Subcommittee on Commerce, Manufacturing, and Trade and Subcommittee on Communications and Technology, United States House of Representatives

Hearing on "Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows"

November 3, 2015

Dr. Joshua P. Meltzer
Senior Fellow in the Global Economy and Development program at the Brookings Institution
Adjunct Professor at the Johns Hopkins University School for Advanced International Studies

Introduction

Chairman Burgess, Chairman Walden, Ranking Member Schakowsky and Ranking Member Eshoo, honorable members of both Committees, thank you for this opportunity to share my views with you on the EU Safe Harbor Decision and the impacts for transatlantic data flows.

Summary

- The U.S.-EU economic relationship is the largest in the world, consisting of trade flows valued at over $1 trillion annually and stocks of investment in each economy close to $4 trillion.
- High levels of Internet penetration, trade and investment underpins and is also enabled by data flows between the U.S. and the EU. For instance, in 2012 U.S. exports to the EU of up to $140 billion in value were delivered online.
- Data flows between the U.S. and the EU have led to a large variety of business models, forms of international trade and investment. Businesses in the U.S. use the Internet and data flows to innovate, engage in R&D with European counterparts and to connect to global supply chains. Access to the cloud requires data to move across borders. U.S. businesses also transfer data amongst subsidiaries located across the EU.

- Small and medium-sized enterprises are taking advantage of the Internet and the ability to move data between the U.S. and the EU to engage in international trade. They are using Internet platforms such as eBay to reach consumers and to export.
- The most significant potential barrier to transatlantic data flows is the EU Privacy Directive, which prevents the transfer of personal data outside of the EU to countries that do not have an adequate level of privacy protection—interpreted in the EU as meaning privacy protection that is essentially equivalent to the EU approach.
- Since 2000, the U.S.-EU Safe Harbor Framework has legalized the transfer of personal data from the EU to the U.S., despite differences in the U.S. and EU approaches to protecting personal information.
- The decision of the European Court (ECJ) of Justice in *Schrems* invalidates the European Commission's finding under the Safe Harbor Framework that U.S. privacy protection is adequate.
- Failure to update the Safe Harbor Framework and to respond fully to the concerns of the ECJ about how EU personal data is protected in the U.S. could lead to prohibitions on transferring personal data to the U.S. The impact of such an outcome on transatlantic trade and investment would be significant.

The transatlantic trade and investment relationship

U.S.-EU trade and investment

The U.S. and the EU economies represent over 50 percent of global GDP, 25 percent of global exports and over 30 percent of global imports. The U.S.-EU economic relationship is the most significant in the world. In 2014, total goods trade with the EU was worth approximately $700 billion. In 2014, U.S. exports of services to the EU were worth over $219 billion and imports were approximately $169 billion; leading to total transatlantic trade in 2014 of $1.09 trillion. This compares with total trade with Canada and China of $741 billion and $646 billion respectively.

The transatlantic investment relationship is also the world's largest. The majority of U.S. foreign direct investment is in Europe and this is also true of European investment in the U.S. The total stock of investment that the U.S. and Europe have invested in each other is worth around $4 trillion.

United States and European investment in each other's markets are important drivers of transatlantic trade. Sixty-one percent of U.S. imports from the EU and 33 percent of EU imports from the U.S. consist of intra firm trade, making the sale of goods and services through foreign affiliates in each country key drivers of transatlantic trade. This compares with intra firm trade as a share of U.S. imports from the Pacific Rim (37.2 percent), and South/Central America (37 percent).[i]

The size of transatlantic data flows

The ability to access, accumulate and transfer data across borders is a function of the globalization of the Internet. Data flows between the U.S. and the EU are the largest globally; approximately 55 percent larger than data flows between the U.S. and Asia and 40 percent larger than data flows between the U.S. and Latin America.[ii]

The size of transatlantic data flows reflects Internet penetration in the U.S. and the EU—which is around 85 percent in the U.S. and 90 percent in the EU—and the importance of data as underpinning and often enabling the bilateral economic relationship.

The importance of cross-border data flows for U.S. and EU trade and investment

There are multiple ways that the free flow of data between the U.S. and Europe generates international trade and investment:[iii]

- When a business in Europe uses the Internet to reach customers in the U.S. to sell products online. Internet commerce in the U.S. grew from $13.63 billion in 2011 to $42.13 billion in 2013 and is expected to reach $133 billion in sales by 2018.[iv] As online marketplaces in the U.S. and the EU mature, consumers will increasingly use the Internet to purchase goods and services from each other's markets, thereby growing transatlantic trade.
- Transatlantic data flows underpin business to business transactions, such as when a U.S. business receives financial advice from Barclays in London. This is a financial service that is delivered online and is itself a trade in services. In addition, using the Internet to access such cutting-edge business services can increase the productivity and competitiveness of

businesses, strengthening their ability to compete in overseas markets, further stimulating international trade. According to an OECD study, a 1 percent increase in the importation of business services is associated with a 0.3 percent higher export share.[v]

- Internet access and the free flow of data supports global value chains. This includes so-called trade in tasks[vi]—the ability of geographically diverse businesses to contribute a task or service as part of supply chains that span the Atlantic.
- The free flow of data between the U.S. and Europe is needed for intra-company purposes and is thereby an important enabler of transatlantic investment. For instance, GE in Atlanta relies on the free flow of data to manage production schedules, HR data and communicate internally with its subsidiaries throughout Europe.
- Investment in data centers that provide access to the cloud in the U.S. and Europe relies on cross-border data flows. For instance, Amazon's data centers in Ireland require regular communication with its U.S.-based data centers to update or duplicate data for security purposes. Cross-border data flows are also necessary to reduce latency, such as when Google caches data on servers located closer to EU residents.
- Internet access and the free flow of data provides businesses and entrepreneurs with information on new markets, opportunities for collaboration and research that can support economic activity and lead to international trade between the U.S. and the EU and globally.

Transatlantic data flows also create opportunities for the U.S. and the EU to expand trade and investment with the developing world. As Internet access expands globally, much of the developing world will access the Internet on mobile devices. And by 2018, 54 percent of these devices will be "smart," up from 21 percent in 2013.[vii] Combining these trends with a growing

middle class in Asia in particular–which is expected to double by 2020 – highlights the potential growth of online international commerce. In fact, globally, people who have made at least one online purchase increased from 38 percent in 2011 to 40.4 percent in 2013, and by 2017 over 45 percent of the world are expected to be engaging in online commerce.[viii] The free flow of data globally will be required to ensure these opportunities are full realized.

The Internet is helping SMEs engage in international trade

Small and medium-sized enterprises (SMEs) are key drivers of U.S. growth and employment. SMEs are the main drivers of job growth in the U.S., accounting for 63 percent of net new private sector jobs since 2002.[ix] Over 80 percent of SME job growth is in the services sector.

Yet, SMEs are underrepresented in international trade. The top 1 percent of large firms in the U.S. account for 90 percent of U.S. trade, but only 15 percent of employment.

The global nature of the Internet is creating new opportunities for SMEs to engage in international trade.[x] For example, 95 percent of SMEs in the U.S. using eBay to sell goods and services export to customers in more than 4 continents—compared with less than 5 percent of U.S. business that export offline. And 74 percent of these SMEs are still exporting after 3 years, compared with 15 percent of offline exporters. [xi]

Calculating the value of digital trade

There is only limited data on the importance of the Internet and cross-border data flows for digital trade. One reason is that public trade data does not distinguish between whether goods and services are delivered offline or online. The impact of the Internet on digital trade is also a

function of the digitization of economies broadly, which has made separating out the impact of the Internet on trade (and GDP) a complex task.

Notwithstanding this limitation, some economic modelling has been done that seeks to quantify the relationship between Internet access, economic growth and trade. A World Bank study found that a 10 percent increase in broadband penetration resulted in a 1.38 percent increase in growth in developing countries and a 1.21 percent increase in growth in developed countries.[xii] In terms of the impact of the Internet on trade, one study concludes that a 10 percent increase in Internet access leads to a 0.2 percent increase in exports.[xiii] Other studies using more recent data find even stronger impacts of Internet use on trade.[xiv]

In terms of U.S.-EU trade and investment that is enabled by data flows, by focusing on services that could be delivered online, I calculated that in 2012, U.S. exports of such digitally deliverable services exports globally were $384 billion, and over $140 billion went to the EU.[xv] Services are also traded online through foreign affiliates in each other's markets. In 2011, U.S. foreign affiliates in Europe delivered $213 billion worth of digitally deliverable services and European businesses in the U.S. provided $215 billion worth of such services.[xvi]

The digitization of the U.S. and EU economies means that the Internet is also affecting trade through its impact on productivity, which in turn increases the competitiveness of these businesses domestically and globally.[xvii] For instance, use of the Internet to collect data and analyze it can improve firm productivity by making supply chains more efficient, improving distribution and transport schedules. Indeed, much of the strong productivity growth in the U.S. in the mid-1990s through to the mid-2000s has been attributed to strong investment in

Iinformation & Communications Technology.[xviii] A recent study of EU firms also found that engaging in e-commerce increases labor productivity—and that e-commerce had accounted for 17 percent of EU labor productivity growth between 2003 and 2010.[xix] A 2014 U.S. International Trade Commission (ITC) report found that the productivity gains from the Internet have increased U.S. real GDP by 3.4-3.5 percent.[xx]

The EU Privacy Directive

Privacy protection is not a new issue. In the 19th century Samuel Warren and Louis Brandeis, concerned about the potential for media to intrude on personal lives, wrote about a "right to be left alone."[xxi] Protecting privacy became increasingly important post-WWII as governments' increasing use of personal data combined with new computing power to process the data. This led to various government reviews of privacy protection and in 1980 the OECD produced *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*—reflecting an OECD consensus on how member countries should handle and protect personal data.[xxii]

Since these 1980 OECD guidelines, the rise of global Internet access and use has exponentially increased the amount of data that is being or can be combined and processed to create individual profiles. This data is also increasingly valuable and in some cases the value from the collection of this data is the basis on which "free" services such as email and social networking are provided. The global nature of the Internet also means that this data can be quickly and easily transferred to third parties in other jurisdictions. This has raised new challenges for how personal data is used, disclosed, monetized and protected. It has also brought to the fore the

need to find a way to achieve privacy protection while avoiding increasing barriers to cross-border data flows, which can undermine the Internet's economic and trade potential.

Governments are taking different approaches to regulating personal data collected by private enterprise.

The EU Data Protection Directive (DPD) adopted in 1995 governs personal data protection in the EU. As a "Directive," implementation of the DPD is left to EU member states. And in practice, member states vary widely in their enforcement of the DPD. The European Commission is seeking to update the DPD in the form of a Regulation.[xxiii]

The DPD defines personal data as "any information relating to an identified or identifiable natural person", and defines an identifiable person as "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more specific factors specific to his physical, physiological, mental, economic, cultural or social identity."[xxiv]

Under the DPD, anyone that processes personal data must comply with five principles. These principles require that personal data is:[xxv]

- Processed fairly and lawfully
- Collected for specific, explicit and legitimate purpose and not further processed in a way incompatible with those purposes
- Adequate, relevant and not excessive in relation to the purposes for which they are collected
- Accurate and where necessary, kept up-to-date

- Kept in a form that permits identification of the data subject for no longer than is necessary for the purpose for which the data were collected

The DPD allows for processing personal data only under specific circumstances. The main ones are where: the data subject has unambiguously given his/her consent; processing is necessary for the performance of a contract to which the data subject is a party, for compliance with a legal obligation to which the controller is subject, to protect the vital interests of the data subject, or it is in the public interest. Processing is also allowed for the purposes of the legitimate interests pursued by the controller, except where such interests are overridden by the fundamental rights and freedoms of the data subject.[xxvi]

For a category of personal data the DPD considers sensitive, such as on racial or ethnic origins, then processing is restricted to situations such as where there is explicit consent, for obligations in the field of employment, or to protect the vital interests of the data subject.

Transferring personal data from the EU to third countries

In the case where the processor is outside of the EU, the transfer of personal data from the EU can only take place under specific conditions.

Adequacy finding

An important mechanism for transferring personal data outside of the EU is for a country to receive a finding from the European Commission that the receiving country provides an adequate level of privacy protection.[xxvii]

So far, outside of Europe and British territories in Europe, only four countries (Argentina, Uruguay, Israel, New Zealand) have been recognized as providing adequate levels of data protection, and Canada and Australia have been recognized as adequate for the purposes of transferring passenger name records. While in determining adequacy the DPD allows for consideration of alternatives to top-down legislated approaches to privacy regulation such as industry self-regulation, all of these countries were found to have adequate privacy protection based on specific economy-wide laws. For instance, Argentina was assessed as providing an adequate level of data protection based on its constitution and other legislation.[xxviii] This was also true for Uruguay.

Model Contracts and Binding Corporate Rules

The DPD also allows for cross-border transfers pursuant to a contract that guarantees the same protection of the personal data as under the DPD. A global conglomerate can transfer data amongst its units where it has implemented binding corporate rules (BCRs) that also ensure data protection consistent with the DPD.

BCRs and contracts are not used much due to the time and expense of getting them approved. Contracts have also been unwieldy for multinational companies, as they must be designed to deal with all possible data transfers, and therefore are unable to respond to issues that might arise without being amended.

In many cases the controller will not have a contract with a data subject. For instance, collecting and processing personal data from Internet use (i.e., "monitoring"), would not create a contractual relationship.

Even where a contract existed, the data transfer must be "necessary" for the performance of the contract. This would include transferring financial and personal information to complete an online transaction but would not include other data incidental to the transaction.

Derogations under the DPD

Personal data can also be transferred to a third country under so-called derogations, the main ones being consent of the data subject, when the transfer is necessary for the performance of a contract between the data subject and the controller, or it is necessary on important public interest grounds.[xxix]

Under the DPD, in order for consent to be effective to authorize cross-border data transfers it must be "specific and informed." This means that merely using an online service that leads to the collection of personal data will not constitute consent. Instead, action such as ticking a box may be required.

The ability to transfer data outside the EU pursuant to a legitimate interest is heavily circumscribed. First, the data must not be frequent or massive so this derogation could not be used to justify an online business that relies on regular data collection. Where businesses seek to use this derogation for more limited data transfers they have to demonstrate that they have put in place appropriate safeguards to protect the data, document the assessment and the appropriate safeguards, and inform the EU supervisory authority of the transfer of data.

The U.S.-EU Safe Harbor framework

The U.S.-EU Safe Harbor framework was developed to respond to a 1999 Opinion from the Article 29 Working Party[xxx] that U.S. privacy protection did not providing adequate protection in all cases for personal data transferred from the EU.[xxxi]

On 26 July 2000, the European Commission recognized the Safe Harbor Privacy Principles and Frequently Asked Questions issued by the Department of Commerce as providing adequate protection for the purposes of personal data transfers from the EU.[xxxii] This Decision allows for the transfer of personal information from the EU to companies in the U.S. that have signed up to the Safe Harbor principles.

The Safe Harbor framework consists of seven principles that largely reflect the key elements of the EU Data Protection Directive. The mains ones are commitments to: give European data subjects notice that a U.S. entity is processing their data; to limit onward transfers of data to countries that also subscribe to the Safe Harbor principles or are the subject of an adequacy finding; to take reasonable steps to protect personal data from loss or misuse; to process

personal data only for the purposes for which the organization intends to use it; to give European data subjects access to their personal information and the ability to correct, amend or delete inaccurate information; and a commitment to enforce the principles and give European data subjects access to affordable enforcement mechanisms.

Under the Safe Harbor framework, U.S. organizations can either join a self-regulatory privacy program that adheres to the Safe Harbor principles or self-certify (most common) to the Department of Commerce that they are complying with these principles. Additionally, U.S. companies must identify in their publically available privacy policy that they adhere to and comply with the Safe Harbor principles. Approximately 4,500 companies are certified under the Safe Harbor framework.

The Safe Harbor framework covers Internet companies and industries including information and computers services, pharmaceuticals, tourism, health and credit card services. Financial services and telecommunications are not subject to Federal Trade Commission Article 5 oversight (see below) and are therefore outside the scope of the Safe Harbor framework. Most of the companies use Safe Harbor to export services to the EU. Subsidiaries of EU firms located in the U.S., such as Nokia and Bayer, also use Safe Harbor to transfer data from the EU.[xxxiii]

Safe Harbor oversight and enforcement

Under the Safe Harbor framework the U.S. Department of Commerce reviews every Safe Harbor self-certification and annual recertification submission it receives from companies. The Department of Commerce also maintains a list of companies on its website that comply with the Safe Harbor Principles.

The FTC enforces the Safe Harbor framework against those companies that self-certify as being in compliance. The FTC can enforce breaches of the Safe Harbor agreement under Article 5 of the Federal Trade Commission Act preventing unfair or deceptive acts. According to the FTC, misrepresenting why information is being collected from consumers or how the information will be used constitutes a deceptive practice. Moreover, under Safe Harbor companies need to certify that they will collect data in accordance with the Safe Harbor principles and the FTC considers that failure to do this would be a misrepresentation and a deceptive practice.

The FTC acts on referrals from EU data protection authorities, third party private dispute resolution providers and on its own.

Safe Harbor framework negotiations

Since 2014 the U.S. and the EU have been renegotiating the Safe Harbor framework. These negotiations started following the Edward Snowden leaks and revelations about NSA bulk surveillance and use of data collected by private U.S. companies that were certified under the Safe Harbor framework. As a result, much of the focus of the European Commission has been addressing the loss of confidence within the EU of the privacy of personal data transferred to the U.S. For example, following the Snowden leaks the Bremen Data Protection Authority requested that companies transferring personal data to the U.S. inform the DPA on how access by the NSA is prevented.[xxxiv]

There is also concern in the EU with U.S. dominance of the I.T. sector. For instance, Google accounts for over 90 percent of Internet searches in Europe. Social networking is dominated by

Facebook and U.S. companies such as Microsoft and Amazon are key players globally when it comes to cloud computing.

As part of the Safe Harbor framework negotiations, the European Commission provided a list of 13 recommendations it wished to have addressed.[xxxv] My understanding is that very good progress has been made on all these recommendations, the most difficult discussions being over how to give effect to recommendations 12, and particularly 13, which requires that the Safe Harbor national security exception is "used only to an extent that is strictly necessary."

The *Schrems* Decision

The case of *Schrems v. Data Protection Commissioner*[xxxvi] before the European Court of Justice (ECJ) addressed whether the Irish Data Protection Authority (DPA) was bound by the European Commission's finding that the U.S., under the Safe Harbor framework, provides an adequate level of protection of persona data. The Irish DPA had found that the Commissions' adequacy decision under the Safe Harbor framework prevented further investigation into whether the use by Facebook of personal data is consistent with the EU Privacy Directive.

The key findings in *Schrems* are:

- The Safe Harbor framework fails to provide an adequate level of protection of personal information for the following reasons:
    - U.S. public authorities are not subject to the Safe Harbor framework
    - U.S. authorities have accessed EU personal data beyond what is strictly necessary and proportionate to the protection of national security

    - There is no administrative or judicial means of redress that allows EU citizens to access their personal data and to have it rectified or erased if needed.
    - The trumping of national security demands when in conflict with the protection of privacy restricts the ability of DPAs to determine compatibility of data transfers with the Safe Harbor framework.
- As a result, the European Commission finding under the Safe Harbor framework that the U.S. provides an adequate level of protection of EU personal information is invalid.
- An adequacy finding by the Commission does not reduce the power of national Data Protection Authorities to determine whether transfers of personal data to the U.S. comply with EU Data Privacy Directive.
- Only the ECJ can declare whether a Commission decisions in invalid.

The Implications of the *Schrems* decision

Following the *Schrems* decision, the Article 29 Working Party—made up of representatives of EU DPAs—stated that it would wait until the end of January 2016 before enforcing *Schrems*.[xxxvii] In the meantime, the Working Party noted that concluding the Safe Harbor negotiations could be part of the solution. Certainly, the European Commission is hoping that the Safe Harbor negotiations can address the concerns laid out by the ECJ.[xxxviii] To achieve this would require passage by the Senate of the Judicial Redress Act.[xxxix] Whether a new Safe Harbor framework satisfies the ECJ will ultimately need to be tested again before that court.

The *Schrems* decision also calls into question the legality of BCRs and contracts for transferring personal data from the EU to the U.S. This is because ECJ concerns about the level of privacy

protection in the U.S. and, in particular, the access of national authorities to personal data for national security purposes would appear to be relevant to all data transfer mechanisms. In this regard, post-*Schrems* German DPAs have called into question the ability to use standards contract and BCRs to transfer personal data to the U.S. and have said that they will not currently issue new authorizations to transfer persona data to the U.S. on the basis of BCRs or model contracts.

Companies can rely on the so-called derogations outlined above, including consent. As outlined, these are limited in scope and therefore are only partial options for companies needing to transfer personal data.

The net result then is considerable legal uncertainty about how to transfer personal data from the EU to the U.S.

The outcome will be particularly costly for SMEs. This is due to the legal and risk management that companies must now undertake—costs that will fall most heavily on smaller companies. In addition, to the extent that BCRs and contracts are still used, these mechanisms are less useful for SMEs. For instance, BCRs apply to conglomerates that have a presence in the EU, which is often not the case for SMEs that are providing online services from the U.S. using Internet platforms.

Conclusion

I appreciate the opportunity to offer my views on this important issue.

[i] Daniel S Hamilton and Joseph P. Quinlan, "The Transatlantic Economy 2014", Volume 1/2014

[ii] This figure is based on data over submarine cables. This figure does not necessarily only capture the end-uses of the data, as data often transits though the U.S. and Europe. For instance, data from Latin America can transit the U.S. on its way to Europe and data from Africa can transit through Europe on its way to the U.S.

[iii] Joshua P. Meltzer, "The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment", Brookings Working Paper 79, October 2014

[iv] Statista Dossier, Global internet usage 2014, p. 47

[v] Frederic Gonzales, J. Bradford Jensen, Yunhee Kim and Hildegunn Kyvik Nordas, "Globalisation of Services and Jobs", in Policy Priorities for International Trade and Jobs (OECD 2012), p. 186

[vi] Gene M. Grossman and Estaben Rossi-Hansberg, "Trading Tasks: A simple Theory of Offshoring", 98:5 American Eco Review (2008), p. 1978

[vii] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013-2018, p. 3

[viii] Statista Dossier, Global internet usage 2014, p. 41

[ix] SBA Advocacy 2014

[x] U.S. International Trade Commission, "Digital Trade in the U.S. and Global Economies, Part 1", Investigation No., 332-531, July 2013, p 3-2

[xi] eBay (2015), 2015 US Small Business Global Growth Report

[xii] Qiang & Rossotto (2009), "Economic Impacts of Broadband in The World Bank (2009)

[xiii] Caroline L. Freund and Diana Weinhold (2004) The effect of the Internet on international trade *Journal of International Economics* 62, 171

[xiv] Huub Meijers (2014), "Does the Internet generate economic growth, international trade, or both?" Int. Econ Policy, 11:162

[xv] Joshua P. Meltzer, "The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment", Brookings Working Paper 79, October 2014

[xvi] Joshua P. Meltzer, "The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment", Brookings Working Paper 79, October 2014

[xvii] Bernard, Jensen & Redding (May 2007),Firms in International Trade *Center for Economic Studies, Bureau of Census* (CES 07-14, p. 5

[xviii] Grossman, G.M., Helpman, E., (1991) Innovation and Growth in the Global Economy MIT Press, Cambridge; Baily, M.N., (2002), The new economy: post mortem or second wind? Distinguished lecture on economics in Government. *Journal of Economic Perspectives* 16 (2), 3-22

[xix] Martin Falk & Eva Hagsten (2015) "E-Commerce Trends and Impacts Across Europe, UNCTAD Discussion Paper No. 220, March 2015, UNCTAD/OSG/DP/2015/2, March 2015

[xx] United States International Trade Commission (August 2014), Digital Trade in the U.S. and Global Economies *Part* 2 *Pub. 4485 Investigation No. 332-540*, 71

[xxi] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy" in *Harvard Law Review* Vol. IV, No. 6 (15 December 1890)

[xxii] OECD (2013) The evolving privacy landscape: 30 years after the OECD Privacy Guidelines (2011) in The OECD Privacy Framework, OECD 2013, p. 69

[xxiii] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012/0011 (COD), Brussels, 25.1.2012. The proposed Regulation includes a Communication from the Commission and a proposed Directive on rules for data processes by authorities for prosecuting criminal offenses. This paper focuses on the Regulation only.

[xxiv] DPD Artilce 2

[xxv] DPD Article 6

[xxvi] DPD Article 7

[xxvii] DOD Article 25

[xxviii] European Commission Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina, C(2003)1731 final, Brussels, 30/06/2003
[xxix] DPD Article 26
[xxx] Advisory working party established under the DPD comprising representatives from Member State data protection authorities and from the European Commission
[xxxi] Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Opinion 1/99 Concerning the Level of Data Protection in the United States and the Ongoing Discussion Between the European Commission and the United States Government*, at 4, DG MARKT Doc. 5092/98/WP 15 (Jan, 26, 1999)
[xxxii] Commission Decision 520/2000/EC of 26 July 2000
[xxxiii] Communication from the Commission to the European Parliament and the Council on the functions of the Safe harbor from the Perspective of EU Citizens and Companies Established in the EU / COM/2013/0847 final
[xxxiv] Communication from the Commission to the European Parliament and the Council on the functions of the Safe harbor from the Perspective of EU Citizens and Companies Established in the EU / COM/2013/0847 final
[xxxv] Communication from the Commission to the European Parliament and the Council on the functions of the Safe harbor from the Perspective of EU Citizens and Companies Established in the EU / COM/2013/0847 final
[xxxvi] Maximillian Schrems v. Data Protection Commissioner, European Court of Justice, Case C-362/13, 6 October 2015
[xxxvii] Statement of the Article 29 Working Party, Brussels, 16 October 2016
[xxxviii] Commissioner Jourova's remarks on Safe Harbor EU Court of Justice judgement before the committee on Civil Liberties, Justice and Home Affairs, 26 October 2015
[xxxix] H.R. 1428 – Judicial Redress Act of 2105