Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 30

Digital Market Liberalization in the EU and the US: Where competition law, trade law, and privacy meet

Nikolaos Theodorakis

2017

TTLF Working Papers

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology-related and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Nikolaos Theodorakis is a Lecturer and Fellow at the University of Oxford and an associate with Alston & Bird LLP, focusing on issues of privacy and data protection, technology, international trade law and competition law.

Nikolaos completed his Ph.D. at the University of Cambridge, where he focused on issues of Corporate Compliance, Liability and Regulation. He also holds degrees from the University of Athens (LL.B.), University of Cambridge (M.Phil.), University of Oxford (PGC), London School of Economics (B.Sc.) and University College London (LL.M.).

Prior to joining Oxford, Nikolaos taught and conducted research at the University of Cambridge, Harvard Law School, and Columbia Law School. Nikolaos has further worked for the U.S. Committee on Capital Markets Regulation, the Legislative Committee at the U.S. Congress and the Library of Congress, and the UK Sentencing Council. Nikolaos has received fellowships and awards from the ESRC, the British Academy, the Greek Parliament, the Greek State Scholarships Foundation, the EU Bursaries and the Corfield foundation, among others. He has published papers on various topics and presented extensively in conferences and symposia.

Nikolaos's recent engagements include serving as a UN international consultant and legal trainer, an OECD expert, an EU Commission international expert, and a Transparency International country assessor. In the past he has also assumed research and teaching fellowships with Harvard University, the Institute of Advanced Legal Studies at the University of London, the British Institute of International and Comparative Law, and the Max Planck Institute of Foreign and International Criminal law.

General Note about the Content

The opinions expressed in this paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum or any of its partner institutions, or the sponsors of this research project.

Suggested Citation

This TTLF Working Paper should be cited as:
Nikolaos Theodorakis, Digital Market Liberalization in the EU and the US: Where competition law, trade law, and privacy meet, Stanford-Vienna TTLF Working Paper No. 30, http://ttlf.stanford.edu.

Copyright

Abstract

The digital market is constantly changing the global economy, yet it still suffers from restrictions that hinder its potential. Over-regulation, through the form of protectionism, often creates more red tape and makes compliance burdensome. Under-regulation, through inadequate or inconsistent laws, creates inefficiency and harms the consumers' trust to the digital economy. In both the EU and the US several legal fields try to regulate the digital market: competition law, trade law, and privacy.

This paper first discusses the benefits and the importance of the digital market to both the EU and the US. It then turns to specific legal challenges that the digital market faces: geo-blocking, that leads to protectionism and fragments the market, transatlantic data protection rules that create a gap between the heavily regulated EU and the less regulated US, and data localization requirements that are a global phenomenon on the rise. The paper finally examines a case study that practically demonstrates how competition law intertwines with privacy and trade in the digital sphere.

Keywords: Digital Market, Geo-blocking, GDPR, Data Localization, E-commerce

Contents

Digital Market Liberalization in the EU and the US

Where competition law, trade law, and privacy meet

1. Introduction

The digital market[1] is bound to completely change the way our world works. Developments such as the Internet of Things aim to interconnect every single device, increase efficiency and drive growth. Yet, the digital market still suffers from restrictions that hinder its potential, either because of protectionism or lack of technological standards consistency. Several legal fields try to regulate the digital market, in more or less successful ways: international trade law, privacy, and competition law.

Over the past years, both the European Union (EU) and the US have moved to regulate digital related activities, including e-commerce and data security. Some of these initiatives may affect access to digital trade services whereas others create further compliance requirements for companies. Finding the right balance is often an arduous task, whereas the EU and the US sometimes adopt a diverging approach. Taking the EU as an example, upcoming legislation like the General Data Protection Regulation (GDPR)[2] and the Payment

[1] In this Working Paper, digital trade is defined as providing products and services electronically over networks. This rather wide definition includes every online activity, within the boundaries of law, which generates revenue.

[2] *See:* http://www.eugdpr.org/

Services Directive 2 (PSD2)[3] regulate aspects of privacy, competition, and finance. However, such legislation may create am additional burden to US companies that wish to be compliant.

In some cases, over-regulation might hamper the true potential of the digital market (e.g. through geo-blocking and data localization). This is because over-regulation creates red tape, makes compliance more complicated, and reduces consumer and business welfare. In other instances, under-regulation (e.g. gaps in privacy and data protection) might equally lead to distrust towards digital trade and significant economic slowdown.

Issues like geo-blocking, transatlantic data protection rules, and data localization requirements, comprise part of the riddle of digital market liberalization. Apart from concerns relevant to international trade legislation, anti-competitive behavior, abuse of dominant behavior and data protection are equally involved. This working paper rests in the crossroad of these three legal fields, deciphering how they try to regulate the digital market and whether this effort has been successful. It also explores how different facets of digital trade regulation affect the EU and US markets going forward.

2. The Importance of the Digital Market in the EU and the US

The EU Digital Single Market strategy is arguably the most important EU initiative on digital trade.[4] It was adopted on 6 May 2015 and includes action points that aim to contribute to digital market liberalization. If completed, this aspirational EU plan could contribute 415 billion Euro per year to Europe's economy and significantly boost its economy.

The Single Market Strategy revolves around three pillars:

[3] For more information, see: https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en

[4] *See:* https://ec.europa.eu/commission/priorities/digital-single-market_en

- Access, that relates to better access for consumers and businesses to digital goods and services across Europe;
- Environment, that refers to creating the appropriate conditions and a level playing field for digital networks and innovative services to flourish;
- Economy & society, which relate to maximizing the growth potential of the digital economy.

Fewer restrictions on digital trade will benefit every party involved. According to estimates, the global e-commerce market is worth over EUR 1.2 trillion, with the market growing at a breathtaking pace of 20 to 25% per year.[5] According to European Commission (Commission) statistics, consumers in the European Union could save EUR 11.7 billion each year if they could choose from a full range of goods and services when shopping online.[6]

Also, digital trade is bringing down trade barriers. For instance, trade costs much less through online channels than for traditional transactions. Digital developments level the playing field between smaller and larger sellers. E-commerce enables even small businesses to reach customers across the globe, as if they were large corporations. Finally, newcomers can grow faster and survive longer when using an online model – which significantly boosts the economy.

Then what is the problem? The –currently- 28 member states of the European Union have different rules that govern digital trade. This discrepancy limits the growth experienced in Europe. Europe's leaders recognize the importance of addressing this inconsistency through the Digital Single Market (DSM). National security considerations also come in the picture, with Europeans often expressing concerns that the American intelligence agencies are

[5]Nielsen report, 2014, E-Commerce: Evolution or Revolution in the Fast-Moving Consumer Goods World? Available at: http://ir.nielsen.com/files/doc_financials/Nielsen-Global-E-commerce-Report-August-2014.pdf.

[6]Why we need a Digital Single Market, EU Commission factsheet, available at: http://ec.europa.eu/priorities/digital-single-market/docs/dsm-factsheet_en.pdf.

overusing national security exceptions. Conversely, developing a system of digital trade that is transparent and protects privacy for all parties will also be beneficial for every party involved.

Figure 1: EU statistics on the size of the Digital Market – Source: European Commission

The value of global technical standards is also relevant. For example, electronic prescriptions are widely used in Sweden, yet a person traveling to other EU member states will likely not be able to benefit from such service. Agreeing on technical standards that would allow cross-selling services and products throughout the EU will promote trade and increase growth altogether.

Business is currently facing strong headwinds in the form of economic slump, rising protectionism, loss of scale and interoperability. Private data flows are approximately 40% of global flows: they make up one layer of complexity. It is necessary to understand which sets of data are free to flow, and which are not. That way, effective regulation can ensure growth.[7]

Globally, B2C online sales are expected to grow by 17.7% in 2017, which demonstrates exactly the impressive growth. The rapid expansion of the Internet and use of mobile devices in emerging markets is a big part of the reason ecommerce is growing, along with better

[7] *See:* http://www.digitaleurope.org/Digital-Headlines/Story/newsID/490

payment options and advanced shipping. Emerging regions, including the BRIC countries, claim an important share of the e-commerce pie. In fact, China alone is expected to surpass the US ecommerce market.[8]

Today, only about 50% of US online retailers engage in cross-border ecommerce. The opportunity for new revenue is significant, however. As such, regulation facilitating ecommerce and motives to companies to engage in ecommerce activities can be instrumental in benefiting from this profitable channel.[9]

3. Digital Market Related Challenges in the EU and the US

Among other challenges, the digital market globally, and in particular in the EU and the US, is facing the following: (i) the restriction of access to websites based on location (geo-blocking);[10] (ii) Data protection and privacy requirements; and (iii) data localization and data storage requirements.

3.1. Geo-blocking restricts the reach of digital trade

Geo-blocking is the practice whereby users are either denied access to a website of a different country, based on their IP address, or they can access the website but cannot order goods shipped to their territory. Such restrictions may be the result of a company policy, a

[8] *See:* https://www.emarketer.com/Article/Global-B2C-Ecommerce-Sales-Hit-15-Trillion-This-Year-Driven-by-Growth-Emerging-Markets/1010575

[9] *See:* http://www.pitneybowes.com/us/global-ecommerce/case-studies/the-growing-importance-of-international-ecommerce.html

[10] In a geo-blocking scheme, the user's location is calculated using geo-location techniques (e.g., IP address). The result of this check will determine whether the system will approve or deny access to the content. Geo-blocking is widely used for multimedia content on the internet (e.g., movies, television shows), but also as a way to introduce price discrimination.

governmental policy, or both. Geo-blocking restricts market access, hampers trade and development, and limits the options that consumers have.[11]

For this purpose, the European Commission launched an antitrust inquiry in May 2015 into the e-commerce sector in the EU. The inquiry focused on potential barriers erected by companies to cross-border online trade in goods and services where e-commerce is most widespread, including trade in electronics, clothing and shoes, and digital content.

In March 2016, the Commission published its initial findings, which included replies from over 1400 retailers and digital content providers. The report showed geo-blocking to be common in the EU for both consumer goods and digital content: almost 4 out of 10 of the retailers selling goods (e.g., clothes, shoes, consumer electronics) and almost 7 out of 10 digital content providers (e.g., music or video broadcasting services) replied that they geo-block consumers located in other EU Member States.[12]

For consumer goods, geo-blocking takes the form of a refusal to deliver abroad (27%), refusal to accept foreign payment methods (22%), re-routing of the customer to other EU Member States (10%), and preventing access to a website (5%). For digital content providers, this is mainly done on the basis of the user's internet protocol (IP) address that identifies and gives the location of his or her computer or smart-phone.

[11]For instance, 74% of the complaints received through the European Consumer Centres Network regarding price differences or other geographical discrimination faced by consumers relate to online cross-border purchases. This translates into lower revenue for companies. It equally translates into a more restricted market and less liberty for consumers.

[12]*See:* http://europa.eu/rapid/press-release_MEMO-16-882_en.htm.

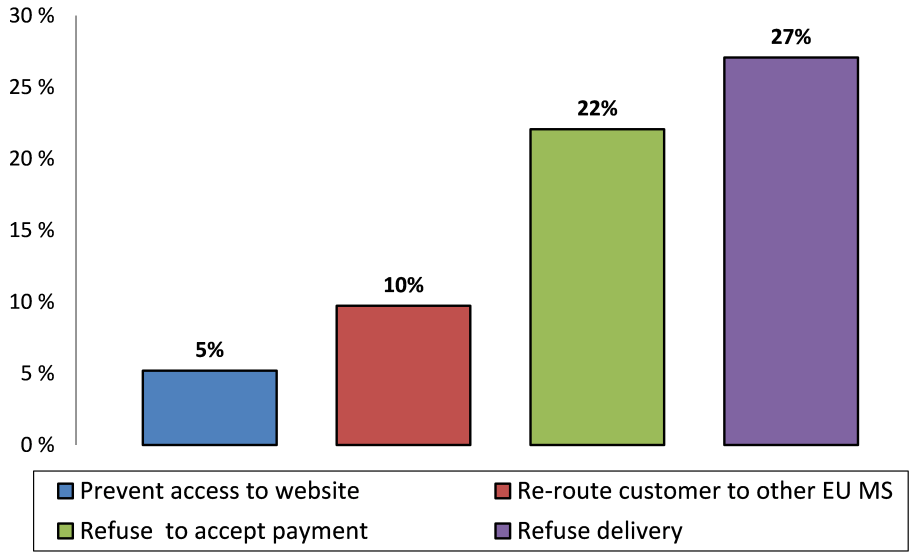

Figure 2: Types of Geo-blocking - Source: European Commission

In relation to geo-blocking overall, the report from the Commission finds an increasing trend in trading goods and services over the internet, yet disproportionately slow growth in cross-border online sales within the EU. Sometimes, geo-blocking appears to be linked to agreements between suppliers and distributors, which may be illegitimate, whereas in others it is a legitimate business decision. Remarkably, all types of content covered by the sector inquiry are affected to some extent by geo-blocking practices.

On 10 May 2017, the European Commission published its final report on the inquiry. As a result of the investigation, the Commission is currently finalizing a Regulation, along with the European Council and the European Parliament, which will aim to end unjustified geo-blocking. Such Regulation, expected to be effective in 2018, will be immediately effective throughout the European Union. With regard to the US, the EU has repeatedly expressed the necessity that the US must not apply geo-blocking to EU consumers depending on their location within the EU, when they use US e-commerce services.

In addition to its legislative efforts, the European Commission opened investigations in February 2017 into three sectors, regarding EU restricting collusive agreements.[13] The Commission is investigating geo-blocking in the video games, consumer electronics and holiday accommodation sectors. This investigation demonstrates in practice the interconnection between competition law, international trade law, and the digital market.

3.2. Transatlantic Data Protection Rules

Data Protection rules have been through significant changes in both the EU and the US over the past years. For instance, in the US there is no single, comprehensive federal law regulating the collection and use of personal data. Instead, the US has various state laws and regulations that may sometimes be overlapping. Guidelines and other self-regulatory instruments are also considered best practices- they have accountability and enforcement components that are increasingly being used as a tool for enforcement by regulators.

There are certain federal privacy-related laws that regulate the collection and use of personal data in several sectors. For instance, some apply to particular categories like health information (HIPA- Health Insurance Portability and Accountability Act), credit reports (FCRA- Fair Credit Reporting Act) and electronic communications (ECPA- Electronic Communications Privacy Act). In addition, there are wide consumer protection laws that are not privacy laws *per se*, but have been used to prohibit unfair or unlawful processing of personal data.

Few US states recognize an individual's right to privacy, a notable exception being California. The right to privacy is provided both in the California Constitution and in several pieces of legislation. The California Online Privacy Protection Act (OPPA) also provides requirements on operators which collect personal information. Recently, lawmakers have

[13] *See:* http://europa.eu/rapid/press-release_IP-17-201_en.htm

proposed legislation to amend the way online businesses handle user information. For instance "Do Not Track" aims to protect more the privacy individuals, however there has been no successful legislation that implements it yet.

The EU approach to data protection is quite different, and this discrepancy creates challenges for how the digital market operates across border. The EU mostly bases its privacy legislation on the European Directive on Data Protection, introduced in 1995. A dated piece of legislation nowadays, the Directive will be replaced by the EU General Data Protection Regulation (GDPR, Regulation 2016/679) in May 2018. This will be the most important change in data privacy regulation in twenty years. This Regulation is the EU's response to rising users' concerns about their privacy. In a recent EU survey, 72% of Internet users in Europe still worry that they are being asked for too much personal data online.[14]

The GDPR is intended to make citizens masters of their personal data, and to simplify the regulatory environment for international businesses. Personal data may range from a name, to a photo, email address, bank details, or a computer's IP address. The regulation applies to data controllers, data processors, and data subjects who are based in the EU. It provides for harmonization of data protection regulations throughout the EU and includes a strict data protection compliance regime. A notable provision is the extraterritorial reach of the GDPR, applying to companies outside the EU territory that process EU personal data. In combination with the very heavy fines, amounting up to 4% of global revenue or EUR 20 million, whichever is higher, this Regulation is a game changer in data privacy. The regulation does not extend to the processing of personal data for national security activities or law enforcement, however.

It remains to be seen how the GDPR will be implemented in practice since it requires comprehensive changes of business practices for companies that had not implemented a

[14] *See:* https://ec.europa.eu/commission/sites/beta-political/files/dsm-factsheet_en.pdf

comparable level of privacy before the regulation entered into force. The most interesting aspect is certainly the GDPR's its extraterritorial application, since it can apply even to US companies that process EU personal data.

For the purpose of bridging the different privacy approaches between the US and the EU, and to comply with the existing Directive, the U.S. Department of Commerce jointly with the European Commission developed a "safe harbor" framework. This framework recognized the US as an adequate country to transfer data, under certain safeguards. The safe harbor was later invalidated by the European Court of Justice. It was subsequently replaced by the EU-US privacy shield, the validity of which is also currently disputed in the EU courts.

In any event, the GDPR is changing the way companies process, transfer and otherwise use personal data. The EU-US digital market connection is becoming increasingly challenging, in terms of compliance, because of the regulatory chasm. The new Regulation creates significant opportunity to protect and grow the digital market, yet at the same time compliance efforts might stall progress.

3.3. Data Localization Requirements- A Global Phenomenon

Data monetization is one of the big bets of the digital market. For instance, the use of big data by the top 100 EU manufacturers could lead to savings worth EUR 425 billion. Studies estimate that, by 2020, big data analytics could boost EU economic growth by an additional 1.9%, equaling a GDP increase of EUR 206 billion.[15] At the same time, certain governments require storage of data on servers physically located in their territories.

[15] *See:* http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589801/EPRS_BRI(2016)589801_EN.pdf

According to a recent research of the Information Technology and Innovation Foundation (ITIF), approximately 34 countries are using in-country data localization rules.[16] Cutting off data flows or making them harder or more expensive puts foreign firms at a considerable disadvantage. Data localization and other barriers to data flows are estimated to reduce the US GDP by 0.1-0.36 percent; and to reduce GDP by 0.7 to 1.7 percent in Brazil, China, the European Union, India, Indonesia, Korea, and Vietnam. The research denies that data localization provides more security, since breaches can occur irrespectively.

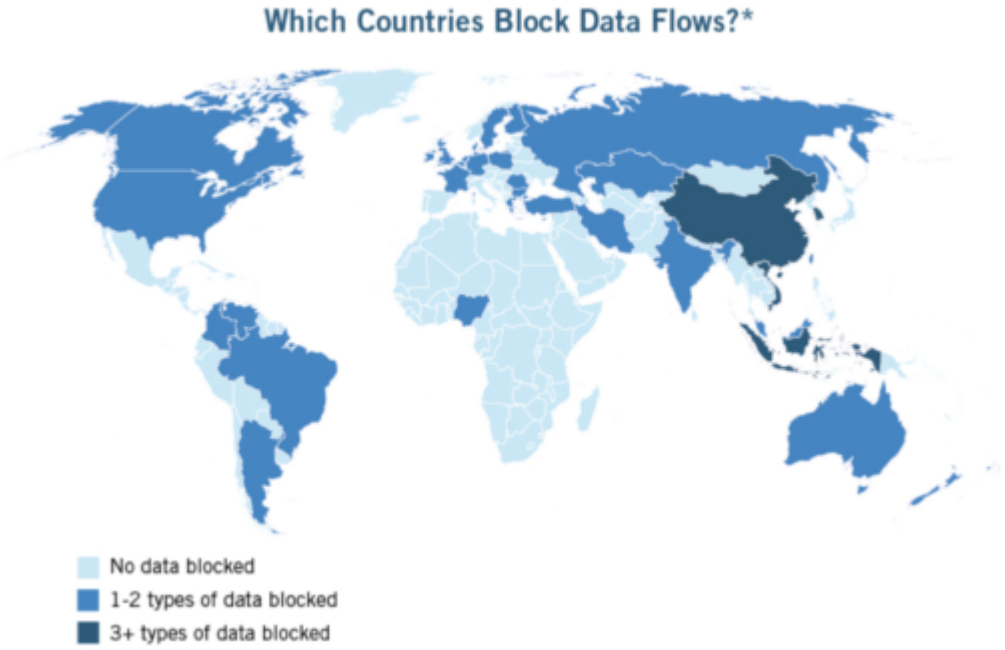

Figure 3: Data Localization Rules Globally - Source: Information Technology & Innovation Foundation

Data localization rules are often put in place to benefit the host country by forcing infrastructure investment. This new form of "digital mercantilism" is similar to how countries use local content requirements and tariffs to protect local manufacturing operations.[17] Instead

[16] *See:* http://www2.itif.org/2017-usitc-global-digital-trade.pdf

[17] *See:* http://diginomica.com/2017/05/03/data-localization-rules-damage-global-digital-economy-says-us-tech-thinktank/

of traditional tariffs, which cannot be enforced on information, countries opt for protective regulations and technical requirements

Local data requirements affect a great number of companies since they increase the cost of doing business, they complicate international data transfers, and render compliance with new laws (e.g. the GDPR that has increased security requirements) even more difficult. Further, companies depend on transferring customer data across borders on a daily basis- their customers may not be happy with them keeping their data in a territory where they do not physically reside.

Data localization raises walls and barriers to the growth of digital trade, whereas at the same time it fragments the markets and creates privacy threats. Indeed, storing the data in several countries because of data localization requirements creates threats to privacy and makes compliance rather chaotic. A fragmented digital market also does not help develop Big Data, the Internet of Things, Cloud computing, and 3D printing.

Data localization is overall an enemy of growth for a number of reasons. First, a significant flow of data currently drives the global digital economy. Every year, the wealth of digital data is becoming overwhelming. Forecasts predict that by 2025 the global datasphere will grow to 163 trillion gigabytes, ten times the amount last year.[18] Any effort to restrict this development only causes anomalies that slow down progress. Also, data currently leads growth, innovation and digitization across all economic sectors. Data monetization is one of the greatest bets for every company, and the relevant economy is only growing more and more. The Big Data sector is growing by approximately 40% per year.

Setting aside the indirect costs to the economy, data localization is directly damaging the companies that have to enforce it. The cost of infrastructure, organizational and information security is significant. Countries often require foreign companies to locate severs

[18] *See:* https://www.ft.com/content/5365c1fa-8369-11e7-94e2-c5b903247afd

and build their data centers locally as a condition for market access. This may cost millions to companies, leaving aside lost efficiency.

For all these reasons, any unnecessary restrictions regarding the location of data should be removed and prevented. The EU is moving to address data localization. The Commission will propose an EU "free flow of data" initiative that tackles restrictions on the free movement of data for reasons other than protecting personal data in the EU, and that addresses unjustified restrictions on the location of data for storage or processing purposes. The Commission further plans on addressing the emerging issues of ownership, interoperability, usability and access to data, for such data types as business-to-business, business-to-consumer, machine-generated, and machine-to-machine.

Apart from the EU and the US, China is the third strongest player who is active in the digital market. China's new cybersecurity law (Cybersecurity Law), which came into force on 1 June 2017, is a milestone.[19] Unlike the EU that has adopted the GDPR, China does not have an *omnibus* data protection law. It instead regulates issues of privacy and cybersecurity over a number of industry-specific laws, like health and education sectors. The cybersecurity law is somewhat different since it has a wide scope and contains provisions relevant both to data privacy and cybersecurity.

The Cybersecurity Law focuses on the protection of personal information and privacy. It regulates the collection and use of personal information. Companies based in or doing business with China, including US and EU companies, will now be required to introduce data protection measures and certain data must be stored locally on domestic servers. Depending on their activity, companies may need to undergo a security clearance prior to moving data out of China. The Cybersecurity Law mainly regulates two types of organizations, network operators and Critical Information Infrastructure (CII) providers.

[19] *See:* https://www.nytimes.com/2017/05/31/business/china-cybersecurity-law.html

Not every aspect of the Cybersecurity Law applies to all companies, however. Many of the law's provisions only apply to the two types of companies mentioned above, network operators and critical information infrastructure providers. However, these categories are defined quite broadly. Even companies that would not ordinarily consider themselves as network operators or CII providers could see the law applying to them. The new cybersecurity law also requires critical information infrastructure providers to store personal information and important data within China and conduct annual security risk assessments. Important data is not defined in the Cybersecurity Law, yet it likely refers to non-personal information that is critical.

Apart from CIIs, it is anticipated that several foreign companies doing business in China will be required to make significant changes on how they handle data. The draft version of the "Measures for Security Assessment", published by the Cyberspace Administration of China, suggests expanding the data localization requirements to all network operators. If adopted, this measure will mean that practically all personal information that network operators collect within China must not leave the country other than for a genuine business need and after a security assessment. In anticipation of this development, there is a trend for foreign companies to set up data centers in China to be able to store data locally.

To address the downsides of data localization, countries can negotiate trade agreements that prohibit and eliminate digital barriers. They must develop better measures of the digital economy and trade, and expand the focus on digital economy and trade issues. Instead of building virtual walls, countries should reap the benefits of digital free trade. Institutions like the World Trade Organization could potentially endorse and assist in this process. A regulation with a nearly global scope can ensure that data localization is the exception only used for critical data piece, and not regular e-commerce activities. Otherwise,

it is likely that countries will continue to exploit the vacuum and introduce further barriers to data flows and digital trade.

International players including the EU and the US are expected to make a move soon to counter the digital protectionism by setting new, high-standard rules that protect data flows. This is in response to threats to digital trade in the EU and the US that are, overall, increasing. (i) Geo-blocking, (ii) data protection regulations that make compliance more perplexed, and (iii) data localization distorts the free market and slows down data liberalization.

3.4 Case study: where competition meets privacy and trade

A recent case study demonstrates how the EU and the US interact in the fields of competition, privacy and digital trade, and how regulatory discrepancy can be negative for companies.

On 18 May 2017, the European Commission fined Facebook EUR 110 million for misrepresentations made in its application for competition clearance of the company's acquisition of WhatsApp.[20] In its merger application, Facebook claimed that it would be unable to automatically match Facebook users' accounts and WhatsApp users' accounts for marketing and other purposes. However, in August 2016, WhatsApp introduced functionality enabling the linking of WhatsApp users' phone numbers with Facebook users' identities. This is the first time since the new Merger Regulation entered into force in 2004 that the Commission has imposed a fine for the provision of misleading information during a merger clearance.

Back in 2014 Facebook asked the Commission to give it the green light to acquire WhatsApp. The Commission conducted an investigation, under the EU Merger Regulation, to

[20] *See:* http://europa.eu/rapid/press-release_IP-17-1369_en.pdf

determine whether the acquisition would violate EU competition rules and give Facebook an undue advantage. One question the Commission asked during the investigation was whether Facebook would be able to automatically match the data of its users with and the data of WhatsApp users. Such automatic data matching could substantially enlarge Facebook's database and enhance use of the data for marketing and other purposes.

During the investigation Facebook informed the Commission that it lacked the technical ability to establish reliable automated data matching. However, the technical possibility of automated matching already existed at the time and was officially introduced on the WhatsApp platform in 2016. The Commission launched an inquiry to investigate the matter. Facebook acknowledged that its provision of incorrect information violated merger procedures and cooperated with the Commission in order to obtain a more lenient fine. This did not prevent the Commission from levying a fine of EUR 110 million Euros, however, which the Commission claimed was both proportionate and deterrent.

The Commission did not state that Facebook's provision of incorrect information had a material effect in getting the deal through. In giving the green light, the Commission had already considered "what if" scenarios that included automated user matching. In particular, the Commission examined whether the acquisition presented significant risks for three different markets: consumer communication services, social networking services, and online advertising. The Commission's assessment was that the two companies were distant competitors and the acquisition posed no significant risks. Had the Commission determined otherwise, it might have attached conditions on clearance, in which case the provision of misleading information on automated data matching could have resulted in an even heavier fine.

This is the first time the Commission has imposed a fine on a company for providing incorrect or misleading information under the Merger Regulation. The fine comes at a time

when EU stakeholders and consumer organizations are pushing hard for greater accountability from companies in relation to users' data. The EU competition authorities are also scrutinizing more closely mergers of online companies for potential consumer harms related to data. This development reflects a general call from the EU Commission to antitrust bodies to work more closely with privacy bodies in regulating the data economy. Recently, for instance, a German antitrust official described Amazon's dual role in collecting data as a reseller and then using it to boost its own retail branch as a "huge issue".

The WhatsApp case therefore signals that the EU is aggressively monitoring data-heavy companies, and that EU merger clearance will take into account the data-related impacts of corporate deals. This is yet another proof that the fields of competition, privacy and trade are constantly converging, with privacy being in the forefront.

4. Conclusion

Different legal fields have tried to regulate the digital market in the EU and the US. Some efforts have been liberal, and others protective. The global reach of digital trade and the protective nature of many states creates this unique spaghetti bowl of regulation that includes competition provisions, online services regulation, data protection and data localization rules. There is no global legal framework governing the digital market that can be used for efficient regulation, which means that for the time being countries have to operate in this context.

Instead of being a supplement to services offered, the digital market is the core hub through which services are delivered. It is now an integral part of almost every financial activity. The challenge for law is to carefully regulate the digital market, at a pace that will facilitate development and not hamper economic welfare. Regulation should create more

transparency, remove virtual walls, and prevent unnecessary restrictions on the location of data.