

The Economic Impact of the European Reform of Data Protection

Stéphane CIRIANI

Regulatory Affairs, Orange, France (*)

Abstract: The economic value of personal data is mainly extracted through online intermediation services and big data analytics. The largest providers of these services are US OTTs. These are global market players with a leading position in the European market. As a result, the personal data of European users are widely processed by these providers. The EU and the US have different approaches to personal data protection and data privacy. In the US, privacy is a property right whereas in the EU, it is a fundamental right, which must be provided by the government. The European Commission has proposed a reform of personal data protection, the General Data Protection Regulation (GDPR), aiming to ensure that European consumers are protected according to European law whenever their data are processed outside the EU by foreign companies. According to the European Commission, the reform will bring economy-wide benefits to the EU. However, several studies on the economic impact of the reform have led to opposing conclusions. They claim that the extraterritorial application of the European law will impose a regulatory cost burden on US providers. This burden would hurt transatlantic trade in services, and would be detrimental to the European economy. Our analysis shows that the GDPR is not a protectionist policy. The extraterritorial application of the European law will neither hinder competition nor disrupt cross-border data flows. On the contrary, the extension of European law to the US OTTs that target European consumers will contribute to establishing a level playing field between European providers and their US competitors in the European market. Both EU and US providers would obey European laws when processing European consumers' personal data. Nevertheless, the literature examined provides no evidence that reinforced standards of protection would foster the competitiveness of European services in world markets. Moreover, studies also suggest that the costs of applying the GDPR in the EU might outweigh the efficiency gains. In conclusion, the optimal trade-off between incentives to provide innovative services and the obligation to protect privacy as a fundamental right has yet to be achieved by the European regulation. Rather than increase administrative burden, an efficient data protection policy should base European users' protection on modernised, more dynamic principles, supporting the capability of European industry to compete and innovate on fair and efficient grounds for the benefit of European users and of the European economy.

Key words: big data, General data protection regulation, over the top, personal data protection, safe harbour.

(*) Disclaimer: The opinions expressed in this article are those of the author and do not necessarily represent the opinions of Orange.

Business models based on personal data are developing rapidly throughout the world. The European ecosystem of infrastructures and services enabling the targeting, collection, storage and processing of personal data is largely dominated by US providers of OTT services, who have succeeded in monetising personal data ¹. The personal data of European consumers are largely processed by these global market players. It appears that the approach on data protection differs across countries. As recalled by MOVIUS & KRUP (2009), privacy is considered a property right in the US and can therefore be traded on a market. In the EU, privacy is a fundamental right guaranteed by law and consequently it cannot be traded.

The European authorities are committed to reinforcing the application of European law to transatlantic data flows. To ensure that European users' privacy will be protected according to European law, the EU has proposed a new legal framework, the General Data Protection Regulation (GDPR) ². This framework will impose European data protection rules on all foreign companies who handle European consumers' digital information. In the following sections, we examine several studies that have drawn attention to the detrimental economic impacts that the GDPR could have on both the EU and the US. These studies are notably concerned with the extraterritorial scope of the GDPR ³. They consider that the new framework will shift the regulatory cost burden from European companies to US companies, and view it as a trade barrier.

Our analysis shows that the European reform of data protection is not a protectionist policy. It will neither disrupt cross-border data flows nor transatlantic trade in services. It will instead help tackle regulatory discrepancies between European and US digital service providers. It will

¹ The Over The Top (OTT) market players provide digital services on the internet. These services encompass search, media streaming, messaging, VoIP, gaming, e-commerce, social network, cloud computing and big data analytics... The main world OTT providers are internet intermediaries such as Google, Facebook, Amazon, eBay, Apple, Skype (Microsoft)...

² http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

³ In Europe, the processing and the transfers of personal data are regulated under the 1995 Data Protection Directive (95/46/EC). It permits to transfer data to a third country outside the EU provided the country is considered to offer «adequate» protection for personal data. In 2014, only twelve countries were recognized to provide adequate data protection. Non adequate countries are allowed to move personal data from the EU under specific agreements such as Safe Harbour agreements (for the US), Model Contracts with clauses in compliance with the European Standards (Model Contract Clauses - MCCs) or Binding Corporate Rules (BCRs).

thus foster fair competition within the European market. However, uncertainties remain concerning the GDPR's cost efficiency and its ability to foster the competitiveness of European providers outside the EU.

The first section addresses the dominance of US OTTs in the world markets of data-intensive services and the extraterritorial application of European data protection laws. The second section examines the studies claiming that the GDPR would raise a trade barrier and distort transatlantic data flows. In the third section, we show that the GDPR will not distort transatlantic trade and instead will aid in establishing a level playing field in the EU. The fourth section looks at the GDPR's impact assessments. It turns out that the GDPR's effects on the European economy and the competitiveness of European companies are uncertain. We must therefore place focus on the need to balance sound privacy protection with business opportunities in order to avoid excess cost burden.

■ The GDPR aims to protect online privacy of EU consumers within the frame of EU law

In the European market, economic value generated from monetizing personal data essentially goes to US providers. These market players process personal data from European consumers without being established or materially based in the EU. Transfers of European personal data to the US are authorized under the Safe Harbour regime. The US OTTs are allowed to move data to the US and process it there as long as they certify that they comply with European data protection law⁴. In addition to Safe Harbour, Article 29 Working Party (the Working Group for all EU Data Protection Authorities) issued a framework for Binding Corporate Rules (BCRs) in 2008, ensuring that the transfer of personal data outside the EU takes place in accordance with EU rules on data protection. The BCRs allow for international transfers of personal data within a single corporate group to

⁴ Under the current European data protection regime, the US are not regarded as equivalent by the European authorities. Transatlantic data transfers are allowed under the Safe Harbour regime, whereby the US companies are required to notify compliance with the European data protection law in order to transfer personal data from the EU to the US. Organizations which are not subject to the jurisdiction of the Federal trade Commission (FTC) cannot participate in the Safe Harbour. These organizations notably include banks and credit institutions, and telecommunications common carriers. <https://safeharbor.export.gov/list.aspx>

entities located in countries which do not provide a level of data protection consistent with European law.

The ecosystem of personal data in Europe is dominated by US OTTs

The global ecosystem of digital services which extract value from personal data is dominated by US OTTs. They are the world leaders in internet intermediation and e-commerce, digital advertising, big data and cloud computing. In May 2014, Google, Facebook and Amazon accounted for 54% of the worldwide market value of the twenty largest internet companies (of which twelve are US and none are European)⁵. Our own estimations show that the US accounted for 83% of worldwide internet intermediation revenue in 2007 and for 81% in 2012, while the EU-27 accounted for 1.1% in 2007 and only 1.7% in 2012⁶. The world market of search engines is dominated by Google, with an 88% market share in 2014. Google also accounted for 86% of the European market of online search in early 2014⁷. American OTTs also lead the mobile advertising world market. Google and Facebook accounted for 70% of overall revenue in 2013⁸. Moreover, sixteen US companies and only three European companies were ranked among the twenty largest big data vendors in 2013⁹. Also, nine of the ten leading world providers of cloud services were US companies in 2013¹⁰. Moreover, 72% of cloud service providers in the EU were storing data in the US in 2014¹¹.

⁵ <http://www.statista.com/statistics/277483/market-value-of-the-largest-internet-companies-worldwide/>

⁶ Our own estimations are based on a sample of 111 companies of the digital sector representing 67% of the global revenue (Source Booz & Co. Thomson Financial data).

⁷ <http://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/>;
<http://etc-digital.org/digital-trends/consumer-behaviour/search-engines/regional-overview/europe/>

⁸ <http://www.emarketer.com/Article/Driven-by-Facebook-Google-Mobile-Ad-Market-Soars-10537-2013/1010690>

⁹ http://wikibon.org/wiki/v/Big_Data_Vendor_Revenue_and_Market_Forecast_2013-2017

¹⁰ <http://talkincloud.com/talkin039-cloud-top-100-cloud-services-providers/top-100-cloud-services-providers-list-2013-ranked-0>

¹¹ <http://www.skyhighnetworks.com/press/9-10-cloud-services-putting-european-businesses-risk/>

The GDPR will ensure EU consumers' data are protected according to EU law when the data are processed by foreign providers outside EU

The new European Commission has endorsed the proposal for a reform of personal data protection (GDPR). It was voted by the European Parliament in March 2014 and has yet to be approved by the Council of the European Union ¹². The GDPR will impose a single European law for personal data protection, which will apply to any provider who tracks, stores and processes European consumers' data. The GDPR will also strengthen current privacy safeguards by adding new requirements. According to the impact assessment conducted by the European Commission (2012), the GDPR would bring €2.3 billion net annual savings in administrative costs thanks to the harmonization of privacy rules across the EU. In its factsheet on data protection reform, the Commission also argues that consumers' confidence in high privacy standards would provide European companies with an advantage over their competitors in foreign markets ¹³.

The extraterritorial scope of GDPR implies that US providers will have to apply European data protection rules whenever they use European consumers' personal information. In a 2013 Communication on the functioning of Safe Harbour, European authorities claimed that the transparency of Safe Harbour members' privacy policies and the effectiveness with which Safe Harbour's privacy principles are applied by companies in the US needed to be reviewed. The European Commission and the Article 29 Working Party on privacy protection affirmed in a 2014 working paper that Safe Harbour's possibility to provide adequate protection for EU citizens was "questionable". The European Parliament adopted a resolution in March 2014 calling for the suspension of Safe Harbour until "transfers of personal data for commercial purposes from the Union to the US can only take place in compliance with highest EU standards" ¹⁴. Also, in 2012, the Article 29 Working Party expressed concerns that Google's privacy policy was not consistent with European data protection laws ¹⁵. Six European Data Protection Authorities initiated investigations on Google's

¹² http://europa.eu/rapid/press-release_MEMO-14-186_fr.htm

¹³ http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/6_en.pdf

¹⁴ <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230>

¹⁵ Google's new privacy policy raises deep concerns about data protection and the respect of the European law", CNIL, 2012.
<http://www.cnil.fr/institution/actualite/article/article/googles-new-privacy-policy-raises-deep-concerns-about-data-protection-and-the-respect-of-the-euro/>

privacy policies, and in 2014, the French Data Protection Authority (CNIL) issued a penalty of €150 000 to Google because its privacy policy did not comply with the French data Protection Act ¹⁶.

The GDPR addresses the issues relating to international differences in privacy policy by ensuring that European citizens' personal data are protected according to European data protection law regardless of their digital service provider and the location of their personal data.

■ Several studies show that extraterritorial application of EU law will shift regulatory cost burden on US OTTs

In this section, we analyze the economic literature opposed to the GDPR's adoption and to the revision of the current Safe Harbour regime by European authorities. These studies claim that the European reform will shift the cost burden of compliance to US companies. They expect European authorities either to repeal the Safe Harbour or enact fierce restrictions on transatlantic data flows in order to make them compatible with the new GDPR rules. They recommend establishing free trade agreements instead of strengthening standards of privacy through a single European law with extraterritorial application.

Several economic studies regard GDPR as a trade barrier imposed on US OTTs and expect it to distort transatlantic trade

HOFHEINZ & MANDEL (2014) claim that the GDPR is a "regulatory wall" extending the protection of personal data "well beyond the normal assurances consumers might expect". The reform is viewed as a "protectionist policy", encouraging "the proliferation of weak national champions by ostentatiously shutting out the world's best, most competitive players". According to the authors, the GDPR would harm US business opportunities in the EU, which rely heavily on US companies for the provision of digital services.

¹⁶ The CNIL's Sanctions Committee issues a 150 000 € monetary penalty to GOOGLE Inc.", CNIL 2014".
<http://www.cnil.fr/english/news-and-events/news/article/the-cnils-sanctions-committee-issues-a-150-000-EUR-monetary-penalty-to-google-inc/>

A study from The ECIPE (2013) on behalf of the US Chamber of Commerce argues that the GDPR would begin to hurt transatlantic trade in services one year after its adoption. It would increase the production costs of European providers, but also those of the US due to the extraterritorial enforcement of European law. This could decrease bilateral trade in services by more than 0.5%. The authors mention that in comparison, the TTIP¹⁷ could raise it by 0.7%. They argue that the GDPR would nearly cancel out the benefits of free trade between the EU and the US. They also consider a scenario in which the GDPR is accompanied by the repeal of the Safe Harbour. Providers from the US and other non-Safe Harbour countries would have to install equipment in the EU to process data from European consumers. Additional costs incurred by the US providers would lower US exports to the EU by more than 20%. Cutting off the supply of digital services used as inputs by European companies would decrease the EU-27 GDP by more than 1%. It could decrease GDP by 4% if the "right to be forgotten" obligation was implemented in addition.

In a more recent study, the ECIPE (2014) estimates that the adoption of the GDPR could decrease the EU-27 GDP by 0.4% in one year. Moreover, coupling the main GDPR rules with a "data localization requirement" or any other "discriminatory privacy laws to similar effect" would decrease the EU-27 GDP by 1.1%¹⁸. The authors consider that the new framework is a protectionist policy, which impedes fair competition in the European market by imposing disproportionate liabilities against non-European providers. They claim that the European framework is only focused on security and privacy laws. This could act as a trade barrier for US providers, disrupt transatlantic trade, and deprive European companies from affordable US input services. They urge policy makers to consider the potentially disruptive impacts of personal data protection on international trade and digital supply chains.

The annual report of the US Trade Representative Office (2014) has claimed that such digital trade barriers would disproportionately affect US service providers because of their strong competitive position in the European market. The US Trade Representative Office reaffirms its willingness to ensure that "US companies have a level playing field to supply new and innovative products and services" in Europe. It also considers that

¹⁷ The Transatlantic Trade and Investment Partnership. <http://www.ustr.gov/ttip>

¹⁸ The authors define "data localization requirement" as the "mandatory storage of critical data on servers physically located inside the country".

the creation of a Europe-only electronic network could lead to an "effective exclusion or discrimination against foreign services suppliers that are directly offering network services, or dependent on them" ¹⁹. For EZELL *et al.* (2013), local data storage requirements damage economies affected by them. The authors argue that localization requirements hinder the cost efficiency of companies because:

"If it made economic sense to localize production in the destination country, they would have already done so".

They strongly oppose mandatory localization of data centers, stating that:

"Coerced local production raises firms' costs, meaning lower profits and less investment in their home nations".

These studies consider that the new European framework is a protectionist policy that will disrupt cross-border data flows, and impede European companies' access to input services (produced in the US or using US digital services as inputs) at competitive prices. A scarcity of digital services in the European market or a rise in their market price will damage European business sectors which make intensive use of digital service inputs. A breakdown in the supply of digital services from US providers will then reduce aggregate output in the EU.

■ The new European personal data protection framework will foster fair competition within the EU

In this section, we show that the new data protection framework is not a protectionist policy, as it would neither introduce any discrimination against US providers nor prevent international transfers of personal data.

The GDPR is not a protectionist policy, as it does not aim to impede US providers exporting their services to the EU

In the EU, privacy is regulated under the 1995 Data Protection Directive (DPD) ²⁰. This Directive was adopted before the worldwide development of

¹⁹ <http://www.reuters.com/article/2014/04/04/us-usa-trade-telecommunications-idUSBREA331W820140404>

²⁰ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

US OTTs. Its purpose was not to palliate an EU trade deficit but to protect privacy according to the European data protection principles. The GDPR does not modify the substance of the 1995 DPD, but rather intends to reinforce privacy safeguards, harmonize its application within the EU, and apply European data protection law extraterritorially. The GDPR could be deemed protectionist if it imposed rules on the foreign providers while exempting EU providers from applying them. This is not the case, as both EU and US providers would have to apply European law when processing data from European consumers. The purpose of the GDPR is to harmonize the protection of European consumers' personal data inside and outside the EU. Transatlantic data flows would therefore not be distorted by enforcement of the GDPR.

Moreover, under the European framework, the regulation of the collection and processing of personal data is lopsided. As ALLOUET *et al.* (2014) have shown, the providers of "Electronic Communications Services" (ECS) have to comply with a wider range of rules than the providers of OTT services, which are classified as providers of "Information Society Services" (ISS) ²¹. However, the new European framework does not address the asymmetry resulting from the classification of digital services. Nevertheless, the European reform of data protection will help move towards a level playing field between European and US providers by ensuring that they comply with the European data protection law when they handle European consumers' personal information. The GDPR will contribute to establishing genuine competition within the EU digital economy.

²¹ ALLOUET *et al.* (2014) show that the European digital services providers do not compete on an equal footing with the US OTTs because of a lack of effective enforcement of European law on US OTT providers and because of asymmetrical regulations which impose more stringent rules to telecommunications operators than to OTTs for the provision of their services, in particular concerning rules for the collection and the processing of personal data. The telecommunications operators who are "Electronic Communications Services" (ECS) providers have to comply with more rules than OTT providers, who are "Information Society Services" (ISS) providers. The Telecom Package provides a stringent regulation of personal data processing, but does not apply to OTT providers.

A "Schengen Routing" has been advocated by some European stakeholders but is contrary to the European reform proposal

Some European stakeholders advocate a "Schengen Routing" policy ²². Its primary aim is to ensure protection of European consumers by maintaining their personal data under European privacy laws. This policy implies that European personal data should only be managed through European data centers and networks ²³. However, this would raise technical issues related to the managing of data from European consumers who would continue to use services provided by US OTTs. A Schengen routing policy might render US services less available to European consumers, but we consider this unlikely to be an efficient policy. Such a policy stands contrary to the European reform proposal, which does not include any location requirements to the US providers. The reform intends to ensure that US providers comply with European law when they process European personal data.

Protectionist policies are not supported by the European authorities, who affirmed their willingness to build an efficient framework for transatlantic data flows in collaboration with US authorities ²⁴. The European authorities are not in favor of negotiating personal data protection within the EU-US free trade agreement (TTIP), as they consider that data protection is a fundamental right that cannot be traded and should not be subject to economic efficiency criteria ²⁵. As a result, the TTIP is unlikely to be the instrument that balances EU data protection requirements with the development of efficient, welfare-enhancing digital services. The European authorities have yet to achieve such an optimal trade-off.

²² <http://www.dw.de/weighing-a-schengen-zone-for-europes-internet-data/a-17443482>;
<http://www.telecompaper.com/news/atos-ceo-says-schengen-for-data-is-no-magical-line-981970>

²³ <http://www.dw.de/deutsche-telekom-internet-data-made-in-germany-should-stay-in-germany/a-17165891>

²⁴ Speech 14-62 from Viviane Reding, the former Vice-President of the European Commission, EU Justice Commissioner. http://europa.eu/rapid/press-release_SPEECH-14-62_fr.htm

²⁵ http://trade.ec.europa.eu/doclib/docs/2015/january/tradoc_152999.2%20Services.pdf

■ Despite harmonising data protection, the GDPR might not foster EU's competitiveness in foreign markets

Several economic assessments concerning the reform's expected impacts conclude that it would be detrimental to the European economy. These assessments, presented below, conclude that the cost burden on European companies will likely outweigh efficiency gains. Additional studies claim that increasing users' confidence in privacy standards might not be sufficient to foster adoption of digital services.

According to economic assessments of EU data protection reform, its cost burden is expected to outweigh its benefits

The following studies claim that the GDPR would impose a net cost on European organizations, due to either new compliance obligations or limitations of business opportunities. They argue that the cost burden from compliance will not be offset by efficiency gains even in the long run.

The UK Ministry of Justice (2012) acknowledges GDPR's benefits from legal harmonization and high standards of privacy. However, it claims that the Commission's assessment has overestimated savings from harmonization and underestimated the new compliance costs imposed on organizations. These costs stem most notably from the obligation to carry Data Protection Impact Assessment (DPIA) ²⁶, hire a Data Protection Officer (DPO) ²⁷, as well as notify data breaches ²⁸. The burden of compliance will translate into additional IT costs for European organizations. As a result, the application of GDPR would induce a net loss to the UK's economy. This net loss would amount to £250 million over one year and £2.1 billion over 14 years.

²⁶ Article 33 of the GDPR introduces obligation of data controllers and processors to carry out a data protection impact assessment prior to risky processes.
http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

²⁷ The Article 35 of the GDPR introduces "mandatory data protection officer for the public sector, and, in the private sector, for large enterprises or where the core activities of the controller or processor consist of processing operations which require regular and systematic monitoring."

²⁸ The Articles 31 and 32 of the GDPR requires data controllers to "notify personal data breaches, building on the personal data breach notification in Article 4(3) of the e-privacy Directive 2002/58/EC".

An econometric study from CHRISTENSEN *et al.* (2013) shows that the GDPR would raise the production costs of European companies. Depending on the sectors, the compliance costs would amount to 20% of their annual IT spending on average. Higher production costs would in turn decrease their labor demand and prevent entry of new competitors. As a result, employment in the EU could decrease by 0.3%, and the number of companies could decrease by 3% on average in the long run.

Qualitative studies have also concluded that the GDPR would be detrimental to the European economy. For PYYKKO (2012), the restrictions on data processing would hamper the effectiveness of financial services, and decrease the amount of credit available to European consumers and companies as well. LLOYD (2012) argues that the new compliance costs would largely outweigh savings from the reform. The author expects GDPR rules such as the "right to be forgotten" and the "right to data portability", along with the obligation to hire a Data Protection Officer (DPO) to increase the regulatory burden. Moreover, GOLDFARB & TUCKER (2011) show that the European personal data protection regulation might hinder the effectiveness of online digital advertising in the EU, and thus the capacity to monetize the digital contents. It is unlikely that The GDPR, which will strengthen the existing rules, would foster the development of digital services in the EU.

The user's trust in the privacy standards of digital providers might foster the adoption of the services they offer

The European Commission (2012) affirms that users' distrust of privacy standards is the main obstacle to the adoption of digital services and the development of the digital economy in the EU ²⁹. According to a report from the Boston Consulting Group (2014), the value of digital services based on the utilization of personal data could represent 8% of the EU-27 GDP by 2020. However, the study claims that the adoption of digital services could be hampered if the providers failed to provide end users with sufficient data protection safeguards. CAMPBELL *et al.* (2003) show that personal data breaches caused a significant drop in the stock market value of 38 large US companies over 1995-2000. ACQUISTI *et al.* (2006) show evidence that

²⁹ According to the EU Commission, 72% of EU citizens are worried that their personal data may be misused and transferred between companies without their permission. http://europa.eu/rapid/press-release_IP-13-57_en.htm

personal data breaches had a significant negative impact on the market value of publicly traded companies (NYSE and NASDAQ) over 2000-2006, although this impact was short lived. For BRADSHAW *et al.* (2012), the protection of data privacy is a major driver of the development of cloud services, which could add €940 billion to the EU-27 GDP by 2020.

Digital services are adopted with no regard for privacy concerns

As shown by TADDICKEN (2013) on a representative sample of internet users, concerns about privacy do not hinder willingness to disclose personal information online. Moreover, as shown by the market dominance of US OTTs, the low level of user trust in standards of privacy has not hampered the adoption and the usage of their services within the EU. The leading position of US OTTs has not been affected by the disclosures of US National Security Agency (NSA) surveillance programs PRISM, through which the US authorities accessed the records of ISPs and CSPs ³⁰.

This tends to show that privacy concerns are not an obstacle to the adoption of digital services. According to IDATE (2014), the lack of trust in standards of privacy might limit the volume of information that users disclose but it might not hinder the adoption of services.

As a result, offering higher standards of privacy might not bring larger market shares to European providers in foreign markets. We can conclude that the GDPR could thus fail to foster the competitiveness of European providers in foreign markets.

Big data could bring economic benefits to the EU provided that GDPR achieves a balance between protection and business opportunities

Achieving an efficient reform of data protection in Europe is particularly important in the field of big data services, which could bring significant economy-wide benefits. For example, the CEBR (2012) expects big data analytics to provide £216 billion to the UK economy over 2012-2017. Big data services will improve customer intelligence, supply chains, health care and public sector management. BUCHHOLTZ *et al.* (2014) show that big

³⁰ <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>

and open data could raise EU-28 GDP by 1.9% by 2020. In particular, big data applications in trade and manufacturing could raise business efficiency. The authors argue that the economic value generated from data processing depends on the regulation of data protection, and recommend that the EU balances the interests of service providers and end-users without creating unnecessary legal burdens. As shown in the first section, the largest providers of big data services are US companies. This implies that the personal information of European users of big data services are generally stored and processed outside the EU. As a result, to reap the economic benefits of big data in the EU, the European authorities should strike a balance between the protection of European consumers' personal data and the opportunities to develop services that fully exploit large sets of data.

With the exception of the impact assessment of the European Commission, all the economic studies we have examined have demonstrated that the GDPR could have detrimental effects on the EU. According to studies examined in the second section, these detrimental effects should stem from the restriction in transatlantic data flows induced by the GDPR. We have shown that the GDPR would not put up any barriers to trade. Consequently, the EU would not suffer from a shortage in digital services because of the GDPR. According to the studies examined in the fourth section, the detrimental economic effects of the reform could stem from the regulatory cost burden that the reform would impose on digital service providers. Further investigation on the dynamic allocation of the reform's costs and benefits is needed in order to assess its expected net impact on the European economy.

■ Conclusion

The market players who have so far succeeded in monetizing personal data are the large providers of OTT services. The European Commission has proposed a reform applying European personal data protection laws to all providers who target, collect, store and process digital information concerning European consumers. Our analysis shows that the extraterritorial application of European law would promote a level playing field within the European market. However, the GDPR might not provide European companies with a competitive edge over US OTTs in foreign markets. Evidence suggests that the provision of high standards of protection might not be sufficient to gain shares of the foreign markets. Moreover, with the

exception of the GDPR's impact assessment conducted by the European Commission, the literature we have examined shows that the costs of GDPR's adoption might offset the efficiency gains. The limitations imposed on the processing of personal data could hamper the capacity of the European companies to monetize them. Further economic analysis of the dynamic trade-off between costs and benefits of the GDPR is needed. The European reform proposal should achieve a balance between privacy protection requirements and business opportunities, while imposing the extraterritorial application of European data protection law. Increasing the administrative burden might not help improve the competitiveness of European digital service providers. An efficient European policy should take more into account the pros and cons of successful personal data-based business models all over the world. It must rebalance the rules with more room given to flexibility and ex-post effects-based accountability in order to support the role of European industry in this new economy of innovative services to the benefit of European users.

References

ACQUISTI, A., FRIEDMAN, A. & TELANG R. (2006): "Is There a Cost to Privacy Breaches? An Event Study", 5th Annual Workshop on the Economics of Information Security, WEIS 2006.

ALLOUET, A.-M., LE FRANC, S., MARQUES, M.-N. & ROSSI L. (2014) : "Achieving a Level Playing Field between the Players of the Internet Value Chain", *Communications & Strategies*, 2014, vol. 1, issue 93, pp. 99-118

Boston Consulting Group (2014): "The Value of our Digital Identity", Liberty Global Policy Series.

<http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf>

BRADSHAW, D., FOLCO, G., CATTANEO, G. & KOLDING M. (2012): "Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Up-Take", IDC Final Report SMART 2011/0045, July 2012.

<http://www.icon-project.eu/docs/upload/201310/Cloud-Computing.pdf>

BUCHHOLTZ S., BUKOWSKI M. & SNIEGOCKI A (2014): "Big and opean data in Europe. A growth engine or a missed opportunity?", The Warsaw Institute for Economic Studies (WIES Institute).

<http://www.microsoft.com/global/eu/RenderingAssets/pdf/2014%20Jan%2028%20E%20ME%20Big%20and%20Open%20Data%20Report%20-%20Final%20Report.pdf>

CAMPBELL K., GORDON L. A, LOEB M. P. & ZHOU L. (2003): "The economic cost of publicly announced information security breaches: empirical evidence from the stock market", *Journal of Computer Security* 11 (2003) 431-448.

CEBR - Centre for Economics and Business Research Ltd (2012): "Data equity. Unlocking the value of big data".

<http://www.sas.com/offices/europe/uk/downloads/data-equity-cebr.pdf>

CHRISTENSEN, L., COLCIAGO, A., ETRO, F. & RAFERT G. (2013): "The Impact of the Data Protection Regulation in the EU", International Think-tank on Innovation and Competition INTERTIC, February 2013.

CNIL (Commission Nationale de l'Informatique et des Libertés) :

- (2012): "Google's new privacy policy raises deep concerns about data protection and the respect of the European law", February.

<http://www.cnil.fr/linstitution/actualite/article/article/googles-new-privacy-policy-raises-deep-concerns-about-data-protection-and-the-respect-of-the-euro/>

- (2014): "The CNIL's Sanctions Committee issues a 150 000 € monetary penalty to GOOGLE Inc.", January. <http://www.cnil.fr/english/news-and-events/news/article/the-cnils-sanctions-committee-issues-a-150-000-EUR-monetary-penalty-to-google-inc/>

Deloitte (2012): "Data nation 2012. Our lives in data", Deloitte Analytics Paper. <http://www.cil.cnrs.fr/CIL/IMG/pdf/uk-mi-da-data-nation-2012.pdf>

ECIPE - European Centre for International Political Economy:

- (2013): "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce".
https://www.uschamber.com/sites/default/files/legacy/reports/020508_EconomicImportance_Final_Revised_Ir.pdf
- (2014): "The Costs of Data Localisation: Friendly Fire on Economic Recovery" Occasional Paper - N°3/2014.
http://www.ecipe.org/media/publication_pdfs/OCC32014_1.pdf

European Commission:

- (2008): Article 29 Data Protection Working Party, "Working Document Setting up a framework for the structure of Binding Corporate Rules", 24 June.
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp154_en.pdf
- (2014): Article 29 Data Protection Working Party, "Appendix: WP29 additional recommendations to strengthen personal data protection under the Safe Harbour Decision". http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf
- (2012): Communication COM(2012) 11 final, "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)", 25 Jan.
http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
- (2013): Communication COM(2013) 847 final "On the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU", 27 Nov. http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf
- (2012): Commission Staff Working Paper 72 final, "Impact Assessment", 25 Jan.
http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf
- (1995): Directive 95/46/EC of the European Parliament and of the Council, 24 Oct.
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>
- (2012): Factsheet, "How will the EU's data protection reform simplify the existing rules?", June.
http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/6_en.pdf
- (2014): MEMO 14-186, "Progress on EU data protection reform now irreversible following European Parliament vote", 12 March.
http://europa.eu/rapid/press-release_MEMO-14-186_fr.htm
- (2013): Press Release 13-57: "European Data Protection Day 2013: Full speed ahead towards reliable and modern EU data protection laws", 28 Jan.
http://europa.eu/rapid/press-release_IP-13-57_en.htm
- (2013): Speech 14-62, "A data protection compact for Europe", 28 Jan.
http://europa.eu/rapid/press-release_SPEECH-14-62_fr.htm
- (2014): European Parliament resolution of 12 March on the US NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens' fundamental rights.
<http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230>

EZELL, S., ATKINSON, R. D. & WEIN M. A. (2013): "Localization Barriers to Trade: Threat to the Global Innovation Economy", The Information Technology & Innovation Foundation (ITIF), September.

HOFHEINZ, P. & MANDEL M. (2014): "Bridging the Data Gap. How Digital Innovation Can Drive Growth and Create Jobs", The Lisbon Council, *Progressive Policy Institute*, Issue 15/2014.

<https://copyrightalliance.org/sites/default/files/resources/2013-localization-barriers-to-trade.pdf>

GOLDFARB, A. & TUCKER C. E. (2011): "Privacy Regulation and Online Advertising," *Management Science*, Vol. 57 (2011), No. 1, p. 68.

IDATE (2014): *Digiworld Yearbook 2014, Les Enjeux du Monde Numérique*.

LLOYD M. (2012): "Data Protection in the EU: The case for a re-think", Confederation of British Industry, Competitive Markets Directorate.

http://www.cbi.org.uk/media/1356711/cbi_response_data_protection_in_the_eu_fe_b_2012_.pdf

MOVIUS, L. B & KRUP N. (2009): "US and EU Privacy Policy: Comparison of Regulatory Approaches", *International Journal of Communications* 3 (2009), 169-187

Office of the United States Trade Representative (2014): "2014 Section 1377 Review On Compliance with Telecommunications Trade Agreements"

<http://www.ustr.gov/sites/default/files/2013-14%20-1377Report-final.pdf>

PYYKKO E. (2012): "Data Protection at the Cost of Economic Growth?", European Credit Research Institute, *ECRI Commentary* N°1, Nov.

TADDICKEN M. (2013): "The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance of Different Forms of Self-Disclosure", *Journal of Computer-Mediated Communication*, Vol. 19, Issue 2, 248-273.

UK Ministry of Justice (2012): "Proposal for a EU Data Protection Regulation – Impact Assessment (IA)", 22 Nov.

<https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/eu-data-protection-reg-impact-assessment.pdf>