States can move slowly through MLAT procedures, taking roughly 10 months per request.

The EU- US MLAT is particularly limited in scope and out of date; it needs to be renewed for the digital age. At the same time, politicians on either side – who are in general concerned about effective law enforcement – need to discuss politically how the transatlantic partners can avoid unnecessary situations of conflict of law.

4.2.3 Encryption and Cybersecurity Cooperation

The debate over data encryption has been heated in the USA ever since the NSA revelations of 2013. US companies, civil liberties advocates, and others favour universal strong encryption. On the security side, law enforcement and intelligence agencies have been pushing back, while the US military appears to favour strong encryption because of a concern for securing critical infrastructure, weapons systems, and C4ISR capabilities (command, control, communications, computers, intelligence, surveillance, and reconnaissance). Congress has called for a commission to study encryption, with Rep. Michael McCaul, co-chair of the Congressional Cybersecurity Caucus, leading the charge. The ENCRYPT Act was introduced

[89] European Commission, 'Agreement between the United States and the European Union on the Protection of Personal Information relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses,' 8 September, 2015, http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf

[90] Council of the European Union, 'Enhanced Data Protection Rights for EU Citizens in Law Enforcement Cooperation: EU and US Sign "Umbrella Agreement,"' 2 June, 2016, http://www.consilium.europa.eu/en/press/press-releases/2016/06/02-umbrella-agreement/

[91] This may be one reason why Dr. Boehm, in her brief analysis of the Umbrella Agreement, expresses doubt as to whether it meets EU data protection requirements; see footnote 80, and in particular Addendum: Brief Analysis of the Umbrella Agreement, pp. 71-74.

[92] G. Nojeim, "MLAT Reform Proposal: Eliminating U.S. Probable Cause and Judicial Review," Lawfare, 4 December, 2015, https://www.lawfareblog.com/mlat-reform-proposal-eliminating-us-probable-cause-and-judicial-review

in February 2016 in an effort to ensure that there is one national standard on encryption, rather than a state-by-state patchwork, which is emerging as a possibility.

Senators Diane Feinstein and Richard Burr, intelligence committee leaders, introduced a bill that seeks to put limits on encryption in April 2016, known as the Compliance with Court Orders Act of 2016. It is already being harshly criticized by privacy advocates and computer security experts alike. It is too soon to predict where the encryption debate in the USA will end up, but if a standard of universal strong encryption were eventually agreed upon as the best option, the specifications would likely be issued by the National Institute of Standards and Technology.

Similarly, recent terror attacks and mounting threats (including the estimated USD 445 billion global cost of cyber-crime) are pushing EU member states to take sides on the issue of encryption. The European Commission has expressed its opposition to any kind of backdoor identification systems based on encryption[93], while the European Parliament has also hinted at its support to encryption as being 'useful to citizens and businesses as a means of ensuring privacy and at least a basic level of communications security[94].' Yet new legislation in various member states might impede a unified approach to encryption in the near future. In particular, surveillance and antiterrorism reforms in the UK and in France could make tech companies liable for refusing to provide encrypted information – or even helping law enforcement agencies to get access to encrypted information[95]. Others, like Germany and the Netherlands, are resisting plans to create backdoors to encryption for national security purposes. In the short term, this might lead them as well to discuss more openly the qualification of computer code as speech – and whether governments can compel writing code or if this would equate to compelling speech[96].

While the debate about encryption is not new – especially with regards to differing approaches between the US administration and the European Commission[97] – it is more than ever linked to increased concerns over the balance between the right to privacy, lawful access to data and unlawful (if not criminal) access to data. Security policy is ultimately a national issue, but 'building resilient defences against such global threats is a mutual interest and could be a constructive area of re-establishing trust[98].' Discussions about an appropriate approach to this issue could also set the stage for further political (as opposed to 'technical') dialogue on such key cybersecurity issues as threat intelligence, industrial espionage, transnational cybercrime and critical infrastructure protection.

Many of these issues are reflected in the Network and Information Security (NIS) Directive[99], where political agreement among the EU institutions in December 2015 paved the way for approval in the Internal Market Committee in the European Parliament in early January 2016[100]. The European Parliament

[93] J. Valero, 'Ansip: 'I am strongly against any backdoor to encrypted systems'', EurActiv, 23 February, 2016, https://www.euractiv.com/section/digital/interview/ansip-i-am-strongly-against-any-backdoor-to-encrypted-systems/

[94] European Parliament, 'Report on Towards a Digital Single Market Act (2015/2147(INI))', A8-0371/2015, 12 December, 2015, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2015-0371+0+DOC+PDF+V0//EN

[95] M. Scott, 'American Tech Giants Face Fight in Europe Over Encrypted Data,' *New Yok Times*, 27 March, 2016, http://www.nytimes.com/2016/03/28/technology/american-tech-giants-face-fight-in-europe-over-encrypted-data.html?_r=0

[96] See for instance: N. Richards, 'Apple's "Code = Speech" Mistake,' MIT Technology Review, 1 March, 2016, https://www.technologyreview.com/s/600916/apples-code-speech-mistake/

[97] See for instance: *The Wall Street Journal*, 'EU Commission Rejects U.S. Plan on Encryption,' 8 October, 1997, http://www.wsj.com/articles/SB876322992856833000

[98] Scott, 'Transatlantic Digital Dialogue,' op. cit., p. 15.

[99] European Commission, 'Commission welcomes agreement to make EU online environment more secure,' 8 December, 2015, http://europa.eu/rapid/press-release_IP-15-6270_en.htm

[100] European Parliament, 'First-ever EU-wide cyber-security rules backed by Internal Market Committee,' 14 January, 2016, http://www.europarl.europa.eu/news/en/news-room/20160114IPR09801/First-ever-EU-wide-cyber-security-rules-backed-by-Internal-Market-Committee

formally adopted the Directive on second reading on 6 July, 2016[101]. While implementation could take up to 21 months after publication, the NIS Directive is a significant step forward towards a unified cybersecurity system in the EU. With on the one hand member states having to identify themselves as operators of essential services, and with on the other hand the inclusion of some digital service providers such as search engines and cloud computing, the directive attempts to strike a balance between privacy, security and the economy.

On the US side, the Cybersecurity National Action Plan (CNAP) was adopted in February 2016. President Obama also signed an executive order that creates the Commission on Enhancing National Cybersecurity to study how to improve security in the digital world, including developing a national plan for the Internet of Things. The Commission's report is due 1 December, 2016. Among other initiatives, CNAP includes the creation of a Federal Chief Information Security Officer and a new Federal Privacy Council, which will bring together the chief privacy officers from 25 federal agencies to coordinate efforts to protect privacy with regards to the information the US government collects. Further, the Cybersecurity Information Sharing Act (CISA) was signed into law in December 2015, soon after the USA Freedom Act. Criticized by some privacy advocates as surveillance by another name, CISA was designed to encourage disclosure and sharing of threat indicators by private companies with the US government. It provides liability protections to reduce fear of lawsuits when a company's data is stolen or manipulated. By encouraging sharing of ever-evolving malicious code and other threat indicators, the new law seeks to improve cyber defences and situational awareness.

Implications for the EU's External Relations

- Transatlantic cooperation in the fight against cross border crime and terrorism is essential. Digital technologies are raising new challenges for law enforcement agencies in the prevention and investigation of criminal and terrorist activities. The US and the EU face similar difficulties in addressing the need for access to information and protecting the rights and freedom of the user, yet there remains too little coordination at the political level.
- The lack of trust between Europe and US when it comes to digital technologies, especially with respect to governmental access to data, could damage transatlantic relations. Many in Washington believe the EU seeks to impose tougher conditions for the protection of EU data in the US than it is asking other, often less democratic, countries to do.
- Beyond the question of trust, current sparks in transatlantic relations related to access to and the free flow of data further indicate the level of interdependence between the EU and the US in this new digital world. While interdependence can lead to greater efficiency and effectiveness in the digital society, it can also lead to strains should partners seek to re-establish national barriers, and damage the transatlantic relation as a whole.
- As a counter-weight to this, working collaboratively with the US and other countries on developing frameworks for managing security concerns in a changing world presents opportunities to shape outcomes and earn good will.
- The Judicial Redress Act has been passed largely with European partners in mind, indicating a desire in the USA to coordinate and collaborate with the EU. There is a broad constituency of willing partners in the USA that wants to reach common ground with EU partners.

[101] European Parliament, 'Cybersecurity: MEPs Back Rules to Help Vital Services Resist On-line Threats,' 6 July 2016, http://www.europarl.europa.eu/pdfs/news/expert/infopress/20160701IPR34481/20160701IPR34481_en.pdf

- The US debate and policy is evolving quickly; it will be important for the EU to closely monitor these developments, especially as a general domestic consensus on what the 'new normal' should look like remains elusive. The push from the private sector on the Internet of Things, smart homes, smart cities, etc. is simultaneously putting pressure on policy makers to resolve security and privacy questions due to the economic potential of these technologies.
- EU policy on cyberspace remains embryonic. Its piecemeal approach to preventing terrorism, fighting organized crime and cybercrime is facing systemic obstacles directly related with member states' competence on matters of national security. Despite existing frameworks, such as the EU-US Cyber Dialogue, clarity on the EU's ability to engage strategic partners on these issues is lacking.
- The EU and the US can set the standard for addressing the nexus between privacy, national security and the economy. Other regions of the world that are faced with similar transformations may adopt such a new equilibrium.

5 The Digital Transformation and Transatlantic Foreign Policy Cooperation

The focus of this paper has been on the most immediate issues surround the digital transformation and the transatlantic relationship – TTIP, Safe Harbour/Privacy Shield and the need for understanding and greater collaboration on the law enforcement and national security aspects of digital personal data.

This, however, only touches the surface of the opportunities for greater foreign policy collaboration between the European Union and the US on digitally-related issues. Precisely because these technologies are becoming so ubiquitous and powerful, they have become critical tools in the foreign relations between the EU, the US and third countries. And it is in this third country aspect that digital technologies can broaden and enrich EU - US relations.

One of the most important of these is democracy promotion. Early collaborative efforts between the EU and the US to promote the internet to build political pluralism occurred in Tunisia and other northern Mediterranean countries in 2006; this may well have been part of the foundation that led to the Arab Spring. While that movement has not yet fully delivered on the promise of strengthened democratic governance in these countries, the tools of the internet are essential for that political transformation to take place. Greater EU - US collaboration here is essential.

This is especially important given that many countries are trying to control their citizens' access to global voices, or worse, to use the internet and social media to weaken democratic traditions, even among Western countries. Here, one of the key responsibilities of the transatlantic partners will be to ensure that the governance of the internet continues to uphold the values of democracy, pluralism and free speech as international governance of the internet is itself transformed into a more 'stakeholder-driven' approach[102]. Transatlantic collaboration here too is essential, as is a sustained political effort to combat the use of the 'dark internet' for more nefarious purposes.

Beyond this, virtually anything the EU or the US might do to promote development in poorer countries can and should now fully engage digital technologies – and all such efforts can only be strengthened by seeking synergies among what the US, the EU and the member states do in their development assistance programs. One of the most basic aspects of this should include accountability for development projects – ensuring that each of these are online and that stakeholders, whether from the local populace, NGOs or

[102] The issue of transatlantic collaboration on "leading in Global Internet Governance" is discussed in more detail in the Atlantic Council report, 'Building a Transatlantic Digital Marketplace' op. cit. see especially pages 31-33.

others – can contribute reports on the efficacy of the efforts, reports which should be publicly available on the web, and to which project officials should try to respond.

But everything from efforts to promote agricultural productivity, environmental monitoring, health care and education initiatives and the like can and should take advantage of the increased ability to gather, analyse and use data.

The internet of things is already a tremendous instrument to promote growth in the EU and the US, and to bind them more closely together. It can do still more in spurring collaboration between them elsewhere around the world, if these efforts are given the appropriate political direction.

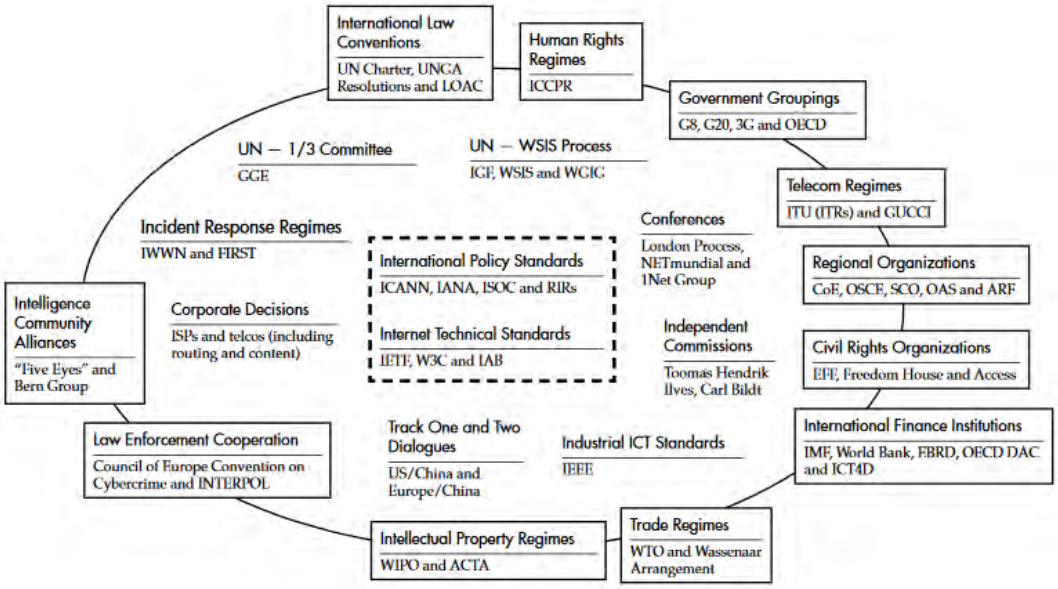
Clarifying the terms used in the international discussion of cyberspace is critical. Although 'cyber' has come to mean only the security aspects of networked electronics, it broadly refers to the same web of electronics that are networked across the globe via the Internet and other transmission mechanism that 'digital' refers to. But the catchall terms 'digital' and 'cyber' are often conceptually separated, to the detriment of law, policy, and discourse. It is confusing to citizens who are strained by a rapidly changing world, and it makes it harder to reach common understandings among policymakers around the globe.

Insofar as certain digital electronic devices are not networked, they are not relevant to questions of international trade and security because their inability to receive and transmit information through the electromagnetic spectrum across borders removes the geopolitical and geo-economic aspects of their use. Thus, discourse in the international arena would be better served by highlighting the specific networks, information flows, and storage locations of electronic data as much as the electronic devices themselves. Moving toward a unified concept of the 'digital' or 'cyber' domain as a catchall term will be important for institutions, strategies, and policies, as well as for communication with the general public. It is worth bearing in mind the technical engineering usage of the term 'digital' versus the political economy concept encapsulated by the terms 'digital economy' or 'digital transformation.' They have very different meanings and confuse discourse when computer engineers try to engage with economists and politicians. In the EU-US context, highlighting these linguistic issues and taking the time to clarify what terms mean would help policymakers and citizens on both sides of the Atlantic reach greater understanding in their conversations and in communicating with their publics.

Aside from the linguistic challenges, digital/cyber/Internet debates have a plethora of forums and decision-making bodies that often make it difficult to know where important decisions are made in the international context. Joe Nye attempted to map the 'regime complex' in a 2014 paper and his illustration provides a useful visual[103].

[103] Joseph S. Nye, Jr. 'The Regime Complex for Managing Global Cyber Activities' *Global Commission on Internet Governance Paper Series No. 1* (May 2014), p. 8, https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities

Figure 9: The Regime Complex for Managing Global Cyber Activities



This constellation of institutions and arrangements can make it difficult for observers and policymakers to understand where important decisions are taken and where real power lies. Though many groupings and organizations can be useful as forums for discussion – such as the Freedom Online Coalition – it can be difficult for citizens, organizations, corporations, and governments to understand where to invest time and resources. It can also lead to forum shopping by different actors with widely varied views of what the internet should be, which can strain the international system and international law that rely on states as the core guarantors of security, rule of law, and stability.

The 'multi-stakeholder' process of governance pioneered by organizations such as ICANN has met resistance in some states, although democracies tend to support it. EU-US collaboration on devising ways to more systematically incorporate 'multi-stakeholder' governance models with the state-led international system is an important aspect of collaboration on foreign policy in this area. Identifying which institutions are important decision-making bodies in the view of the US and EU, and which ones are more consultative, could help the two sides better shape global governance of cyberspace more broadly. Recognizing that institutional forms of governance such as ICANN's are fairly novel in terms of governance will be necessary in building more constructive common positions vis-à-vis countries such as Russia or China. Explaining the value of this model in clear and precise terms could help dispel some of the intense disagreement about the appropriate role of the state in Internet governance.

This process of collaborating on linguistic and institutional clarification could help build greater trust on cyber/digital issues between the EU and the US, in addition to facilitating forging a common agenda in the global context. The challenges to the structure of the international system posed by increasing connectivity and borderless data flows are real and will require creative thinking about how the system should evolve to meet these challenges.

Implications for the EU's External Relations

- The digital transformation can and should be incorporated into all aspects of foreign and development policy, given the connectedness of the globe and its importance in virtually everything we do. Extensive sharing of best practices between transatlantic partners can help both the EU and the US implement this vision.
- Transatlantic cooperation on internet governance will be more difficult if there is not mutual understanding of concepts and terms in international discourse, as well as which institutions that is

most important as decision-making bodies. Neglecting to take the time to clarify these important questions could lead to unnecessary US-EU friction.

- The opportunities for engaging third countries on digital transformation would benefit from shared understandings of priorities between the EU and US, and creation of as much of a common agenda as possible.

6 Recommendations

General Recommendations

Recommendation 1: Restore clarity in the debate about digital transformation

Much of the confusion about greater transatlantic cooperation on digital issues stems from the lack of clarity between the various issues at stake. In the political discussion about the digital transformation in the EU, privacy, data protection, digital flows, commercial use of data, digital rights, etc., are often bundled together. Yet these are very different policies, with very different implications on economies and societies. In this connection, it is particularly important to understand the immense benefits that the digital transformation can bring, while at the same time distinguishing between how the commercial sector in general handles the personal data it collects, with obligations that may be placed on firms by governments in whose jurisdictions they operate. Additionally, the discourse surrounding the terms *digital*, *cyberspace*, and *the internet* should be clarified, because these terms all refer to networked computers and other electronics in some fashion, but whether they are being used interchangeably or to describe distinct phenomena is poorly understood by policy makers around the world, as well as publics. Breaking down the discourse and clarifying what these words mean through clear definitions is essential to effective debate on policy and legal questions.

Recommendation 2: Affirm EU principles on promoting and protecting citizens' rights online

Europeans should stand by and affirm that the right to privacy is a fundamental right in the EU. Without giving in to the temptation of digital protectionism, and with a good measure of security threats weighing on the continent, the EU should continue upholding the same level of principle as it always has when it comes to the protection of personal data. But this principle must also be pragmatically tempered by the realities of digital transformation, with the appropriate balances sought between digital growth, data protection and national security.

Recommendation 3: Build certainty in the framework to transfer data across borders

The Privacy Shield agreement should help to restore legal certainty in the transfer of data across the Atlantic, but uncertainty will remain about it and other mechanisms for facilitating commercial data transfers until the European Court of Justice rules on the underlying adequacy of 'democratic controls' in the USA. But resolving the transatlantic issue may not resolve the broader question that faces operators in the EU – namely, whether other mechanisms are sufficient in the absence of a firm legal ruling about the adequacy of democratic controls in all *other* countries. In today's digital world, it cannot be the legislator's intent to prohibit all transfers of personal data – including pursuant to personal decisions – to these countries, as this is undoubtedly 'impractical' (as was indicated in the case of China, see page 30). The EU institutions may need to provide some political guidance on this question to the Data Protection Authorities and other relevant bodies in the EU.

Recommendation 4: Strengthen the Transatlantic Digital Dialogue in all EU institutions, and establish an explicit goal of creating a Transatlantic Digital Marketplace

The Commission and its US counterparts have numerous 'digital dialogues' at various levels. Given the importance and transformational nature of the internet and the digital world, the transatlantic partners would benefit from a cross-sectoral higher-level discussion that brings these strands together, much as the EU - US Energy Council has done. But this high-level political dialogue can and should go beyond the Commission to involve the Council, member states, European Parliament and indeed relevant players in key national parliaments.

Recommendation 5: Explicitly include the digital economy as part of trade and investment negotiations

With progress being made in the TTIP negotiations in chapters touching upon the central elements of the digital economy, especially on e-commerce services and regulatory cooperation on ICTs, TTIP provides an opportunity for the EU to further define an ambitious template for digital provisions in its trade agreements. The EU's Trade for All Communication seeks to facilitate digital trade and tackle new forms of digital protectionism, and this spirit should be fully incorporated in its other trade agreements, including with developing countries.

Recommendations for the European Parliament

Recommendation 6: Use the Transatlantic Legislators' Dialogue to explore collaboration on rules for the digital age

Issues related to the digital economy and to data privacy are politically sensitive on both sides of the Atlantic. Hence, the involvement of both members of the European Parliament and members of Congress is crucial for providing political guidance to the US administration and the European Commission as they move ahead to try to find the right balance between privacy, security and the economy. Moreover, legislators benefit from a degree of legitimacy that many citizens appreciate seeing in institutions that may decide on the treatment of their personal information.

While many discussions take place between relevant committees of the European Parliament and their US Congressional counterparts, the Transatlantic Legislators' Dialogue (TLD) provides a unique opportunity to bring various specific concerns together and to identify common threads among them for a more robust political discussion. This is particularly true as both Congress and EP members serve in many different committees, facilitating the multi-sectoral perspectives so important when considering policies affecting the digitalizing world.

One specific area TLD could explore is comparing and assessing steps both sides are considering to create rules for the Internet of Things, including with respect to privacy and security by design, encryption and the like. Another important theme should be joint efforts to promote and safeguard the multi-stakeholder governance process in ICANN and elsewhere.

Recommendation 7: Assess the quality of 'democratic controls' over government access to personal data in the EU, the US and elsewhere

In the aftermath of the Snowden revelations, the US Congress and Administration enacted significant steps to limit the ability of national security and law enforcement agencies to access personal data held by companies. While national security remains the purview of the member states, the European Parliament could, with the help of the European Union Agency for Fundamental Rights, assess how these steps compare with current and proposed practice in member states and other key countries.

Recommendation 8: Monitor the implementation of new digital legislation and its impact on transatlantic relations

Legislation stemming from the Digital Single Market, as well as implementation of Privacy Shield, the Umbrella Agreement, the General Data Protection Regulation, the Data Protection Directive for Law Enforcement and the PNR Directive, will all affect transatlantic relations as well as the EU's broader foreign policy. These dynamics will be overseen by the relevant committees concerned, but it will be important as well to monitor their overall cumulative impact on the transatlantic relationship from a holistic approach.

Recommendations for the European Commission

Recommendation 9: Upgrade the EU-US Information Society Dialogue and ensure coherence between policies adopted within the Commission and the US Administration

The Juncker Commission's primary goal of generating growth and jobs in the EU will depend to large extent on the EU's ability to harness the digital technologies of the future – the focus of the Digital Single Market. But the success of that effort itself will depend on building a Transatlantic Digital Marketplace – one that in many ways already exists, but which is sometimes buffeted by counter-vailing winds from other policy measures, whether from the US or from within the EU. A political level, multi-sectoral dialogue, along the lines of the EU-US Energy Council, between the Commission and the Administration should be able to identify opportunities as well as challenges, to build synergies and to mitigate some of these cross-currents.

Recommendation 10: Use this Dialogue and other established transatlantic channels to address and ensure coherence in the key digital law enforcement issues – general oversight, mutual legal assistance, and encryption and cybersecurity.

These issues were discussed at length in Chapter 4, but the critical issue here is that while they are largely in the domain of DG Justice and DG Home, decisions made in the law enforcement domain have implications that extend well beyond the remit of law enforcement and citizens' rights issues. These must be coordinated and balanced internally, and in tandem with appropriate US counterparts.

Recommendation 11: Develop a cross-sectoral approach and a common vision for the digitalisation of the industry in Europe

Most experts, policymakers and business recognize that the next step in digital transformation will affect non-digital industries. For that matter, the greatest potential of growth in digitalisation may very well be in traditional industries. While some cross-sectoral initiatives exist, often in the form of public-private partnerships, the European Commission should develop a clear vision on the digitalisation of European industries, and should extend this view beyond the current horizon of 2020. The Industrial Renaissance of the EU will likely not be complete without a dimension taking into account digital transformation.

Notwithstanding the economic opportunities that such innovations would bring, they will raise a number of new questions with regard to digital rights, including the exchange of personal data from machine to machine without any humans viewing that data. They will also raise concerns when it comes to the potentially disruptive effect of digitalisation on the jobs market in Europe – a discussion the European Commission should anticipate.

Recommendations for the Council and for member states

Recommendation 12: Swiftly transpose EU legislation on the digital economy and data privacy

Whether it is the PNR Directive, the GDPR or the NIS Directive, initiatives launched years ago have been heavily delayed through the legislative process. Their implementation in member states should also be prioritized as the EU moves forward in creating the DSM.

Recommendation 13: Pro-actively work with the Commission on transatlantic digital law enforcement issues

While the EU Treaties retain important differences in the roles of the Commission, the Council and the member states on law enforcement issues, all of them need to work together to protect EU citizens' security in the years ahead. Success here will require close collaboration with the US and its law enforcement and national security agencies. While such collaboration can and should continue at the member state level, it also needs to be fully informed and coordinated by all concerned in Brussels.

Recommendation 14: Better engage EU citizens on transatlantic trust in digital issues

One of the biggest obstacles to digital transformation in Europe remains the lack of trust between citizens and governments, and in particular towards the US government. In addition, fears of US digital dominance of Europe tend to veer towards protectionism. This is due in part to the lack of engagement

from national governments to adequately inform their citizens on the actual state of the transatlantic relationship on these issues. Member states could therefore reach out more often and better to the general public to inform and reassure citizens on the consequences of digital transformation. For instance, a first step could be to reframe the debate on what the '*Uberisation*' of economies and societies really means – and if it is actually the right notion to use for ongoing disruptions.

Recommendations for the European External Action Service

Recommendation 15: Strengthen the EU- US Cyber Dialogue

In addition to supporting a strengthened political-level Transatlantic Digital Dialogue (Recommendations 4 and 9), the EEAS should work with relevant bodies in the Commission to strengthen the EU - US Cyber Dialogue. This could help Europe and US develop a better narrative on issues governing law enforcement, national security and critical infrastructure protection. While immediate policy priorities might differ, and while principled assumptions might persist, setting a common vision of the future of these issues on both sides of the Atlantic is essential.

Recommendation 16: Include internet freedom and access to digital content and technologies as part of external policies toward developing and emerging countries

As part of its new global strategy, the European Union should include internet freedom, access to digital content and digital technologies as core elements of its external action. The right to have access to the internet, and connectivity through digital technologies, will be key indicators of development in the next phase of globalization. In addition, the rights associated with access to the internet – such as the right to assemble or to free speech – are limited in a number of countries. What the EU stands for offline, it should stand for online. Further, these technologies can be broadly used in virtually every aspect of development policy. An active digital external policy could provide the EEAS with new tools for accomplishing its external policy goals.

7 Conclusion

Transatlantic relations regarding the digital economy and data privacy are currently both hopeful and contentious, reflecting the great opportunities and challenges offered by the digital transformation of transatlantic societies and economies. Ongoing debates about access to personal data, extraterritoriality of law enforcement, standards in digital technologies, norms for cybersecurity, and the future of global internet governance will establish a transatlantic approach to digitalisation. It may also see the rise of a true transatlantic digital marketplace. Finding an appropriate equilibrium between privacy, security and the economy should be a priority for the EU and the US. But this will not go without tensions as policymakers are faced with varying threats, perceptions and opportunities.

As transatlantic partners undergo this digital transformation, they should be mindful of the global implications of the choices they make. Greater cooperation between the EU and the US on digital issues will have a significant effect on other countries. The EU's external relations may be affected by this to a much greater extent than currently assumed. If transatlantic partners seek to set global standards and templates for digital globalisation then this will surely raise eyebrows in many capitals. Thus, the transatlantic partners could set the standards for the global and digitalised economy of the future, but they will need to work together to address opposition from other countries who perceive differently the challenges and opportunities linked with greater openness and connectivity.

8 List of Acronyms

ACLU	American Civil Liberties Union
ACTA	Anti-Counterfeit Trade Agreement
B2B	Business-to-Business
B2C	Business-to-Consumer
BND	German Federal Intelligence Service
ECHR	European Convention on Human Rights
ECJ	European Court of Justice
EEAS	European External Action Service
EU	European Union
CALEA	Communications Assistance for Law Enforcement Act
CEO	Chief Executive Officer
CISA	Cybersecurity Information Sharing Act
CNAP	Cybersecurity National Action Plan
DG	Directorate General
DPA	Data Protection Authorities
DSM	Digital Single Market
ECPA	Electronic Communications Privacy Act
EEAS	European External Action Service
ENCRYPT	Ensuring National Constitutional Rights for Your Private Telecommunications Act
EPSC	European Political Strategy Center
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FDI	Foreign Direct Investment
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FTA	Free Trade Agreement
FTC	Federal Trade Commission
GATS	WTO's General Agreement on Trade in Services
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communications Technology

IoT	Internet of Things
ISP	Internet Service Provider
ITA	WTO's Information and Technology Agreement
ITU	International Telecommunication Union
LEADS	Law Enforcement Access to Data Stored Abroad Act
MLAT	Mutual Legal Assistant Treaty
NGO	Non-Governmental Organization
NIS	Networks Information and Security
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development
PCLOB	Privacy and Civil Liberties Oversight Board
PNR	Passenger Name Records
PRISM	NSA's Personal Record Information System Methodology
RFID	Radio-Frequency Identification Device
SME	Small and Medium-Sized Enterprises
SOPA	Stop On-Line Piracy Act
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TBps	Terabytes per Second
TFTP	Terrorism Financing Tracking Program
TiSA	Trade in Services Agreement
TPP	Trans-Pacific Partnership
TTIP	Transatlantic Trade and Investment Partnership
UNESCO	United Nations Educational, Scientific and Cultural Organization
US	United States
USITC	US International Trade Commission
USTR	United States Trade Representative
VAT	Value-added tax
WTO	World Trade Organisation

Bibliography

Boehm Franziska, 'A Comparison between US and EU Data Protection Legislation for Law Enforcement Purposes,' European Parliament, Directorate for Internal Policies, Policy Department C: Citizens' rights and Constitutional Affairs, study commissioned at the request of the LIBE Committee, September 2015, http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf

Bourgeois Jacques, Kerry Cameron F., Long William, Meulenbelt Maarten, Raul Alan Charles, 'Essentially Equivalent: A Comparison of the Legal Orders for Privacy and Data Protection in the United States and the European Union,' Sidley Austin LLP, January 25, 2016, http://www.sidley.com/publications/essentially-equivalent

Bildt Carl, Kennard William, 'Building a Transatlantic Digital Marketplace: Twenty Steps to 2020,' Atlantic Council, April 2016, http://www.atlanticcouncil.org/images/publications/Building_a_Transatlantic_Digital_Marketplace_web_0406.pdf

Bradford Jensen J., Kletzer Lori G. 'Tradable Services: Understanding the Scope and Impact of Services Outsourcing,' Peterson Institute for International Economics Working Paper 5-9, September 2005, https://piie.com/publications/wp/wp05-9.pdf

Brynjolfsson Erik, McAfee Andrew, Spence Michael, 'New World Order,' Foreign Affairs, Volume 93 No 4, July/August 2014, https://www.foreignaffairs.com/articles/united-states/2014-06-04/new-world-order

Carswell Simon, 'Microsoft warns of risks to Irish operation in US search warrant case,' *The Irish Times*, February 25, 2016, http://www.irishtimes.com/business/microsoft-warns-of-risks-to-irish-operation-in-us-search-warrant-case-1.2548718

Chase Peter, Pelkmans Jacques, 'This Time It's Different: Turbo-charging Regulatory Cooperation in TTIP', Centre for European Policy Studies, Paper No 7 in the CEPS-CTR project 'TTIP in the Balance' and CEPS Special Report No 110, June 4, 2015, https://www.ceps.eu/publications/time-it%E2%80%99s-different-turbo-charging-regulatory-cooperation-ttip

Cisco, 'Visual Networking Index (VNI): Forecast and Methodology2014-2019 White Paper', May 2015, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html

Cisco, 'The Zettabyte Era - Trends and Analysis,' June 23, 2015, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html?referring_site=RE&pos=2&page=http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vn

Connolly Kate, 'German secret service BND reduces cooperation with NSA,' *The Guardian*, May 7, 2015, http://www.theguardian.com/world/2015/may/07/german-secret-service-bnd-restricts-cooperation-nsa-us-online-surveillance-spy

Cook Tim, 'A Message to Our Customers,' Apple, February 16, 2016, http://www.apple.com/customer-letter/

Davies Ron., Briefing: The Internet of Things: Opportunities and Challenges', European Parliament Research Service, May 2015, http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf

DIGITALEUROPE, 'Assessment of the Trans-Pacific Partnership Provisions - Our recommendations for the Transatlantic Trade and Investment Partnership (TTIP) and the Trade in Services Agreement (TiSA),' January 2016, http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&entryID=1090&PortalId=0&TabId=353

DIGITALEUROPE, Information Technology Industry Council, 'ICT Industry Recommendations for Regulatory Cooperation in the Transatlantic Trade and Investment Partnership', February 2, 2015, http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&entryID=901&PortalId=0&TabId=353

Eurojust, 'Agreement between Eurojust and the United States of America,' November 6, 2006, http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/agreements/Agreement%20Eurojust-USA%20(2006)/Eurojust-USA-2006-11-06-EN.pdf

European Commission, 'Agreement between the United States and the European Union on the Protection of Personal Information relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses,' September 8, 2015, http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf

European Commission, 'Agreement on extradition between the European Union and the United States of America,' June 25, 2003, http://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?step=0&redirect=true&treatyId=5461

European Commission, Article 29 Data Protection Working Party, 'Opinion 01/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision,' 16/EN, WP 238, April 13, 2016, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

European Commission, 'Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries,' http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

European Commission, 'COMMISSION IMPLEMENTING DECISION pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield,' http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf

European Commission, 'Commission welcomes agreement to make EU online environment more secure,' December 8, 2015, http://europa.eu/rapid/press-release_IP-15-6270_en.htm

European Commission, 'Countries and regions - United States', http://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states/

European Commission, 'EU-U.S. Joint Statement on Trade Principles for Information and Communications Technologies Services,' preamble, April 4, 2011, http://trade.ec.europa.eu/doclib/docs/2011/april/tradoc_147780.pdf

European Commission, 'EU-U.S. Mutual Legal Assistance Agreement,' June 6, 2003, http://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?redirect=true&treatyId=5441

European Commission, 'Final Report of the High Level Working Group on Jobs and Growth', February 11, 2013, http://trade.ec.europa.eu/doclib/docs/2013/february/tradoc_150519.pdf

European Commission, 'Joint Statement for the 2015 (13th) EU-U.S. Information Society Dialogue', April 14, 2015, https://ec.europa.eu/digital-single-market/en/news/joint-statement-2015-eu-us-information-society-dialogue

European Commission, 'List of companies for which the EU BCR cooperation procedure is closed,' http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm

European Commission, 'Regulation 2016/679 of the European Parliament and of the Council of 27 April, 2016, on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)' April 27, 2016, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

European Commission, 'Report for the 13th Round of Negotiations for the Transatlantic Trade and Investment Partnership,' New York, 25-29 April 2016, http://trade.ec.europa.eu/doclib/docs/2016/may/tradoc_154581.pdf

European Commission, Statements by Ignacio Garcia-Bercero, 'EC technical briefing on-the-record on the 13th TTIP negotiations round debriefing,' May 2, 2016, http://ec.europa.eu/avservices/video/player.cfm?sitelang=en&ref=I120640

European Commission, 'Statement by President Barroso on the EU-US trade agreement with U.S. President Barack Obama, the President of the European Council Herman Van Rompuy and UK Prime Minister David Cameron,' June 17, 2013, http://europa.eu/rapid/press-release_SPEECH-13-544_en.htm

European Commission, 'Statement of the Article 29 Working Party,' October 16, 2015, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

European Commission, 'Trade for All -- Toward a More Responsible Trade and Investment Policy,' October 2015, http://trade.ec.europa.eu/doclib/docs/2015/october/tradoc_153846.pdf

European Council, 'Council Adopts new EU-US Agreement on Passenger Name Records (PNR),' 9186/12, PRESSE 173, April 26, 2012, http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/129806.pdf

European Council, 'Directives for the negotiation on the Transatlantic Trade and Investment Partnership between the European Union and the United States of America,' Approved by the Foreign Affairs Council (Trade) on June 14, October 9, 2014, http://data.consilium.europa.eu/doc/document/ST-11103-2013-DCL-1/en/pdf

European Court of Human Rights, 'Arbitrary and Abusive Secret Surveillance of Mobile Telephone Communications in Russia,' Roman Zakharov v Russia (47143/06), December 4, 2015, http://hudoc.echr.coe.int/eng?i=001-159324#{itemid:[001-159324]}

European Parliament, 'EU Passenger Name Record (PNR) proposal: an overview,' December 14, 2015, http://www.europarl.europa.eu/news/en/news-room/20150123BKG12902/EU-Passenger-Name-Record-(PNR)-proposal-an-overview

European Parliament, 'European Parliament Resolution of 26 May 2016 on Transatlantic Data Flows,' May 26 2016. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0233+0+DOC+XML+V0//EN&language=EN

European Parliament, 'First-ever EU-wide cyber-security rules backed by Internal Market Committee,' January 14, 2016, http://www.europarl.europa.eu/news/en/news-room/20160114IPR09801/First-ever-EU-wide-cyber-security-rules-backed-by-Internal-Market-Committee

European Parliament, 'Report on Towards a Digital Single Market Act (2015/2147(INI))', A8-0371/2015, December 12, 2015, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2015-0371+0+DOC+PDF+V0//EN

European Political Strategy Center, 'Strategic Note - The Integration of Products and Services - Taking the Single Market into the 21st Century,' Issue 7, October 6, 2015, http://ec.europa.eu/epsc/pdf/publications/strategic_note_issue_7.pdf

European Union Agency for Fundamental Rights, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU,' November 18, 2015, http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services

Europol, External Relations, Operational Agreements with Non-EU States,' https://www.europol.europa.eu/content/page/external-cooperation-31

EUR-Lex,'2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.),' July 26, 2000, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000D0520&from=en

EUR-Lex, 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.' October 24, 1995, http://eur-lex.europa.eu/legal content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=EN

Government of the United Kingdom, 'Chancellor's speech to GCHQ on cyber security,' November 17, 2015, https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

Hamilton Daniel S., Quinlan Joseph P., *Sleeping Giant: Awakening the Transatlantic Services Economy*, Washington, D.C.: Center for Transatlantic Relations, Paul H. Nitze School of Advanced International Studies, Johns Hopkins University, November 2007.

Hert Paul, Papakonstantinou Vagelis, 'The Data Protection Regime in China,' European Parliament, Directorate for Internal Policies, Policy Department C: Citizens' rights and Constitutional Affairs, study commissioned at the request of the LIBE Committee, October 2015, http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf

Hofheinz Paul, Mandel Michael, Uncovering the Hidden Value of Digital Trade: toward a 21st Century Agenda for Transatlantic Prosperity, Lisbon Council and Progressive Policy Institute Joint Paper, July 2015, http://www.lisboncouncil.net/publication/publication/127-uncovering-the-hidden-value-of-digital-trade-towards-a-21st-century-agenda-of-transatlantic-prosperity.html

InfoCuria, 'Judgement of the Court (Grand Chamber), Case C-362/14, in re Maximillian Schrems v. Data Protection Commissioner,' October 6, 2015, http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EN

International Telecommunication Union, United Nations Educational, Scientific and Cultural Organization, 'The State of Broadband 2015: Broadband as a Foundation for Sustainable Development,'

Switzerland, Geneva, September 2015, http://www.broadbandcommission.org/Documents/reports/bb-annualreport2015.pdf

Italian Ministry of Economic Development, 'Joint Declaration by G-7 ICT Ministers', April 2016, http://www.mise.gov.it/images/stories/documenti/02_The_Declaration.pdf

Joseph S. Nye, Jr. 'The Regime Complex for Managing Global Cyber Activities' Global Commission on Internet Governance' Paper Series No. *1*, May 2014, https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities

MacDonnell Paul, Castro Daniel, 'Europe Should Embrace the Data Revolution,' Center for Data Innovation, February 29, 2016, http://www2.datainnovation.org/2016-europe-embrace-data-revolution.pdf

Manyika James, Lund Susan, Bughin Jacques, Woetzel Jonathan, Stamenov Kalin, Dhingra Dhruv, 'Digital Globalization: The New Era of Global Flows,' McKinsey & Company, March 2016, http://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows

Maxim Rob, Aaronson Ariel Susan, 'Trade and the Internet: The Challenge of the NSA Revelations Policies in the US, EU, and Canada,' Elliot School of International Affairs, The Georgetown University, Institute for International Economic Policy, MacArhtur Foundation, https://www.gwu.edu/~iiep/assets/docs/papers/Aaronson_Maxim_Trade_Internet.pdf

Meltzer Joshua P., 'The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment,' Brookings Institution, Global Economy and Development Center, Working Paper 79, October 2014, http://www.brookings.edu/~/media/research/files/papers/2014/10/internet-transatlantic-data-flows-meltzer/internet-transatlantic-data-flows-version-2.pdf

Microsoft, Brief of Amici Curiae Amazon.com, Box, Cisco Systems, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest, Pintrest, Slack, Snapchat, Whatsapp and Yahoo in support of Apple, Inc.' ED No CM 16-10 (SP), March 22, 2016, http://mscorpmedia.azureedge.net/mscorpmedia/2016/03/smith_post.pdf

Mortera-Martinez Camino, 'Big Data, Big Brother: How to Secure Europeans' Safety and Privacy,' Center for European Reform, Open Society Foundation, December 2015, http://www.cer.org.uk/sites/default/files/pb_CMM_bigbrother_4dec15.pdf

Nojeim Greg, 'MLAT Reform Proposal: Eliminating U.S. Probable Cause and Judicial Review,' Lawfare, December 4, 2015, https://www.lawfareblog.com/mlat-reform-proposal-eliminating-us-probable-cause-and-judicial-review

O'Reilly Michael, FCC Commissioner, 'Affirmatively Expand Permissible Foreign Ownership,' Federal Communications Commission, March 3, 2015, https://www.fcc.gov/news-events/blog/2015/03/03/affirmatively-expand-permissible-foreign-ownership

PostNord, 'E-Commerce in Europe, 2015,' September 2015, http://www.postnord.com/globalassets/global/english/document/publications/2015/en_e-commerce_in_europe_20150902.pdf

Power Leonie, 'Getting to Know the GDPR, Part 9 - Data Transfer Restrictions are Here to Stay, but so are BCR,' Field Fischer Privacy, Security and Information Blog, February 24, 2016, http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-gdpr-part-9-data-transfer-restrictions-are-here-to-stay-but-so-are-bcr/

Privacy and Civil Liberties Oversight Board, 'Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act,' July 2, 2014, https://www.pclob.gov/library/702-Report.pdf

Privacy and Civil Liberties Oversight Board, 'Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court,' January 23, 2014, https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf

Public Citizen, 'Only One of 44 Attempts to Use the GATT Article XX/GATS Article XIV 'General Exception' has Ever Succeeded: Replicating the WTO Exception Construct will not Provide for an Effective TPP General Exception', August 2015, https://www.citizen.org/documents/general-exception.pdf

Renda Andrea, Yoo Christopher, 'Telecommunications and Internet Services: The Digital Side of TTIP', Centre for European Policy Studies and the Center for Transatlantic Relations, the Paul Nitze School of Advanced International Studies, Johns Hopkins University, Paper No 8 in the CEPS-CTR Project 'TTIP in the Balance' and CEPS Special Report No 112, July 2015, https://www.ceps.eu/publications/telecommunications-and-internet-services-digital-side-ttip

Richards Neil, 'Apple's 'Code = Speech' Mistake,' MIT Technology Review, March 1, 2016, https://www.technologyreview.com/s/600916/apples-code-speech-mistake/

Scott Ben, 'Transatlantic Digital Dialogue: Rebuilding Trust through Cooperative Reform,' The German Marshall Fund of the United States, Stiftung fuer Neue Verantwortung, November 5, 2015, http://www.gmfus.org/publications/transatlantic-digital-dialogue-rebuilding-trust-through-cooperative-reform

Scott Mark, 'American Tech Giants Face Fight in Europe Over Encrypted Data,' *New Yok Times*, March 27, 2016, http://www.nytimes.com/2016/03/28/technology/american-tech-giants-face-fight-in-europe-over-encrypted-data.html?_r=0

Soroka Natalie, 'U.S. Trading Companies, 2012,' US Department of Commerce, November 2014, http://www.trade.gov/mas/ian/build/groups/public/@tg_ian/documents/webcontent/tg_ian_004048.pdf

Kommerskollegium (Swedish National Board of Foreign trade), 'E-Commerce: New Opportunities, New Barriers: A Survey of E-Commerce Barriers in countries outside the EU,' November 2012, https://www.wto.org/english/tratop_e/serv_e/wkshop_june13_e/ecom_national_board_e.pdf

Swire Peter, 'U.S. Surveillance Law, Safe Harbor and Reforms since 2013,' December 17, 2015, https://fpf.org/wp-content/uploads/2015/12/White-Paper-Swire-US-EU-Surveillance.pdf

The European Consumer Organization, Data Flows in TTIP Fact Sheet, http://www.beuc.eu/publications/beuc-x-2015-073_factsheet_data_flows_in_ttip.pdf

The European Consumer Organization (BEUC), Position Statement: Consumers at the Heart of the Transatlantic Trade and Investment Partnership, updated as of May 21, 2014, http://www.beuc.eu/publications/beuc-x-2014-031_mgo_ttip_updated.pdf

The Wall Street Journal, 'EU Commission Rejects U.S. Plan on Encryption,' October 8, 1997, http://www.wsj.com/articles/SB876322992856833000

Transatlantic Consumer Dialogue, Resolution: The Consumer Perspective on Addressing the E-Commerce within the Transatlantic Trade and Investment Partnership, October 2013,

http://www.consumersinternational.org/media/1402110/tacd-infosoc-resolution-on-e-commerce-in-the-transatlantic-trade-and-investment-partnership.pdf

U.S. Congress, 'H.R.1174 - Law Enforcement Access to Data Stored Abroad Act,' February 27, 2015, https://www.congress.gov/bill/114th-congress/house-bill/1174

US Congress, 'H.R.699 - Email Privacy Act,' April 2, 2015, https://www.congress.gov/bill/114th-congress/house-bill/699

US International Trade Commission, 'Digital Trade in the U.S. and Global Economies, Part 1,' Investigation number 332-531, USITC Publication 4415, July 2013, https://www.usitc.gov/publications/332/pub4415.pdf

US International Trade Commission, 'Digital Trade in the U.S. and Global Economies, Part 2,' Publication Number: 4485 Investigation Number: 332-540, August 2014, https://www.usitc.gov/publications/332/pub4485.pdf

US Trade Representative, 'Letter from Ambassador Demetrios Marantis, Acting U.S. Trade Representative, to Congress,' March 20, 2013, https://ustr.gov/sites/default/files/03202013%20TTIP%20Notification%20Letter.PDF

US Trade Representative, 'Trans-Pacific Partnership Agreement, Chapter 29, Exceptions and General Provisions' https://ustr.gov/sites/default/files/TPP-Final-Text-Exceptions-and-General-Provisions.pdf

Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein (Independent Centre for Privacy Protection Schleswig-Holstein), 'Positionspapier des ULD zum Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2015, C-362/14,' October 14, 2015, https://www.datenschutzzentrum.de/uploads/internationales/20151014_ULD-Positionspapier-zum-EuGH-Urteil.pdf

Valero Jorge, 'Ansip: 'I am strongly against any backdoor to encrypted systems'', EurActiv, February 23, 2016. https://www.euractiv.com/section/digital/interview/ansip-i-am-strongly-against-any-backdoor-to-encrypted-systems/

White House, 'Liberty and Security in a Changing World - Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies,' December 12, 2013, https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

White House, 'Presidential Policy Directive/PPD-28,' January 17, 2014. https://www.whitehouse.gov/sites/default/files/docs/2014sigint_mem_ppd_rel.pdf

White House, 'Remarks by President Obama at the Hannover Messe Trade Show Opening,' April 24, 2016,' https://www.whitehouse.gov/the-press-office/2016/04/24/remarks-president-obama-hannover-messe-trade-show-opening

World Trade Organization, 'Information and Technology Agreement -- An Explanation,' https://www.wto.org/english/tratop_e/inftec_e/itaintro_e.htm

World Trade Organization, 'Uruguay Round Agreement - General Agreement on Trade in Services,' https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm

CATALOGUE QA-01-16-195-EN-C (paper)
CATALOGUE QA-01-16-195-EN-N (pdf)

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES

POLICY DEPARTMENT

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas

Foreign Affairs

- Human Rights
- Security and Defence

Development

International Trade

Documents

Visit the European Parliament website:
http://www.europarl.europa.eu/supporting-analyses

PHOTO CREDIT: iStock International Inc.

ISBN 978-92-823-9848-7 (paper)
ISBN 978-92-823-8660-6 (pdf)
doi:10.2861/771804 (paper)
doi:10.2861/173823 (pdf)

Publications Office