POLICY PAPER 204 7 SEPTEMBER 2017

JACQUES DELORS INSTITUT
BERLIN

# BALANCING AMBITION AND PRAGMATISM FOR THE DIGITAL SINGLE MARKET

Paul-Jasper Dittrich | *Research Fellow at the Jacques Delors Institut – Berlin*

## SUMMARY

This paper critically evaluates the progress of the Digital Single Market Strategy and puts forward policy recommendations for upcoming digital policy challenges in the Single Market. The debate on the effectiveness of the Digital Single Market is crucial: The EU is still lagging far behind other countries and regions when it comes to digital cross-border trade, digital skills, innovative regulation and investment in digital infrastructure. It is widely acknowledged that this is to a large extent the result of a fragmented Single Market, which hinders digital trade between EU-countries and hampers the scaling up of young European digital platforms and start-ups.

The first part of the paper therefore examines the DSM strategy so far and takes a more detailed look at the Midterm Review of the strategy published in May 2017. It concludes that some of the success stories the Commission highlighted in its midterm review are of more symbolic than real economic value for European consumers. But the general criticism of the DSM strategy goes further: instead of helping to alleviate fragmented markets, it suffers from over-regulation, vested interests and a general lack of economic liberalization. It is unclear whether the strategy as it stands will lead to the expected economic gains.

The second part of the paper adds policy recommendations for upcoming digital policy challenges in the DSM framework: cyber security, platform regulation and the European data economy. All three of them are of great importance for the future economic integration of the Union and should therefore be approached with the ambition of fostering economic integration and the pragmatism to regulate only where necessary.

- Regarding the European data economy and the free flow of data, the Commission should urge Member States to abolish as many data localization measures as possible while at the same time guaranteeing the privacy rights of European citizens.

- The regulation of platforms should not target non-European platforms, but instead focus on the conditions in which European digital platforms can grow faster.

- In order to correct market failures, the EU should also hasten to develop harmonized rules and standards for product security in the Internet of Things.

# TABLE OF CONTENTS

# INTRODUCTION: CONFRONTING THE EU'S DIGITAL BACKLOG

The internet is borderless by definition. Information and data flow freely and have the potential to be used, stored, analysed and multiplied *ad infinitum*. The combination and re-use of information and data allows for constant innovation and the creation of new business models on a daily basis. The emerging platform economy and network effects accelerate the speed of this expansion: start-ups are able to scale up into globally dominant digital platforms within a few years, if they find the right regulatory preconditions in place.

> "ONLY FOUR PERCENT OF ALL DIGITAL SERVICES CONSUMED IN THE EU ARE SOLD CROSS-BORDER."

The EU, with the largest Single Market in the world, could theoretically be an ideal place to found and develop global digital champions of the likes of Facebook, Alibaba or Google. Yet the reality of the European digital economy and digital trade is rather different, as market fragmentation still prevails. Only four percent of all digital services consumed in the EU are sold cross-border, yet more than 50 percent are provided by American digital companies.[1] The European Single Market has turned out not to be borderless at all when it comes to the regulation of digital services, products and information flows across European borders.

In order to stem the tide, the European Commission has made the digital overhaul of its Single Market a No.1 priority and put many resources into its Digital Single Market (DSM) Strategy. At the onset of the strategy in May 2015, the Commission did not shy away from raising large economic expectations: the economic gains from full execution of the DSM strategy were estimated to be as high as up to €415 billion per year.[2] The core of the strategy consists of 16 key measures (and even more accompanying policy initiatives) in different policy areas, which were gradually launched between May 2015 and November 2016 (see table on the next page for an overview). New rules for businesses and fewer restrictions on cross-border consumption should "unlock the digital potential of Europe".

**The DSM, a mix of ambition and pragmatism**

Does the DSM strategy deliver on its promise? According to the midterm review published in May 2017, it is on the right track.[3] In the report, the Commission highlights success stories and the role of the General Data Protection Regulation (GDPR), which is not an integral part of the DSM strategy itself. The report also outlines three policy areas for which the Commission will present policy proposals during the autumn of 2017 (data economy, platform regulation and cyber security). The GDPR will enter into force in May 2018 and act as an "overarching dome". One harmonized European data protection regime is thought to be preparing the ground on which the initiatives of the DSM can unfold their potential. If the negotiations are successful, the Commission hopes to complete the strategy by 2019.

1. European Commission, Why we need a Digital Single Market, Fact Sheet.
2. European Commission, Digital Single Market. Bringing down barriers to unlock online opportunities. Homepage of the European Commission.
3. European Commission, Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy. A Connected Digital Single Market for all, May 2017.

**TABLE 1 ► Overview of key measures and policy initiatives of the Digital Single Market Strategy**

| POLICY AREA | MAIN PROPOSALS[4] |
|---|---|
| Access | Cross-border E-commerce: Harmonization of VAT and consumer protection, better enforcement of consumer rights, harmonized parcel delivery, end of "unjustified" geo-blocking<br>Temporary portability for audio-visual content across EU-borders<br>A reform of copyright legislation |
| Network Environment | Telecoms Single Market: Modernization of EU telecoms legislation<br>Data Protection and Privacy: Modernization of EU data privacy legislation (E-Privacy Directive)<br>Measures on Cyber Security<br>Inquiry into Online Platforms |
| Growth | Promote Digital Skills<br>Free Flow of Data: Abolishing barriers to the flow of data across Europe, European Cloud Initiative<br>Definition of Inter-Operability Standards |

However, despite the self-praise, the reality of the DSM is not fully keeping pace with the ambition. The "success stories" of the Digital Single Market presented in the DSM Review of May 2017 appear to be rather low-hanging fruit in terms of economic integration: the abolishing of roaming charges, temporary portability for audio-visual content and the initiative for public Wi-Fi have high symbolic and communicative value, but do not significantly deepen the Single Market (section 1). The matters currently under negotiation between the Parliament and the Council are more ambitious, but they run the risk of being diluted by over-regulation and distorted by vested interests. Regulatory overlap in some cases and a general lack of focus on economic liberalization add to the list of the inadequacies of the current DSM strategy (section 2).[5] More than two years after its launch, it appears unlikely that the DSM strategy will meet its ambitious economic goals. Integration via market regulation prevails over integration via market creation. Instead of enhancing Europe's potential, parts of the strategy could turn out to hamper innovation and drive young innovative companies in some sectors out of the EU.

Future policy proposals should therefore be designed with pragmatism and geared towards integration via market creation, with less market regulation. The emerging policy fields identified in the report (for which proposals are slated for the fall of 2017) are "tough nuts" in this regard. They are economically highly important for a functioning Single Market yet politically controversial, and should be handled with the right mix of ambition and pragmatism: cyber security, platform regulation and, in particular, the free flow of data will be detrimental to the successful completion of a truly Digital Single Market (section 3).

# 1. "Success stories" of mainly symbolic value

Three achievements are highlighted in the Midterm Review as an early "triple win for EU-consumers" from the DSM strategy: the abolishing of roaming charges, the envisioned temporary portability for audio-visual content and Wifi4EU, and an investment project intended to help communities to establish free Wi-Fi capacities in major European cities in the coming years.[6] Against the backdrop of the ambitious goals of the DSM, however, the actual welfare gains for European consumers and opportunities for companies from these successes appear limited. While all three projects have high symbolic value, their impact in terms of economic integration and market liberalization is low.

### Roaming, portability and Wifi4EU: low-hanging fruit?

**Roaming charges:** After a lengthy process that started as early as 2007, roaming charges have been abolished since mid-June 2017. Tourists and business people can finally use their mobile phone subscriptions at almost the same prices as in their home countries. While the abolition of the charges is an important symbolic step for the physical coalescing of the Union, it is only a small step in terms of economic integration and market creation. It does not tackle the initial reasons for the very different prices: market fragmentation in the telecommunication services sector

4. A full overview over the Commission's 16 key measures and policy initiatives can be found here.
5. See on this point also Enderlein, Henrik, P-J Dittrich and D Rinaldi (2017), "#DigitalAmitié, A Franco-German axis to drive digital growth and integration", Jacques Delors Institut, 10 March 2017.
6. European Commission, Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy. A Connected Digital Single Market for all, May 2017.

across the EU, which in turn is the result of different wage and price structures ranging from Luxembourg to Bulgaria. Market fragmentation has a negative impact on investment in modern communication infrastructure. The EU can rightly claim a European success which affects millions of Europeans every day. Still, a much more important factor for the future of European competitiveness is major investment in communication networks. Without it, it will be difficult to roll out 5-G services in time and profit from next-generation access services and products.

> "THE TOTAL NUMBER OF CITIZENS POTENTIALLY BENEFITING FROM A (TEMPORARY) END TO GEO-BLOCKING IS LOW."

**Temporary portability:** The move to partly end geo-blocking for audio-visual content offers a similar combination of high symbolic value and low economic integration. The proposed changes make audio-visual content partly portable. European consumers can access their "home" subscriptions from on-demand providers like Netflix temporarily when they are abroad on a holiday or business trip. While this will certainly be welcomed by many European citizens, especially frequent travellers, it does not affect the majority of Europeans in their day-to-day lives. A 2016 report for the European Parliament estimates that between 900,000 and a maximum of 5.4 million Europeans per day will potentially benefit from the "roaming for Netflix" proposal for portability, depending on the specific details of the directive.[7] A Eurobarometer poll in 2015 revealed that 54 percent of subscribers to on-demand services have never tried to use their service in another Member State and do not intend to do so in the future. According to the same survey, only 20 percent of European internet users are subscribers to on-demand services, so that the total number of citizens potentially benefiting from a (temporary) end to geo-blocking for copyrighted material is low.[8]

Would it help if pan-European licensing were introduced instead, to offer all Europeans access to the entire audio-visual content of the EU? It appears that, due to language and cultural barriers, interest in works from other countries is astonishingly low in general. Few European Internet users (eight percent) have tried to access content through online services generally meant for users in other Member States, most usually audio-visual content (five percent).[9] Audio-visual content might therefore only be a matter of secondary importance as regards integration in the Single Market.

**Wifi4EU:** The object of this initiative is to provide some 6000 European municipalities with high-speed, free-access Wi-Fi hotspots in public squares or public buildings via EU-grants and public-private partnerships. Investment in fast broadband and transmission technology is generally more than welcome as it increases the long-term potential for economic growth. The EU is also to a large extent lagging behind in the deployment and proliferation of fast internet connections, especially in public places. However, the Wifi4EU framework, with a budget of only €120 million, cannot really achieve much to remedy this situation. Hastily stitched together in the run-up to Jean-Claude Juncker's state of the Union speech in November 2016 (in which the program was revealed), the under-funded initiative might be no more than a drop in the ocean.[10]

Summing up, the success stories of the DSM strategy presented by the Commission in the midterm report were low-hanging fruit: easy to pick and easy to sell owing to their highly symbolic or tangible value to the European consumer / citizen, yet without much to offer for a truly integrated Single Market for digital services.

## 2. Four criticisms of the DSM strategy

The bulk of the DSM strategy is at the moment midway through the ordinary legislative procedure. Having been proposed by the Commission between 2015 and 2016, the initiatives of the 16 policy measures are being negotiated between the Council and the Parliament. Among them are proposals to modernize copyrights, harmonize various rules for European e-commerce, facilitate parcel delivery and level the playing field between

7. Felice Simonelli, DIRECTORATE-GENERAL FOR INTERNAL POLICIES POLICY DEPARTMENT A: ECONOMIC AND SCIENTIFIC POLICY Combating Consumer Discrimination in the Digital Single Market: Preventing Geo-Blocking and Other Forms of Geo-Discrimination, Study for the European Parliament, June 2016.
8. Flash Eurobarometer 411, Cross-Border Access to Content, Report of August 2015.
9. Ibid.
10. Thomas Flanagan, EU wins approval to waste €120m on pitiful public Wi-Fi, The Register, 5 June 2017.

telecommunication operators and OTT-players such as WhatsApp or Telegram. The Commission would like to see negotiations completed by 2018.[11]

This timetable has, however, been brought into question. Even though all of the proposals were delivered on time by the Commission, it is quite unlikely that the time frame can be held to. Past examples point to a different experience: the now much-touted abolishing of roaming charges was in fact a very gradual process which was around ten years in the making.[12] Given the rapid pace of current online and digital innovation, the DSM proposals should be finalized quickly or else they will be outdated by the time of their transposition into national law. Hopes rest at the moment on the Estonian presidency of the EU Council: many commentators expect that the tech-savvy government of Estonia will seek to find compromises on some of the more controversial dossiers by the end of 2017.[13]

There are also more general criticisms. Despite initial praise from the business community, national governments and interest groups for the ambitious scope of the strategy, criticism from different sides is now mounting. While the intentions and aims of its critics differ, the objections to parts of the DSM-strategy can be loosely grouped into four categories: 1) over-regulation; 2) succumbing to national or industry interests; 3) creation of regulatory overlap; and 4) lack of real economic liberalization.

## 2.1. Over-regulation and vested interests

> "IT WOULD BE MISGUIDED TO TRY TO FORCE REGULATION FROM AN ANALOGUE ERA ONTO NEW BUSINESS MODELS."

In a world where the copying, re-mixing and distribution of protected works have become much easier, it would be misguided to try to force regulation from an analogue era onto new business models. Yet the proposals to modernize copyright in the Union and adapt it to new technical realities are a good example of the kind of over-regulation and vested interests within the DSM framework, which does just that.[14] One concrete example is the introduction of ancillary copyrights for press publishers which were included in the Commission proposal largely under pressure from the European publishing industry. If an ancillary copyright (a "link tax") is introduced as provided for by the Commission, it will be much harder for young companies with innovative tools for news aggregation or media services to scale up and challenge larger incumbent players which have the resources to share their advertising revenue with publishing companies from the start.

The copyright proposals are also worrying for what they do not include in terms of a forward looking, inclusive and more modern copyright. The "freedom of panorama" is not included and remix culture and fair use cases are not adequately addressed.[15] What is also lacking is a modern take on internet phenomena such as memes or gifs. On the contrary, the proposals as they stand could make the creation of a meme or a gif an illegal copyright infringement if they include copyrighted material even in a standstill.[16] An example of the power of (national) vested interests is the Audio-Visual Media Services Directive (AVMSD): in an attempt to harmonize rules between traditional broadcasters and new over-the-top players such as on-demand video platforms, instruments such as quotas for national content on the platforms will be introduced in an attempt to protect national movie industries.[17]

## 2.2. Regulatory overlap and lack of economic liberalization

Regulatory overlap and confusing or contradictory policy proposals are other aspects of the DSM strategy which are often criticized. A case in point is the relation between the General Data Protection Regulation and the e-Privacy Regulation, which are partly at odds with each other. Where the GDPR, for example, asks for explicit user consent in order to allow tracking activities, the e-Privacy Regulation allows tracking without consent in certain

11. European Commission, Commission publishes mid-term review of the 2015 Digital Single Market strategy, 10 May 2017.
12. Gonzi & Associates Advocates, The Abolishment of Roaming Charges, Lexology, 14 November 2016.
13. Arne Koeppel, Stephen Jackson, Estonian EU Council Presidency: Great Expectations, FTI Consulting, June 2017.
14. Natasha Lomas, EU digital copyright reform proposals slammed as regressive, TechCrunch, 14 September 2016.
15. Copyfighters: Position paper on a modern copyright reform, May 2017 Position paper for EuroDIG.
16. Cynthia Kroet, Influencers: digital single market performance worst on copyright, cross-border data, Politico, 9 May 2017.
17. Catherine Stupp, MEPs raise Netflix quota to 30% and sharpen rules on violent online posts, 26 April 2017.

cases.[18] Worries about the regulatory overlap are so prevalent that the Commission has postponed the date of implementation of the e-Privacy Regulation (initially planned to be on the same date as the GDPR in May 2018).

The harshest critique of the entire DSM strategy, however, is its lack of real progress on economic liberalization and of measures to complete the Single Market.[19] Aside from the proposals for e-commerce, which would likely increase online cross-border trade in goods and services significantly, few of the proposals for the DSM will actually lead to integration via market creation. It remains to be seen if the promise of €415 billion per year in additional GDP can be kept with the proposals as they currently stand. The largest chunk of this increase in GDP is expected to be brought about through a more harmonized market for e-commerce and parcel delivery.[20] However, even if e-commerce harmonization delivers high welfare gains, it is questionable whether the current DSM-strategy will unlock €415 billion of additional GDP growth per year.

## 2.3. Aligning ambition and pragmatism

In short, many of the initiatives in the DSM strategy suffer from over-regulation, are ambiguous and generally lack elements of economic liberalization. Parts of the regulation will certainly harm innovative business models. An example is the growing number of text- and data-mining start-ups, which will probably have to leave the EU for the US under the current proposals for copyright. This is an unnecessary waste of potential. The EU should not prematurely forgo the possibilities that its Single Market offers for digital services to flourish and young start-ups to grow. Instead it should re-align its priorities.

- Economic integration should take centre stage: future policy proposals within the framework of the Digital Agenda and the Digital Single Market should be more pragmatic and set economic integration and the creation of new business opportunities and markets as the focus of ambition.

- The upcoming policy challenges – cyber security, platform regulation and the "free flow of data" – are crucial: they can add important pieces to a framework for the future success of the European digital economy. The EU should aim for regulation that allows young companies to grow and innovative business models to thrive in a secure environment, which at the same time respects Europeans' needs for privacy. Regulations should only be issued if absolutely necessary in order to avoid the mistakes of over-regulation.

# 3. Emerging tough nuts: data localization, platform regulation, cybersecurity

## 3.1. Three initiatives of high relevance for economic integration

In autumn 2017 the Commission is expected to present key measures in three highly relevant digital-related policy areas: new proposals for how to achieve a higher level of cybersecurity, for the regulation of online platforms in the EU and for the European data economy (especially regarding the "free flow of data"). If tackled in an open and pragmatic way, they can contribute to the development of infant digital industries, create new markets and help to make the European digital economy more secure.

- *Data economy.* If the Commission comes forward with a strong and concrete proposal relating to the free flow of data, possibly acknowledging it as the "fifth freedom" of the Single Market, it would significantly strengthen the European data economy. Such a step would create many new business opportunities for young companies and make the exchange of data much more efficient. However, data protection and privacy concerns should be addressed properly, in order not to lose public trust in the EU's capacity to guarantee a high level of protection of personal data.

18. Matthew Sullivan, Preparing for e-Privacy Regulation in the European Union, Lexology, 12 June 2017.
19. Hosuk Lee-Makiyama, Philipp Legrain, Open Up. How to fix the flaws in the EU's Digital Single Market. OPEN, January 2017.
20. Civic Consulting, Contribution of the Internal Market and Consumer Protection to Growth, Report to the European Parliament, 2014.

- *Platform regulation*. With the new regulation of online platforms and digital marketplaces, the EU seeks to address unfair business practices and enable fair competition between existing players in the platform economy.[21] But such steps will most likely not solve the problem of the EU lagging behind in growth and global dominance as regards digital platforms. A forward-looking policy mix for platforms should thus not only attempt to draw up new rules for existing platforms, but also be designed to help European platforms scale up faster.

- *Cybersecurity*. Cyber-attacks already cost European industries and economies billions of euros, even though determining the exact costs is tricky.[22] The emerging Internet of Things (IoT) could further degrade the security situation, if the EU does not take swift and pragmatic action. Higher security standards are especially needed for the upcoming Consumer Internet of Things (CIoT). Since the EU has a clear mandate to regulate in the event of market failures, the Commission should make regulation towards higher product and IT-security for IoT a top priority of its cyber strategy.

## 3.2. Countering the trend of data localization

The amount of data produced daily is growing at an exponential rate, and the economic importance of data as a resource for companies and governments is constantly growing with it. The analysis of large troves of data facilitates new production processes and inspires new business models in almost every industry. As citizens, consumers and patients, many people in the EU are already benefiting from these developments.

> "IN RECENT YEARS, EUROPEAN MEMBER STATES HAVE ISSUED MORE AND MORE RESTRICTIONS ON THE FREE FLOW OF DATA."

Digital information is an intangible and non-rival good. Data can be easily stored, processed and analysed wherever it is considered most efficient to do so. Within the European Union this means that data flows regularly across borders or is stored in only one Member State. In recent years, however, European Member States have issued more and more restrictions on this free flow of data. Following a worldwide trend, governments force companies to store data within the country where it is accrued. Data that has to be stored nationally is usually considered too sensitive by the government concerned to be allowed to be stored outside its own jurisdiction. However, the definition of "sensitive data" differs widely within the EU: some countries consider health or accounting data to be sensitive, others require data on online gambling to be stored locally.[23] The new German law on data retention requires telecommunication companies to temporarily store communication data on German servers. This fragmentation of the Single Market by data localization measures is costly, especially for start-ups. Young companies might have to rent additional server capacities or even invest in infrastructure in every Member State just to comply with the localization measures. Forced localization also means that companies are less able to experiment with pooling data in order to create new insights and, potentially, new services for consumers.

**Can and should data become the fifth freedom?**

A Digital Single Market without restrictions on cross-border data flows would gain economic benefits: the European Centre for International Political Economy has calculated that a "free flow of data" would create a significant ramp-up in digital trade between Member States. Besides lower costs for data storage in the EU, companies would be able to offer their digital services much more easily on a cross-border basis. The ECIPE estimates the efficiency gains from increased digital trade within the EU at €8 billion per year.[24] It is estimated that 0.08 percent of economic gain would be generated by more efficient use of data servers, more possibilities for small companies to set up their operations across the Single Market and fewer overall costs due to higher competition among data centres across the EU.

- Defend the "free flow of data": The Commission's proposals should include a forceful drive towards the abolishing of as many data localization measures as possible and should defend the free exchange of data

21. European Commission, Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy. A Connected Digital Single Market for all, May 2017
22. Enisa, The costs of incidents affecting CIIs. Systematic review of studies concerning the economic impact of cyber-security incidents on critical information infrastructures (CII), August 2016.
23. Matthias Bauer et al., Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States, ECIPE Policy Brief No 03/2016.
24. Ibid.

across European borders against the tendency of national governments to increasingly enforce data localization measures.

What is making national governments increasingly adopt data localization measures? The main arguments put forward against the abolition of data localization are privacy, data security outside the "home country" and concerns regarding state sovereignty over certain types of data. Within the EU, these concerns are voiced, for example, by the French or German administrations. While Germany is generally more concerned about storing sensitive data about its citizens outside Germany, owing to privacy and security issues, the French administration has voiced concerns over the free flow of data out of fear of losing sovereignty over the use and storage of data about its citizens.

**Addressing concerns about the "free flow of data"**

Both concerns are at least partly unfounded: it is to date unclear how exactly abolishing data localization measures would make data less secure, as that generally depends on the precautions taken by (usually) private storage facilities to secure data. Private companies offering server hosting or data storage services, on the other hand, have strong business incentives to keep their data as secure as possible. Generally, the new French administration under President Emmanuel Macron is expected to relax its opposition to letting data flow more freely between different EU Member States.[25]

> "UNDER THE 2018 GDPR, ONLY ONE DATA PROTECTION AUTHORITY WILL SUPERVISE CROSS-BORDER DATA-PROCESSING OPERATIONS BY ONE COMPANY."

Privacy is a more sensitive matter, but the General Data Protection which is coming into force EU-wide in May 2018 will probably clear most of the concerns out of the way: the new regulation states that private data, wherever stored in the EU, falls under the same harmonized level of protection. In its January 2017 Communication on "Building a European Data Economy", the Commission stresses that under the 2018 GDPR "there will be one single pan-European set of rules contrary to 28 national laws today".[26] There will be a one-stop-shop mechanism under which only one Data Protection Authority will supervise cross-border data-processing operations by one company. The GDPR is also important as it will create a single level playing field between the EU and foreign companies whereby foreign companies will have to abide by exactly the same rules as European companies when they process data about European citizens across borders.

There are also other concerns. The relationship between privacy and the "free flow of data" is an important aspect of the ongoing negotiations on the Trade in Services Agreement (TiSA). Some critics argue that the agreement, if it entered into force, could tear down the European level of data protection and allow the storage of even the most sensitive data (usually health-related data) in countries outside the EU.[27] At the moment, however, European officials are confident that TiSA will not allow a complete transfer of data to third countries.[28]

- Address privacy concerns up front: to increase public acceptance, the EU should make it crystal-clear that the "free flow of data" and the far-reaching TiSA-negotiations, which involve more than 20 countries around the world (in addition to the EU-28), will not water down any aspects of the GDPR.

## 3.3. Regulating platforms: pragmatic, sector-specific and innovation-friendly

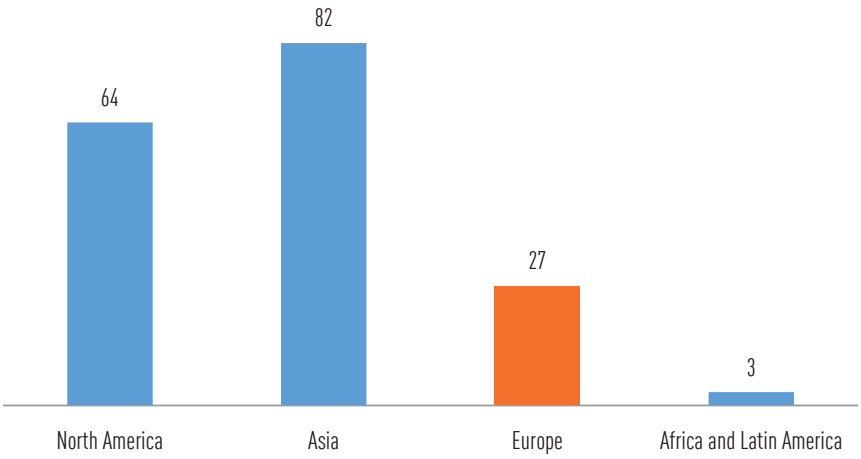
**Still no "European Google" in sight**

More and more services are being offered via platforms, online marketplaces using multi-sided business models, such as AirBnB, TaskRabbit, Uber or Zalando. This process has brought the regulatory environment for platforms into the focus of attention of policy makers around the world. The disruptive potential which online platforms (often non-European) carry into traditional sectors of the EU economy has so far been met with a mix of admiration and fear. In the EU, policy makers are worried about the dominance of American platforms in the

25. Brunswick, Digital Single Market Review. A last chance to deliver, May 2017.
26. European Commission, Building a European Data Economy, European Commission Communication, 10 January 2017.
27. Jane Kelsey, TiSA. Foul Play. Report prepared for UNI Global Union, 2017.
28. Catherine Stupp, European Commission paralyzed over data flows in TiSA trade deal, EurActiv, 11 October 2016.

European digital economy. A comparison of the key figures reveals why: a global survey of the platform economy since 2015 by the Global Enterprise Institute underlined how far the EU lags behind in the sheer number of platforms, market capitalization or the number of employees for digital platforms (see graphs on the next page). Brexit in 2019 will deal an even bigger blow to the EU's share of digital platforms as the United Kingdom is Europe's frontrunner in digital platforms.[29] The European Single Market is technically the largest market in the world, but it lacks crucial features: a harmonized legal environment and streamlined regulation, enabling platforms to scale up faster and more easily.[30]

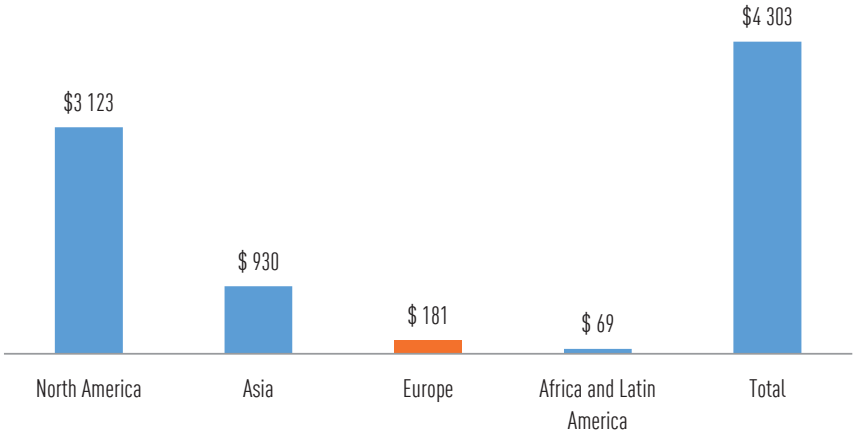
**FIGURE 1 ► Number of platforms worldwide with a market capitalization higher than $1 billion in 2015, by region**




Source: Peter C. Evans, Annabelle Gawer, The Center for Global Enterprise, 2015

Finding the right regulatory balance for digital platforms is important for the EU on an economic as well as on a (geo-) political level. The more economic power internet platforms such as Alibaba, Google or Amazon amass, the greater their global political clout becomes – in setting standards and norms for the future governance of the Internet, for example. Testimony to the new political power of internet platforms can be seen in actions such as the recent decision of the Danish government to appoint ambassadors to internet platforms or in the way Google or Amazon are trying to shape the outcome of the TISA-negotiations.[31] If the EU aspires to retain its standing as a global power in the setting of rules and standards in transnational commerce, it will have to do much more to nurture a European brand of global digital platforms.

**FIGURE 2 ► Market capitalization of platforms with a market capitalization higher than $1 billion in 2015, by region in $ billion**




Source: Peter C. Evans, Annabelle Gawer, The Center for Global Enterprise, 2015.

29. House of Lords, Online Platforms and the Digital Single Market, Report, 20 April 2016.
30. See on this point also H. Enderlein, P-J Dittrich and D Rinaldi (2017), "#DigitalAmitié, A Franco-German axis to drive digital growth and integration", Jacques Delors Institut, 10 May 2017.
31. Jane Kelsey, TiSA. Foul Play. Report prepared for UNI Global Union, 2017.

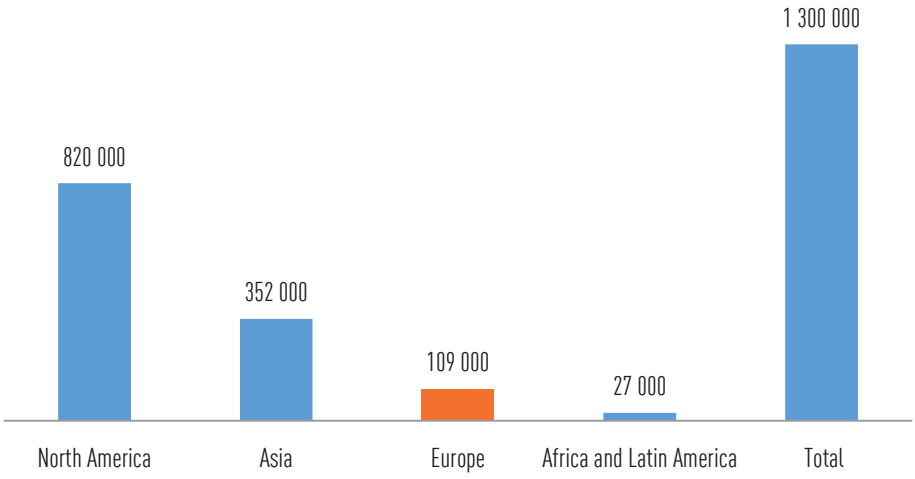
**Regulation should be sector-specific and help small European platforms to grow.**

At the same time, the urge to regulate digital platforms should not translate into neo-protectionist measures against American or Asian players. Large platforms like Google or Facebook do have worrying market positions similar to monopolies on certain markets. However, where there is abuse or the suspicion of it, European competition authorities are already investigating and imposing fines against platforms abusing their market position.[32] It is important to ensure fair business practices. However, the EU should also focus on preparing the ground for large European digital platforms which are able to compete on global markets through size and innovation.

- Tackle the definition and legal status of platforms: there is an ongoing debate as to whether the EU should classify platforms as "facilitators" of transactions or as the actual suppliers of a good and in what circumstances the platform could be made liable vis-à-vis one side of the transaction.[33] Making platforms liable for the actions of third parties on their platforms can be a double-edged sword: depending on the sector, it could potentially deal a blow to aspiring young companies if they had to fear intermediary liability claims; in a worst-case scenario it would even deter them from developing new and innovative services. Without an exemption from liability, American e-commerce platforms would never have enjoyed the growth rates they did in the '90s.[34] Regulation on platforms should always carefully take sector-specific features into account. Large platforms like Facebook, on the other hand, which some already consider to be the largest publisher and newspaper in the world, have different responsibilities towards societies. They can be forced to step up their actions against hate speech and other crimes by making them liable for the content posted on their platform.

- Address scaling-up problems: the Commission should put forward proposals to take some of the regulatory burden off European digital start-ups and platforms. The EU could, for example, encourage Member States to exempt start-ups from national regulation for five years after market entry via mutual recognition.

FIGURE 3 ► **Number of employees working for platforms with a market capitalization higher than $1 billion in 2015, by region**




Source: Peter C. Evans, Annabelle Gawer, The Center for Global Enterprise, 2015.

32. Mark Scott, Google Fined Record $2.7 Billion in E.U. Antitrust Ruling, New York Times, 27 June 2017.
33. Christoph Busch et al., The Rise of the Platform Economy: A New Challenge for EU Consumer Law, 5 (2016) Journal of European Consumer and Market Law 3 (Publisher: C.H.Beck). Available at SSRN.
34. Anupam Chander, Internet Intermediaries as Platforms for Expression and Innovation, Global Commission on Internet Governance Paper Series No. 42 – November 2016.

## 3.4. Securing the Internet of Things on a European level

### Which part of "cyber security" should the EU address?

Cyber security has become a No.1 policy priority across the Western World in recent years, owing to widespread cyber theft, cyber-attacks by foreign powers and attempts to influence election outcomes via social media manipulation.[35] The challenges and policy questions surrounding cyber security have become so diverse and extensive in recent years that it has become somewhat unclear which specific kind of cyber security is actually being referred to in a given situation. Instead of one, there are at least three main debates and policy areas surrounding cyber security (see the table on the next page): IT /product security for the Internet of Things (IoT), questions regarding the protection of critical infrastructure and issues related to the foreign-policy or security-policy dimensions of cyber security (election hacking etc.). In addition to clarifying the role of its own cyber security agency, ENISA, the EU should make security for IoT products a No 1 priority.

"IN PRODUCT SECURITY FOR THE IOT THERE IS A CLEAR CASE FOR EU-WIDE REGULATION."

- Focus on product security for IoT: At the moment product and IT security seems to be the only policy area where the EU has a full mandate to enact regulation for the Single Market. In product security for the IoT there is a clear case for EU-wide regulation. The current situation in the market for IoT devices, especially in the consumer sector, constitutes a case of market failure. The market delivers no incentives for producers to produce safer connected devices or for consumers to demand them. If private routers are turned into a botnet by criminals in order to execute DoS attacks on a network, their owners are rarely even aware of it and producers are not liable for any damage caused by their products. The resulting harm to society can thus be considered a negative externality, which should be corrected for the entire Single Market.

The protection of critical infrastructure and the developing of policy responses to cyber-attacks by foreign governments are more political in nature. They touch upon the national sovereignty of each Member State. Subsidiarity concerns are therefore much higher than with the more economic question of product security for IoT.

TABLE 2 ► Overview of different aspects of cyber-attacks in the EU

| THREAT | POLICY AREA | MAIN AGGRESSOR | POSSIBLE ROLE FOR EU |
|---|---|---|---|
| Extortion, theft | IT security, product security | Criminals, mainly private actors | Regulation in the Single Market via standards; long-term: possibly a product liability regime |
| Attack on critical infrastructure | National security, infrastructure security | Private and state actors | Coordination, pressure on governments to act; long-term: beefing up of own reaction capabilities (ENISA) |
| Cyber espionage, PsyOps | Foreign policy, security policy | Mainly state actors | Coordination, establishing a response mechanism; long-term: developing own systems |

### How to make IoT more secure in the EU?

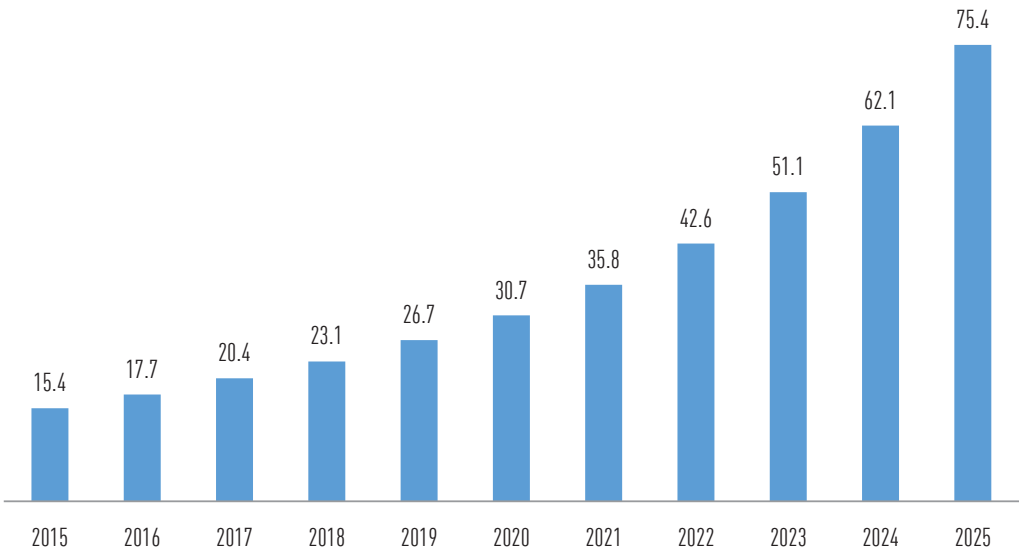
The number of connected devices is expected to grow rapidly worldwide in the next few years (see graph on next page). Such growth rates make policy questions concerning their security even more important. A more secure Internet of Things will thereby not only substantially reduce harm inflicted on European societies by cyber attacks. It can also increase the acceptance of connected devices for consumers. This will in turn allow an even faster expansion of the emerging economy around connected devices and services in the EU.

35. Arthur Beesley, EU suffers jump in aggressive cyber-attacks, Financial Times, 8 January 2017.

> "IS PRODUCT LIABILITY REALLY THE BEST ANSWER FOR THE EU AT THE MOMENT? NOT NECESSARILY."

How can regulation help reduce the negative externalities created by unsecure connected devices? Several policy options are available. In order to increase product security, the EU could force producers to develop standards, issue security labels or introduce a liability regime for producers. The idea of extending product liability to connected devices has its proponents among European policy-makers. After several high-profile cyber-attacks in 2016 and 2017 used botnets made out of CIoT devices, national and European politicians demanded an extension of product liability to producers of internet-enabled devices.[36] The Commission has already addressed the question in its Communication on "Building a European Data Economy".[37] It has promised to clarify whether the current set of rules regarding product liability (for example, the "defective product liability directive" of 1986) is still fit-for-purpose in an IoT environment. The answer will most likely be no. Connected devices and their complex interplay of software and hardware will probably demand a complete re-drafting of liability rules. But is product liability really the best answer for the EU at the moment? Not necessarily. Due to the complexity of the production structure for connected devices (with hardware and software producers as well as intermediaries and distributors), the need for constant updating of software and phenomena like open-source software, the ultimate question of "Who is liable?" is much harder to answer in the case of connected devices in the Internet of Things than for analogue products. Instead of extending product liability, it might be more rewarding to commit producers to common standards first.

**FIGURE 4 ► Estimated number of connected devices worldwide, in billion, from 2015 to 2025**




Source: IHS, IoT Platforms: enabling the Internet of Things, March 2016.

- Standards before liability: a hasty introduction of an ill-fated product liability regime for IoT-devices might be not advisable. It will be more important to obligate producers to set security standards first (for example, on regular updates for the software of their connected devices). Despite political pressure and the rapid development both of the IoT-sector and in the distribution of malware and other hacking tools, a pragmatic approach to more cyber security within the Single Market should be to force producers to adopt common standards before introducing a liability regime.[38]

36. For example in Germany: Deutschlandfunk, Klingbeil fordert, dass Hersteller von Routern haften, Interview with German public radio on 29 November 2016.
37. European Commission, Building a European Data Economy, European Commission Communication, 10 January 2017.
38. Hans-Jürgen Kleinhans, IT-Sicherheit im Internet der Dinge. Handlungsoptionen für Politik und Gesellschaft, Stiftung Neue Verantwortung, November 2016.

## CONCLUSION

The EU is lagging far behind other countries and regions when it comes to digital cross-border trade, digital skills, innovative regulation and investment in digital infrastructure. It is widely acknowledged that this is to a large extent the result of a fragmented Single Market, which hinders digital trade between EU countries and hampers the scaling up of young European digital platforms and start-ups.

The DSM strategy was designed to tackle these problems. Yet in its current form it does not seem to thoroughly address most of the more urgent problems of Europe's digital economy. Some of the success stories the Commission highlighted in its midterm review are of more symbolic than real economic value for European consumers. Instead of helping to alleviate fragmented markets, the DSM suffers from over-regulation, vested interests and a general lack of economic liberalization.

The Commission has announced policy proposals for important digital policy areas in autumn 2017: cyber security, platform regulation and the European data economy and, in particular, the free flow of data. All three of them are of great importance for the future economic integration of the Union and should therefore be approached with the ambition of fostering economic integration and the pragmatism to regulate only where necessary. As regards the free flow of data, the Commission should urge Member States to abolish as many data localization measures as possible while at the same guaranteeing the privacy rights of European citizens. The regulation of platforms should not target non-European platforms, but instead focus on the conditions in which European digital platforms can grow faster. In order to correct market failures, the EU should also hasten to develop harmonized rules and standards for product security in the Internet of Things.

On the same themes...

#DIGITALAMITIÉ A FRANCO-GERMAN AXIS TO DRIVE DIGITAL GROWTH AND INTEGRATION
Henrik Enderlein, Paul-Jasper Dittrich and David Rinaldi, Policy Paper No. 187, 30 March 2017

RESKILLING FOR THE FOURTH INDUSTRIAL REVOLUTION. FORMULATING A EUROPEAN STRATEGY
Paul-Jasper Dittrich, Policy Paper No. 175, 3 November 2016

GROWTH AND EURO AREA STABILITY: THE DOUBLE DIVIDEND OF A DEEPENED EUROPEAN SINGLE MARKET FOR SERVICES
Anna auf dem Brinke, Katharina Gnath, Jörg Haas Background Note, 26 June 2015



NOTRE EUROPE JACQUES DELORS INSTITUTE
Hertie School of Governance

Pariser Platz 6, D – 10117 Berlin
19 rue de Milan, F – 75009 Paris
office@delorsinstitut.de
www.delorsinstitut.de