Bauer, Matthias; Erixon, Fredrik

Research Report

Europe's quest for technology sovereignty: Opportunities and pitfalls

ECIPE Occasional Paper, No. 02/2020

Provided in Cooperation with:
European Centre for International Political Economy (ECIPE), Brussels

Suggested Citation: Bauer, Matthias; Erixon, Fredrik (2020) : Europe's quest for technology sovereignty: Opportunities and pitfalls, ECIPE Occasional Paper, No. 02/2020, European Centre for International Political Economy (ECIPE), Brussels

This Version is available at:
https://hdl.handle.net/10419/251089

ECIPE OCCASIONAL PAPER ▪ 02/2020

Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls

By **Matthias Bauer** *and* **Fredrik Erixon**

ECIPE | EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY

EXECUTIVE SUMMARY

Covid-19 and its broader implications have highlighted the importance of Europe's digital transformation to ensure Europeans' social and economic well-being. It provides important new learnings about Europe's quest for "technology sovereignty".

While the debate about technology sovereignty is timely, the precise meaning of sovereignty or autonomy in the realm of technologies remains ambiguous. It should be noted that the political discussions about European technology sovereignty emerged far before the outbreak of the Coronavirus. The European Commission's recently updated industrial and digital policy strategies "institutionalised" different notions of sovereignty, reflecting perceptions that more EU action is needed to defend perceived European values and to secure Europe's industrial competitiveness. Often the political rhetoric reflected perceptions that Europe is losing global economic clout and geopolitical influence. It was said that dependency on technological solutions, often originating abroad, would require a European industrial and regulatory response. Against this background, the Corona crisis provides two important lessons for EU technology policymaking.

Firstly, during the crisis digital technologies and solutions made European citizens stronger. Technology kept Europe open for business despite the lock-down by enabling Europeans to work from home, receive essential home deliveries, home schooling, online deliveries and to use online payments, etc. In addition, Europe's citizens became more sovereign with respect to accessing information and data that helped track and contain the spread of the virus.

Secondly, the crisis tested Europe's resilience and perceived dependency on (foreign) technology solutions. Early developments indicate that Member States' homemade solutions did not fare better than existing European and international solutions. A few national and EU IT solutions failed while existing European and global solutions, from cloud infrastructure to communications, payments to streaming services, all continued to work well.

Politically, however, the crisis could be used to justify more EU or national government interference in Europe's digital transformation. Indeed, for some the debate about European technology sovereignty is largely about designing prescriptive policies, which paradoxically risk reducing Europeans' access to the innovative technologies, products and services that helped Europe through the crisis. Policies taken into consideration include new subsidies to politically picked companies, or new rules and obligations for certain online business models. Policy-makers advocating for such policies tend to ignore critical insights from the Covid-19 crisis and failed industrial policy initiatives, including sunk public investments and protracted subsidies for industrial laggards.

In a time of economic hardship, the EU and national governments should be wary of spending even more taxpayer money to replicate existing world-class technology solutions, that in most cases are used in combination with local technologies, with "Made in EU" services of inferior quality and reliability. Moreover, due to different levels of economic development and differences in regulatory cultures, prescriptive technology policies would exclude many Member States from utilising existing and new opportunities that arise from digitalisation, slowing down economic renewal and convergence.

The EU cannot be considered a monolithic block that thrives on a unique set of prescriptive technology policies. Before the Corona pandemic, initiatives towards European technology sovereignty were mainly pushed by France and Germany, fed by concerns over their companies' industrial strength in times of growing economic and geopolitical competition. Industrial and technology policies favoured by the EU's two largest countries will have a disproportionately negative impact on Europe's smaller open economies, whose companies and citizens could be

deprived from cutting-edge technologies, new economic opportunities and partnerships on global markets, undermining these economies' development and international competitiveness.

Any EU-imposed technology protectionism along the lines suggested by some policy-makers in large EU Member States would leave the entire EU worse off. It would disproportionately hurt countries in Europe's northern, eastern and southern countries more than the large countries whose economies are generally more diverse than Europe's smaller Member States.

It would, however, make sense for the EU to agree on a shared definition of "technology sovereignty". Different interpretations could cause serious policy inconsistencies, undermining the effectiveness of EU and national economic policies. Anchored in technological openness, technology sovereignty can indeed be a useful ambition to let Europe's highly diverse economies leapfrog by using existing technologies. To become more sovereign in a global economy, Europeans need to focus on becoming global leaders in economic innovation – not just in regulation. If anchored in mercantilist or protectionist ideas, technological sovereignty would make it harder for many Member States to access modern technologies, adopt new business models and attract foreign investment – with adverse implications on future global competitiveness, economic renewal and economic convergence.

Policymaking towards a European technology sovereignty that benefits the greatest number of Europeans – not just a few politically selected "winners" – should aim for a regulatory environment in which technology companies and technology adopters can thrive across EU Member States' national borders. The European Single Market has deteriorated in recent years and significantly during the crisis. The new von der Leyen Commission has now repeatedly called for a strengthening of the Single Market. Becoming a world leader in innovation requires a real Single Market in which companies can scale up, with as few hurdles as possible, and then compete globally. It should be supplemented by pro-competitive policies and incentives for research and investment.

Brussels cannot set the global standards in technology policymaking alone. Europe's policy-makers should aim for closer market integration and regulatory cooperation with trustworthy international partners such as the G7 or the larger group of the OECD countries. It is in the EU's self-interest to advocate for a rules-based international order with open markets. International cooperation should be extended beyond trade to include cooperation on technology policies, e.g. artificial intelligence. Regulatory cooperation with allies such as the USA is essential to jointly set global standards that are based on shared values. Both the EU and the US have much more to gain if they prioritise such alignment, to advance a shared vision for a revamped open international trading system, in a world increasingly influenced by regimes with fundamentally different views on state intervention and human rights. Anchored in technological openness, the EU and the US can promote technology sovereignty that allows for development and renewal elsewhere in the world.

TABLE OF CONTENTS

1. INTRODUCTION[1]

Some leaders in Europe are calling for policies to promote "European Technology Sovereignty" or "Digital Sovereignty" (we use these terms interchangeably in this paper). The concept of technology sovereignty is not new – it has a long and chequered past – and its exact meaning is disputed. For some it is mostly about economic strategy, while others view technology sovereignty through the lenses of values, history or international public law.

It is obvious that economic success will never be the result of a policy that intends to make Europe independent of technological developments abroad, and – thankfully – there aren't many politicians making the case for technology independence. It is equally obvious that such a conception of sovereignty does not sit comfortably in the European Union: for some EU countries, it would primarily mean independence from other Member States, leading to more friction in Europe. Consequently, a European policy of technology independence would imperil Europeans' own economic future.

Fortunately, there are other ways to look at technology sovereignty and the purpose of this paper is to explore how Europe could improve its technology sovereignty while promoting technology openness. The two aren't mutually exclusive: in a modern economy they rather reinforce each other. Our view takes aim at deepening the Single Market – which is still incomplete and fragmented by national regulations – and how that would improve Europe's capacity to influence its own future. We will make the point that, for the economy and the protection of key values, Europe should encourage closer market integration and regulatory cooperation with key international partners, such as OECD countries. The transatlantic relationship will also be key, especially its combination of values, economic size and a place at the technological frontier(s). By working together, Europe and the US can set the market norms and the global standards. However, if both sides pursue competing standards, then neither side will be able to shape how a digital and technology-driven economy will influence them.

It is critical for Europe's ability to shape its own technological future that European policy-makers cooperate with others. If the economic and societal consequences of Covid-19 and the pandemic have showed anything, it is that resilience comes from adaptability and reliance on a

[1] ECIPE gratefully acknowledges support to this study by the Computer & Communications Industry Association. The paper was completed in May 2020.

multitude of sources – not from autarkic policies or "putting all your eggs in one basket". During the pandemic crisis, many different domestic and foreign actors have contributed to the supply of much-needed medical goods and food products, or taken actions to ensure basic services like telecoms and audio-visual services work despite enormous stress.

The Covid-19 crisis disrupted industrial value chains, while digital services continued to work, kept Europe open for business, more resilient and thus more sovereign. This was recognised by Werner Stengg, Cabinet Expert for Digital Policy to European Commission Executive Vice President Margrethe Vestager, who stated in May 2020 that the "[t]he only thing that really worked during the height of the crisis was digital." (Access Partnership 2020)

For a country or a regional entity like the EU, the capacity to effectively shape outcomes – to have effective sovereignty – depends crucially on policies and behaviour that harness the energy and ingenuity of many actors. The same conclusion holds for technology policy: Europe's capacity to prosper on the back of technology comes from the ability of individuals, firms and governments to make use of frontier technologies in many different ways.

The paper is structured as follows. Section 2 discusses notions of sovereignty and autonomy (occasionally independence) and their implications for policymaking. Section 3 explains the background to the current debate about a European technology sovereignty. We explore multiple origins of the debate, which we classify as the "4 Cs" – culture, control, competitiveness and cybersecurity. Section 4 discusses misguided industrial policy and the potential cost of an EU-imposed technology protectionism in the light of the EU's new industrial and digital policy strategies. It provides recommendations on how the EU's diverse Member States can become more sovereign from policies that embrace investment, encourage innovation and help facilitate structural economic renewal.

2. SOVEREIGNTY, AUTONOMY AND INTERNATIONAL ECONOMIC INTERDEPENDENCE

What is sovereignty, and what does it mean in the context of technology and digital policy?

Obviously, sovereignty can have different meanings. At its core, it refers to having "supreme authority within a territory" largely corresponding with "political authority over a certain territory".[2] The notion of "sovereignty" in the context of technology has been used in recent years to describe various forms of independence, control and autonomy over digital technologies, business models and contents. In France, for example, a popular view of digital sovereignty means "the control of our present and of our destiny as they manifest and orient themselves through the use of technologies and computer networks" (Bellanger 2011). According to the author of these words, it is a loss of sovereignty when the government does not control the evolution of digital networks (Couture and Toupin 2017).

In more general terms, sovereignty means that countries are "free to choose their own form of government" and that they are protected from interventions in their internal affairs by other countries (see, e.g., Besson 2011; Berger 2010; Krasner 2001). In this way, sovereignty for states became a rather straightforward concept enshrined in international law. However, it gets more problematic once sovereignty gets to mean something else, e.g. policy-makers suggesting that states are or should be truly independent from each other and free to make any decision about its affairs, even when it affects others. For a long time now, governments have cooperated and contracted with other governments about what rules that should apply in interstate relations. Even if governments can renege on their international obligations, they tend to accept certain

[2] See, e.g., Stanford Encyclopedia of Philosophy.

limits on national sovereignty because alternative forms to govern intergovernmental relations come with negative consequences.

In international economic regulation, for instance, states agree with each other on specific behavioural codes of conduct – in everything from sanitary and phytosanitary (SPS) rules to the conduct of competition policy. A good example is the European Union itself: in commercial policy, it establishes the rules of competitive behaviour. This is also true for digital and technology regulations. Even if such regulations remain incomplete, there are many international agreements – including bilateral trade agreements – that reduce the sovereignty of governments to make certain decisions.

The real ability to influence the future also depends on actual performance. To become more sovereign in an increasingly interlinked global economy, Europe needs to focus on becoming a global leader in economic innovation – not just a leader in regulation and good governance. As argued by Leonard et al. (2019),

> [t]here is no such thing as technological independence in an open, interconnected economy. But an economy of 450 million inhabitants (excluding the UK) with a GDP of €14,000 billion can aim to master key generic technologies and infrastructures. The EU's aim should be to become a player in all fields that are vital for the resilience of the economic system and/or that contribute to shaping the future in a critical way.

A popular way to think about sovereignty is based on autonomy. Jean-Claude Juncker, the former President of the European Commission, proclaimed in 2018 that now is the "The Hour of European Sovereignty". (European Commission 2018) There is also much talk about "strategic autonomy" for the EU as a whole and such claims featured widely in the European election in 2019. While strategic autonomy was often thought of as a vehicle for closer European cooperation, it is notable that individual Member States also increasingly refer to autonomy in relation to big EU countries like France and Germany. For several Member States, strategic autonomy often means avoiding dependence on European economic and political powers.

For the European Commission, European autonomy largely means that Europe's policy-makers retain the capacity to cater for European firms and advance Europe's economic interests globally (European Commission 2020a, 2020b, 2020c). While this starting point makes sense, it immediately follows that Europe should focus on realistic opportunities for European policy-makers to shape – together with non-Europeans – the laws, rules and norms that will define digital performance, commercial cooperation and competition. In a digitised world with global value chains, autonomy simply cannot mean independence from others. It's too costly. Trade controls, subsidies or industrial policy cannot substitute for the benefits that Europeans and others draw from technological and digital openness.

Global economic developments suggest that Europe has strong interests to collaborate with others. The centre of the world's economic gravity is shifting. McKinsey (2019) suggests Asia will account for 50% of global GDP by 2040. Until 2050, says the PWC (2017), the EU and the US will steadily lose ground to the rising economies of India and China. The share of EU-27 gross domestic product (GDP) in global GDP will fall to some 9%, while US GDP is expected to stand at a somewhat higher 12% of world GDP in 2050.[3]

[3] Expectations of this shift are already strong. Even though the EU is still the world's second-largest economy by GDP, only a few people globally actually consider it an economic leader ahead of the US or China. According to a PEW (2017) survey across the 38 nations, a median of just 9% considered the countries of the EU as the world's leading economic power. 42% named the US and 32% pointed to China, while an additional 7% referred to Japan. It is noteworthy that even in the 10 EU countries covered by the survey, a median of only 9% viewed the EU as the world's top economy.

There are three important takeaways for Europe as policy-makers consider their options. First, neither Europe nor the US will be able to rely on their own market size as the main source of maintaining autonomy, sovereignty and influence in the global economy. Other countries, e.g. Japan, are confronted with the same reality. Rising powers like China and India may gain tremendously in market clout and increase political pressure on others to conform to their laws, rules and norms, but none of them will come close to the same dominance in global rulemaking that the US and Europe had in the period that followed the Second World War. Global economic power will be rather more distributed.

Most regions in the world struggle to improve data integrity and protect networks from intrusions – even when their governments are perpetrators.[4] Europe is not alone in wanting the behaviour of Internet users – governments, businesses and citizens – to follow fundamental rights. Similarly, Europeans are not alone in feeling that the economic payoff from digitalisation could improve. Several governments also feel that digitalisation is just a one-way street of benefits going to big technology firms. It is an opinion also shared among some American politicians, despite the US being the birthplace of internationally successful technology companies. However, it is a testimony to the current structural technology transformation of the economy that everyone seems to think they are a loser and that the winners are foreigners. In reality, the benefits of the digital economy are much more evenly spread across economies – proven by the uptake of ICT goods and digital services by consumers. After all, most of the economic benefits from new technologies and new business models are reaped where they are adopted.

The second takeaway point is that, with falling relative economic power, Europe will have to improve its capacity to influence global rules and performance by being home to innovative companies. When quantity does not count in its favour anymore, at least not in the way it used to do, Europe will have to improve regulatory skills at home to encourage innovation and become an example that others want to follow. With a 9% share in the global economy, Europe will become increasingly dependent on other parts of the world in the provision of frontier technology and digital services. Frankly, it is not possible to reduce global dependence at the same time as one's relative economic size is falling.

The third takeaway point is that the Single Market is the source of Europe's autonomy – and that it needs to deepen for autonomy to increase. Size matters, and with a larger economy that allows for cross-border commerce and technology development, Europe can make itself more attractive as a place to innovate and develop the future economy. Moreover, with more economic clout, the EU will also have a stronger voice to influence global norms and standards for technology.

3. MAJOR ROOT CAUSES OF EUROPE' DEBATE ON TECHNOLOGY SOVEREIGNTY

Why is Europe exploring concepts of technology sovereignty – and why now? Motivations vary between observers. Many concepts of technology sovereignty revolve around data privacy, trust and reliable content (e.g. Popp 2019; Benhamou 2018; Goujard 2018; Pohlmann 2014). Some use sovereignty to make a case for addressing perceived challenges arising from certain technology companies (Gueham 2017). Others refer to consumer protection (e.g. German Advisory Council for Consumer Affairs 2017). A large body of the technology sovereignty literature is about artificial intelligence (e.g. DigitalGipfel 2018) and cybersecurity (e.g. Bonenfant 2018). Others refer to payment sovereignty (e.g. ECB 2019). Further notions relate to "general" access to critical technologies (e.g. Drent 2018) and "technology dependencies" in defence and general public procurement (e.g. Fiott 2018; FMIBC 2019; Lippert et al. 2019). Obviously, many of these motivations aim to define the concept of economic sovereignty.

[4] We view "data integrity" as overall accuracy, completeness and consistency of data, but also safety of data in regards to regulatory compliance, e.g. compliance with data protection regulations.

There are, in our view, four broader factors behind the emergence of technology sovereignty as a desirable political ambition. These factors are summarised in what we call the 4Cs: culture, control, competitiveness and cybersecurity.

1. Culture: the "cultural" approach to technology sovereignty starts from the assumption that Europe is different from other parts in the world in our defence of values and market regulations – manifested for instance in data protection rights. At the heart of this view is the perception that, in particular, digital regulation presents a fundamental choice between individual rights and business freedom, and that Europe has made its choice to protect human values and rights over business freedom.

2. Control: there is a strand in the debate that takes a command-and-control view of technological sovereignty, arguing that the EU or individual Member States need to have the policy instruments to control the outcomes of the digital economy in general and how citizens and companies use modern digital services.

3. Competitiveness: another viewpoint collects different thoughts and considerations around industrial competitiveness – the future capacity of European multinational enterprises to compete on world markets and fears about declining European influence vis-à-vis other standard-setting powers.

4. Cybersecurity: finally, there is a growing demand for new policies to protect personal and business data, and to have at disposal all the tools and technologies necessary to protect digital integrity and digital resilience.

3.1. Culture and Control: A Static Approach to Regulation

3.1.1. Culture

The cultural approach to technology sovereignty – the first C – reflects two views that are often taken by European policy-makers to support certain regulatory approaches: first, the view that Europe is a monolithic block with respect to key values (all share the same preferences) and that these values are different from the values of other countries, e.g. China, the USA or Switzerland. It is assumed that if other countries regulate their digital economies in a different way than Europe, for instance, they do so because their values are different. And second, that digital and technology regulation often (but not always) is a choice between values and rights, on the one hand, and economic freedom on the other. Both views are reflected in the economic policy mandates of the executive branch of the European Commission (see Box 1).

Both views are misguided and see value conflicts where there are none. There are of course value differences in the world, and they can also manifest themselves in regulations. But the reality is that most governments in the world have converged quite substantially in how they regulate – and also in the motivations for why they regulate. Likewise, the conflict between individual rights and economic freedoms is an exaggeration. It is true that such conflicts over values sometimes arise, but what is more fundamental is that long-term economic freedom and economic success are indivisible for a culture that also promotes human integrity and individual rights.

An example of Europe's value-based approach is the EU's new digital strategy, Shaping Europe's digital future. The communication was published by the European Commission in February 2020 and says it wants a "European society powered by digital solutions that are strongly rooted in our common values […]" (European Commission 2020b, p. 1). Furthermore, it argues that "[w]hile we cannot predict the future of digital technology, European values and ethical rules and social and environmental norms must apply also in the digital space" (p. 10).

BOX 1: EUROPEAN COMMISSIONERS' ECONOMIC POLICY MANDATES IN DEFENCE OF EUROPEAN VALUES

In December 2019, European Commission President Ursula von der Leyen formally mandated the EU's new Commissioners to support the EU's technological sovereignty by the use of economic, trade and industrial policymaking aiming to defend "European values".

Margrethe Vestager, the EU's new Executive Vice-President for "A Europe fit for the Digital Age", was mandated to develop an EU industrial strategy that "mobilise[s] the EU toolbox to support the development of key value chains and technologies that are of strategic importance for Europe […] because they contribute to technological sovereignty or because of their enabling character for a wide range of industries throughout Europe".

Commissioner Vestager was also assigned the task to find "a European approach on Artificial Intelligence, including its human and ethical implications. This effort will feed into the broader work stream on industrial policy and technological sovereignty […]". Vestager shall "ensure that the European way is characterised by our human and ethical approach. New technologies can never mean new values" (von der Leyen 2019a).

Thierry Breton, the EU's new Commissioner for the Internal Market, was tasked to enhance "[…] Europe's technological sovereignty", by "[…] investing in the next frontier of technologies, such as blockchain, high-performance computing, algorithms, and data-sharing and data-usage tools. It also means jointly defining standards for 5G networks and new-generation technologies." Mr Breton's "task for the next five years is to put in place the right framework to allow Europe to make the most of the digital transition, while ensuring that our enduring values are respected as new technologies develop" (von der Leyen 2019b).

Phil Hogan, the EU's new Commissioner for International Market, was tasked to ensure that EU "trade policy [remains] a strategic asset for Europe. It allows us to build partnerships, protect our market from unfair practices and ensure our values and our standards are respected."

Sources: Letters sent by European Commission President Ursula von der Leyen (2019a, 2019b, 2019c).

These are good ambitions, but they are not novel or exclusive to Europe. Unfortunately, they all too often come at the expense of policy detail – and if there is one charge that can be made against this type of value-based policymaking, it is that it comes across as hollow grandstanding. In this case, notions of European values aim to guide a large package of legislation on data, artificial intelligence, industrial policy, small and medium-sized enterprises (SMEs) and the Single Market. Furthermore, these values intend to influence regulatory standards, public procurement and trade policy – all in the purpose of improving Europe's global influence and the competitiveness of its industry. A similar policy motivation became obvious in the EU's attempt to establish a Union-wide tax on certain digital services. Another example of how European values power political thinking was the attempt by the new Commission to have a Commissioner to protect the "European way of life" ("protecting our citizens and our values").

In the political guidelines for the new European Commission, Ursula von der Leyen stated that "[i]n this field [protecting the sovereignty of individuals and ensuring they have full control over their own data] Europe has acted from a position of common strength. And that's what makes it special." Referring to one of the Juncker Commission's major political achievements, the adoption of a largely harmonised EU data protection regulation, the new Commission President wants to call out the willingness to maintain "our European way, balancing the flow and wide use of data while preserving high privacy, security, safety and ethical standards. We already achieved this with the General Data Protection Regulation [GDPR], and many countries have followed our path" (von der Leyen 2019d). In the debate about a European technology sovereignty, similar statements have been made by policy-makers from Member States and the European Parliament (see Table 1).

TABLE 1: EUROPEAN POLICYMAKERS' STATED MOTIVATIONS FOR DIGITAL POLICIES: CULTURE

"Ultimately it's about sovereignty. It's about protecting the sovereignty of individuals and ensuring they have full control over their own data. In this field Europe has acted from a position of common strength. And that's what makes it special."	Ursula von der Leyen, European Commission President, Speech, 8.11.2019.
"Digital sovereignty means: allowing the use of data from European citizens and the use of digital technologies only when our standards are fulfilled."	Axel Voss, MEP (EPP, Germany), Twitter, 18.1.2020.
"Europe must protect its digital sovereignty. We need to develop a third–European–way of digitalisation, based on our values."	Axel Voss, MEP (EPP, Germany, Twitter, 18.1.2020.
"The question is how can we work with very good industries without being impacted by the CLOUD Act."	Guillaume Poupard, Chief Cybersecurity Official, France, quoted in Politico, 2.2.2020.
"We also need to be sure that we protect our citizens against U.S. regulation with extraterritorial applications. The CLOUD Act is a risk for us. There's no debate about this. Other U.S. regulations are considered risks too."	Guillaume Poupard – Chief Cybersecurity Official, France, quoted in Politico, 2.2.2020.
"Digital sovereignty is about being able to control what we are doing. Not to do everything by ourselves or being completely independent. But to have the final say about what is ongoing here in order to maintain our regulatory sovereignty."	Margrethe Vestager, Speech at CERRE event on "Digital sovereignty in the age of pandemics", 24.4.2020

Source: ECIPE.

A good example to show how the real policy choice is often not about commercial freedoms versus individual rights can be found in the debate about the new policy ideas set out by the Commission in February 2020, in which the Commission acknowledges the general positive impact of digitalisation on Europe's societies. The Commission recognises the need for substantial investment in the EU to narrow the gaps vis-à-vis China and the USA. But it is striking how different Commission documents take aim at different strategies, suggesting that there is severe clash between regulatory cultures within the Commission. While the (French) Single Market commissioner has set out a somewhat interventionist Data Strategy, the (Danish) Competition and Digital Strategy commissioner has launched more liberal approaches in her recent Digital Strategy and the White Paper on Artificial Intelligence. Recent discussions on European competition policy demonstrate that there are similar clashes between EU Member States on competition issues.

While Commissioner Vestager's approach aims to spur competition, avoid market and data concentration, and create dynamic opportunities for Europe to benefit on the back of a global technology revolution, Commissioner Breton appears to see opportunities in an approach that creates market opportunities for those that would benefit from getting EU and national government protection against foreign competition. Commissioner Breton's Data Strategy advances the idea of creating a European Data Space that may limit the participation of foreign providers of data services. It is stated that "for access […] use of data […] there is an open, but assertive approach to international data flows, based on European values" (European Commission 2020c, p. 5). A European data space would, it is claimed, improve security and trust, and "give businesses in the EU the possibility to build on the scale of the single market" (p. 17), while stimulating creators of industrial data to share this data more freely. As Europe hosts some of the biggest generators of industrial data in the world, it is said to have a comparative advantage in this field that can only be exploited if there is a higher degree of European control of the data infrastructure.

Data storage has become a bugbear for those who think that current market solutions do not respect European values. Germany now wants to create a cloud-computing platform, Gaia-X, that is, by origin, European and would work with rules that eventually can become the European regulatory standard. Many supporters of the initiative think this is the starting point for getting a cloud platform that is a better fit with European values.

Perhaps that is the case, but it remains unclear exactly what market problem that a "European" platform would resolve. After all, the idea of creating a European data space is not new at all. A few powerful European legacy operators and their national governments have, over the years, pushed similar ideas, e.g. a "Schengen area of data". EU legislation is already in place to ensure the free flow of data in the EU Single Market (GDPR and the Regulation on the free-flow of non-personal data). Legal exemptions for allowing the flow of personal data from the EU to the rest of the world are few and under constant threat of invalidation.

But more to the point, European companies and public authorities can already today decide how and where they want to store their data, e.g. in-country or even on-premise. There are hundreds (if not thousands) of cloud service providers operating on the promise to exclusively store data within the border of EU Member States, e.g. nextcloud and owncloud (Stackfield 2019). Europeans have a much greater choice than they admit over where and how to store their data. It appears that the main reason is rather to fix a perceived commercial problem: that many of the most popular companies in the fields of data storage and processing are non-European. What is new is the political will in some EU Member States and in Brussels, to accommodate repeated calls by some national champions to stack market rules in their favour.

To be fair, Europe is not so different from other countries in its desire to safeguard data integrity. Most OECD countries already have or are considering high standards for data privacy and security. Accordingly, Europeans can rely on commercial solutions from a host of its partners in its quest for data integrity. Also, most actors, including European governments and industrial firms, take a far more sophisticated view on data security. They partner with several application and security vendors in a strategy to make it impossible for anyone who may get their hands on their data to actually make use of it. For those who store data that is covered by European data protection regulations, they routinely contract with their cloud providers about a strategy that comply with these regulations. These contracts rarely rest on the notion that data storage can only take place within one territory for the simple reason that the more data is distributed, the less it is concentrated and therefore less vulnerable. Data residency in itself does not equate IT security. The security of the data depends on the security governance and controls implemented, not on the localisation of the data. Data can be localised in a certain premise with a very low level of security.

It is notable how fast that some European policy-makers are jumping to the conclusion that radical measures are needed to create notional data sovereignty, reinforcing a misguided view that in order to create a greater digital autonomy, Europe must close itself off from the rest of the world. Europe's digital sovereignty is rather based on the capacity to have access to key services and be independently capable to understand, use and alter these services, with the view of using it for the purposes of protecting rights and generating economic and social development.

Supporters of European data spaces often argue that the US Cloud Act from 2018 allows for widespread snooping and mass data surveillance of personal data by US law enforcement agencies. That view is clearly exaggerated and misleading (see Box 2). European institutions and governments are in fact pushing for their own legislation to more effectively access data stored abroad in their criminal investigations. To make this work, the EU is conducting negotiations with US authorities for an EU-US cloud framework. This agreement would help European agencies to facilitate faster access to electronic (or data) evidence in criminal investigations. France, Germany and the European Commission have signalled that their ambitions are aligned with the US view and that there is a need to speed up data sharing between law enforcement agencies that have legitimate requests about data evidence stored in another country (European Commission 2019a).

This makes sense. As an open and export-driven economy, it is in the EU's interest to advocate for a rules-based international order. An EU-US cloud framework assisting the investigation of serious crime would be in Europe's interest. Yet the EU-US negotiations have stumbled and the

EU still does not have a clear negotiation position, e.g. an adopted EU e-evidence legislative proposal. The US, on the other hand, is moving ahead with Cloud Act agreements with non-EU countries, e.g. the recent UK-US agreement and the agreement between the US and Australia (USDJ 2019a; 2019b).

BOX 2: US CLOUD ACT, GDPR AND THE FUTURE OF AN EU-US AGREEMENT FOR E-EVIDENCE DATA-SHARING

Law enforcement officials around the world are struggling to combat crime as evidence is increasingly stored online and in other jurisdictions.

The US Clarifying Lawful Overseas Use of Data Act (US Cloud Act) was passed in 2018. It gives law enforcement authorities in the US the legal means to request data stored by US and non-EU service providers with "sufficient contact" with the United States, even if this data is stored outside the US.

The Cloud Act amended the US Stored Communications Act (SCA). It explicitly allows US law enforcement through a warrant, subpoena or court order to access electronically stored communications data located outside the US, based on the following two conditions: the issue must involve a criminal complaint and the servers must be controlled by a US company.

The Cloud Act also created a framework under which the US can sign bilateral agreements with foreign governments. Based on such agreements, US law enforcement authorities as well as foreign governments would be allowed to make requests directly to local law enforcement and service providers located in the other jurisdiction. Accordingly, under an EU-US agreement, an EU government could directly contact a service provider or local law enforcement authority in the US to request information stored in the US, and vice versa.

Following Linklaters (2019), the US Cloud Act will "only streamline and expedite the information-sharing process between foreign law enforcement agencies, instead of relying on traditionally slower Mutual Legal Assistance Treaty (MLAT) requests". At the same time, a number of safeguard provisions ensure that the risk of abuse is effectively limited. Similarly, as outlined by Hogan Lovells (2019),

the CLOUD Act allows foreign governments to enter into new bilateral executive agreements (EAs) with the United States. These EAs would permit streamlined foreign law enforcement requests directly to U.S. service providers and would complement the procedures in existing Mutual Legal Assistance Treaties (MLATs).

The US Cloud Act does not allow mass collection of data and indiscriminate collection of communications data: an order seeking, for example, stored contents of communications must be for specific data and will only be granted where the government can establish "probable cause" that a particular criminal offence has been committed and there is "reasonable belief" or justification that the information sought is "relevant and material" to that ongoing criminal investigation.

With regard to data stored in the EU, the European Data Protection Board (EDPB) in a joint response with the European Data Protection Supervisor (EDPS; in a non-binding opinion) referred to Article 48 of the GDPR, which provides that a foreign court order or decision of an administrative authority will not be automatically recognised and enforced in the EU, unless made under MLATs. It is argued that "[a] request from a foreign authority does not in itself constitute a legal ground for transfer. The order can only be recognised 'if based on an international agreement such as a mutual legal assistance treaty [MLAT], in force between the requesting third country and the Union or a Member State'" (EDPB 2019, p. 3).

Companies which today respond to an order from US law enforcement authorities are at risk of breaching the GDPR and risk fines of up to EUR 20 million or 4% of their annual worldwide turnover. As argued by Linklaters (2019), "[g]iven the sensitivity of this issue and the desire to protect the EU's 'data sovereignty', the prospect of very significant sanctions is quite plausible". According to the Cloud Act, service providers then have "the possibility to appeal an order if a required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government" (see also KPMG 2019).

In September 2019, the European Commission and the US Department of Justice officials published a joint statement on the opening of negotiations for an "EU-US agreement to facilitate access to electronic evidence in criminal investigations" (European Commission 2019a). The US uses its Cloud Act as its starting points in the negotiations. EU Member States agreed to give two mandates, which include "provisions on strong fundamental rights safeguards on data protection, privacy and the procedural rights of individuals, which will have to be an integral part of any future agreement". Then European Commissioner Dimitris Avramopoulos clarified that the EU's own policy objectives for cross-border law enforcement are generally aligned with those in the US: "Criminals operate across borders and the evidence we need to investigate their crimes is often in other jurisdictions. Our law enforcement authorities need to be able to swiftly get access to this evidence" (European Commission 2019b).

Summarising the above: European allegations that the US Cloud Act undermines the EU's GDPR requirements by compelling US and non-US firms (which are also caught by the Cloud Act if they have operations/customers in the US) to allow access to certain types of data from EU citizens are exaggerated. At the same time, an international (EU-US) agreement is needed to modernise law enforcement cooperation and ensure legal certainty for citizens and businesses.

3.1.2. Control

The second C – control – is rooted in political desires to control technology and digital platforms that store Europe-generated data. It links up with some general attitudes around data protection. At the heart, however, it considers the reliance on foreign platforms and cloud providers to be a source of instability for data integrity: European firms and public authorities are considered victims. It is said that Europeans are forced to use foreign technologies and services because there are no European options.

Command-and-control approaches generally rest on a state-centric approach to digitalisation. Its core manifestation is reflected by the notion that the digital revolution has left Europe a bit stranded by making European firms less globally competitive and its governments less able to control the outcomes of markets and technological change. There is a sentiment that European blue-chip firms, in particular, are losing out to global tech giants and that there is inevitably a loss of competitiveness for Europe when the industrial heartland gets ever more dependent on data and services provided by these (foreign) firms (see Table 2).

TABLE 2: EUROPEAN POLICY-MAKERS' STATED MOTIVATIONS FOR DIGITAL POLICIES: CONTROL

"We must have mastery and ownership of key technologies in Europe."	Ursula von der Leyen, President of the European Commission, Inaugural Speech at European Parliament, 27.11.2019.
"Bruno Le Maire, French finance minister, has called for a 'new empire' of Europe to resist attempts by rival superpowers in the US."	Bruno Le Maire, French Minister for Economy and Finance, quoted in Financial Times, 2.4.2019.
"France's position is that we should not let Americans have the FAANG, Chinese have the BATX and leave Europe with the GDPR. It would be a big problem for sovereignty, jobs and the European social model."	Cédric O, French Digital Minister, Politico, 10.2.2020.
"Protecting our industrial heritage means protecting data"	Bruno Le Maire, French Minister for Economy and Finance, L'Express, 5.2.2020.

Source: ECIPE.

Such perceptions are echoed in the European Commission's recent strategy for governing data in the EU. The Commission sets out the ambition for the EU to become a leader in data innovation, but then wants to spend several billions of EU taxpayers' money on replicating data infrastructure that already exists or which there appears no commercial demand for. A "key action" outlined by recent Data Strategy is to invest "in a High Impact project on European data spaces, encompassing data sharing architectures" (including standards for data sharing, best practices, tools) and governance mechanisms, as well as the "European federation (i.e. interconnection) of energy-efficient and trustworthy edge and cloud infrastructures (Infrastructure-as-a-Service, Platform-as-a-Service and Software-as-a-Service services)", with a view to facilitating combined investments of "€4-6 billion", of which the Commission "could aim at investing €2 billion". (European Commission 2020c, p. 16)

Europe's policy-makers should not expect European companies to become more innovative by embracing dirigiste – government-directed – policies. Data-sharing obligations can create the opposite of what was actually intended. In the European Commission's White Paper on data it is argued that "data should be available to all". However, the Commission does not take its own claim too seriously. A few lines below the radical vision of an open data space, it is argued that data should be "as open as possible, as closed as necessary". Commissioner Breton also stated: "[w]hen we talk about data sharing, we're not talking about essential data, because companies would never do it – and rightly so" (Politico 2020a). Indeed, many companies are unwilling to give away data, such as trade secrets, that are essential for their survival.

For some time now there have been growing concerns about the lack of speed in Europe's digitalisation, especially on the corporate side. While Europe hosts many multinational firms that are at the frontier of the digital revolution, many SMEs have failed to seize digital opportunities and to make necessary investments. As a result, Europe is generally considered to lag behind many other advanced economies on key indicators for the adoption of digital technologies.

The concept of data sovereignty gets interesting in this context. Two things are obvious from economic research. First, many European firms do not have the autonomy and the opportunity to follow digital developments, let alone to be at its vanguard. There are critical problems for the provision of all the tools and instruments needed to be at the frontier – and many of them are based on the lack of supply of human capital (IT skills) and policy barriers to the supply of services across European borders (i.e. a Single Market problem). There is a significant shortage of computer engineers and labour with the right IT skills, e.g. in artificial intelligence. The lack of supply of educated labour naturally creates a wedge between large multinationals (that can draw on international supply and expertise) and the smaller home-oriented firms.

There are clear and direct policy implications that follow from these observations. None of them implies shutting foreign providers off from Europe. On the contrary, without them Europe would be even less sovereign when it comes to having the autonomy to access, understand and use digital opportunities. In the area of data, Europe's policy-makers should rather work towards making more data publicly available, starting with public data, and then allow citizens to use the best infrastructure and software tools available to nurture the next wave of data innovations.

Secondly, and related, Europe can improve its own capacity by reducing the barriers to cross-border supply of digital services. Business statistics indicate that companies in the EU find it harder to grow compared to companies in the US. The average number of employees of a large US company is about twice as high as the average number of employees of a large company that is based in the EU. These numbers indicate that in the past it was generally easier for US companies to scale than for companies in the EU. This situation seems to persist: of the top 10 companies in the US, five are less than 20 years old, while all of the top 10 companies in Europe are more than a century old (CSIS 2020). Compared to companies in the EU, US businesses benefit from less legally restricted and therefore easier access to a greater US consumer base (Table 3). In other words: the United States Single Market is more complete than the common market shared by EU Member States.

TABLE 3: THE EU'S DISTINCT PRODUCTIVITY PERFORMANCE GAPS

Productivity gaps of high number of firms	Productivity gaps in entire industries	Some Digital Flagship" Member States
▪ Too many EU organisations lag in their adoption of past and current waves of ICT ▪ Considerable gap between leading firms and "zombie firms", i.e. firms with low productivity growth and limited ICT adoption) ▪ EU has a significantly larger share of employment in small, relatively low-productivity, low-ICT-using firms protected by public policies ▪ Lack of policy environment that provides incentives to not get big, as getting big brings with it a host of regulatory and tax obligations.	▪ Productivity gaps not just between firms but industries ▪ ICT adoption is less even between European industries than it is in the US ▪ Firm-level productivity gaps lead to distinct productivity gaps of entire Member State economies	▪ Yet: some EU nations, such as the Nordic nations, are on par with, or even ahead of, the US. But many other EU nations, including the EU-10 and southern EU nations, lag significantly behind EU leaders in ICT development and adoption.5

Source: ITIF (2019).

Similarly, most companies in the EU are SMEs (99%). However, business statistics also demonstrate that despite a much smaller total population, the US is home to a far greater number of SMEs than the EU. Adjusted by the size of the labour force, the number of SMEs in the EU is still significantly lower compared to the US. The EU's "SME deficit" in large SMEs (50 to 249 employees) is 36%, while the EU's SME deficit in medium-sized SMEs (20 to 49 employees) is 25% (Table 4).

TABLE 4: THE EU'S DISTINCT SME PERFORMANCE GAPS

Significantly lower number of SMEs in the EU	Lower number of growing/large SMEs	Single Market still disproportionately benefits large businesses
▪ US Census and Eurostat statistics demonstrate that the US is home to a far greater number of SMEs than the EU ▪ Normalised by the number of working age population, the number of SMEs in the EU is generally significantly lower compared to the US ▪ The difference in the number of SMEs per 1,000 workers is particularly pronounced for companies with 50 to 249 (EU) and 299 (US) employees. Standardised by the size of the labour force, the "EU SME deficit" in large SMEs with 50 to 249 employees is 36%, while the EU SME deficit in medium-sized companies with 20 to 49 employees amounts to 25%	▪ EU businesses find it harder to grow compared to companies in the US ▪ The average number of employees of a large US company is about twice as high as the average number of employees of a large company that is based in the EU (2,150 for large US companies; 1,022 for large EU companies). These numbers indicate that, due to a less restricted access to a greater consumer bases, in the US, it is easier for US companies to scale than for companies in the EU.	▪ Many SMEs in the EU benefit from the Single Market ▪ Yet: the share of large EU companies that trade across EU borders (55%) is substantially higher than the share of SMEs that trade across EU borders (20% to 40% for medium-sized companies) ▪ The larger a company, the more likely it is that it trades across EU and non-EU borders ▪ The Single Market still disproportionately benefits large businesses, which are better equipped to successfully cope with differences in sector-specific or horizontal laws and regulations

Source: ECIPE (2020).

[5] In May 2004, 10 countries joined the EU: Cyprus, Czechia, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovenia and Slovakia. Similar considerations apply for Bulgaria, Romania and Croatia. In January 2007, Bulgaria and Romania became members of the EU. The latest country to accede was Croatia on July 2013.

In fact, a market that is more single will have a direct impact on reducing these gaps. A more complete single market would also close the gap between European firms at the frontier and those that are distant from the frontier. It would allow European SMEs and start-ups to innovate and scale to competitiveness. A more complete single market that encourages entrepreneurship would also increase the likelihood of "more radical innovation": new firms that are more likely to commercialise radical innovation than incumbents.[6]

The importance of a real European Single Market is increasingly emphasised by the new Commission. In its 2020 Single Market Barriers report, the Commission acknowledges the "cost of non-Europe" and outlines a number of "frequently reported" policy obstacles and highlights Member States' resistance to properly transpose, implement and enforce EU Directives (European Commission 2020f). However, it remains to be seen if these observations will form part of a powerful agenda for revitalising the Single Market and make Europe more friendly to digital investment and innovation.

Commissioner Vestager has pointed to the non-existence of a real European Single Market several times, and she has made the point that regulatory fragmentation is at the heart of Europe's underperformance in digital industries. In her opening statement in the European Parliament Hearing in October 2019 on a "Europe fit for the Digital Age", she praised the Single Market and the digitalisation of European economy. She argued that "our Single Market gives European businesses room to grow and to innovate and be the best in the world at what they do" (Vestager 2019). Vestager also stated that "as global competition gets tougher, we'll need to work harder to preserve a level-playing field […] [b]ecause Europeans deserve an economy where companies compete to serve customers better not just to get bigger subsidies from government."

In February 2020, Commissioner Vestager followed that up and said that "[o]ne of the reasons why we don't have a Facebook and we don't have a Tencent is that we never gave European businesses a full single market where they could scale up […] Now when we have a second go, the least we can do is to make sure that you have a real single market" (Politico 2020b).

Policy-makers in many European capitals have in the past objected the development of a complete and deep single market, and they have done so because it would entail a loss of control or a loss in national sovereignty on their part. For example, under the Juncker Commission the regulatory restrictiveness increased in many of the EU's service industries, sectors that are relevant for cross-border commerce in the EU. EU and Member State governments defended national laws regarding these sectors and generally failed to give up on own regulations, with adverse effects on businesses using these services.

The EU's exclusive focus on perceived digital barriers has created another problem. Current political rhetoric and the latest communications from the European Commission demonstrate that Europe's political leaders are still largely ignoring the need to implement fully harmonised EU rules for trade in a truly common European market. The promotion of politically "easy-to-sell" digital policies distracted public attention and political capital away from the fragmentary nature of the Single Market. EU governments continued to use their legal competences to implement laws and regulations that, on aggregate, resulted in more differences (layers) in Member State regulations, increasing confusion and uncertainty for EU businesses and consumers respectively.

A more complete Single Market would essentially entail that countries and firms would make themselves more dependent on each other, which is the reality of modern business and the inter-

[6] Due to incumbents' established processes and management practices (Henderson and Clark 1990); incumbents' rigidity due to accumulated organisational and technological knowledge (Christensen and Bower 1996); incumbents inability to lead several technological waves (Benner and Tushman 2002); and incumbents' fears to cannibalise own markets.

national division of labour. No firm can excel at everything and they have to draw on the inputs and services from others to be competitive. To increase the autonomy of firms – their capability to better manage their own future – they have to become less independent.

A recent example of command-and-control thinking in EU digital policymaking can be observed in the EU thinking of future regulation of artificial intelligence (AI). While European policy-makers have embraced the promises of AI, including in mitigating the Coronavirus and future pandemics, they have often started on a defensive note, fearing that the development may lead to outcomes they cannot control. A new idea that has been going around European capitals in recent time is the concept of establishing a sort of "conformity assessment" for AI, based on testing the applications before they can be marketed in the EU (European Commission 2020e).

There are some obvious practical implications of such an idea: there is generally an AI skills shortage in Europe, and this shortage is even stronger among government agencies. A process of ex-ante testing of AI applications risks becoming a time-consuming affair that will slow down the market entry of technologies that would help Europe's industry to improve their performance and competitiveness. A bureaucratic EU AI testing system would almost guarantee that Europe would always run behind the USA and China in the global AI race, in particular for European SMEs with little capacity to handle administrative burdens. The proposed system will inevitably have adverse feedback effects on downstream sectors. As outlined in the EU's 2019 R&D Investment Scoreboard: "Big Data and AI can be broadly applied in most sectors [of the economy]. Looking at the sector level, AI and Big Data are also most widely considered as highly relevant for future competitiveness" (European Commission 2019c).

Another concern is that the system will provide opportunities for the EU to deny market access for AI applications from other countries. It has long been established by economic research that a licence-to-operate procedure has negative consequences on competition and dynamic market behaviour, and there are clear risks of that kind in this case as well. Remove sufficient AI skills among authorities and there is a risk that the actual testing of foreign AI applications would be outsourced to firms in Europe that are competitors to the firm that apply for an AI market licence. This conflicts with EU policies to protect intellectual property rights and trade secrets, which are at the heart of Europe's knowledge-driven economies.

Ex-ante conformity assessments would incentivise European companies to relocate to other jurisdictions, most likely the US, where they can launch immediately rather than wait for EU approval. The EU's scarce AI expertise would be spent on testing the AI innovations created elsewhere. Non-EU technology companies would reconsider engagements in the EU because of high compliance cost, bureaucratic hurdles and the risk that their knowledge falls into the hands of potential competitors. From a dynamic perspective, mandatory conformity assessments would worsen the EU's R&D investment gaps and exert a negative impact on European firms that are prevented from the application of Big Data and AI solutions.

The process forward for an effective form of control is to work with non-European governments that share Europe's view of rights and associated regulations. A licence procedure only gives the semblance of being in control of the actual concern, while it provides ample opportunities to rig market rules and approvals in a way that lead to fewer opportunities for European firms to access AI applications on competitive terms. Fewer opportunities, together with potential retaliatory measures targeted at European businesses in non-European markets, would leave the EU with a profound loss of autonomy and sovereignty.

3.2. European Responses to Stronger International Competition: Competitiveness

A major concern behind the calls for technology sovereignty is the fear of declining industrial competitiveness and international relevance – leading to less influence shaping new international standards for industries.[7] Our third C – competitiveness – thus reflects the widespread (but misplaced) anxiety that Europe is inevitably on the decline and that competitiveness can only be rescued by direct and indirect industrial support. In this section, we will take a closer look at some initiatives that are associated with such views, of which some manifestations are outlined in Table 5.

TABLE 5: EUROPEAN POLICYMAKERS' STATED MOTIVATIONS FOR DIGITAL POLICIES: COMPETITIVENESS

"Europe only accounts for 10% of tech indicators. We cannot accept this situation. Our sovereignty and the jobs of tomorrow are at stake. ChooseFrance"	Cedric O, French Digital Minister, Twitter, 19.9.2020.
"Europe's quest for tech sovereignty is as much about the United States as it is about China."	Guillaume Poupard, French Chief Cybersecurity Official, Politico, 10.2.2019.
"It is not too late to achieve technological sovereignty in some critical technology areas. We will jointly define standards for this new generation of technologies that will become the global norm."	Ursula von der Leyen, European Commission President, Politico, 28.10.2019.
"On digital sovereignty, you know that this is one of the projects that the President of the Republic defends with great determination and that we want to implement here. European digital sovereignty involves a number of projects, notably the future European cloud, which must be linked to our sovereign cloud projects in France. We will therefore look in the coming weeks at how we articulate the French sovereign cloud project, which is progressing well and which should be able to be implemented in the coming months, and the European cloud project. The two projects are completely complementary and must make it possible to guarantee national and European sovereignty over the data. I repeat how sovereignty over data, especially industrial data but also health data, is absolutely strategic for our country and for the European continent. Today there can be no political sovereignty without sovereignty over the data."	Bruno Le Maire, French Minister for Economy and Finance, Joint Declaration with Thierry Breton, 7.2.2020.
"We are determined to ensure that these industrial data, which will emerge in the weeks, in the months, in the coming semesters, in particular through the development of critical networks, such as for example the 5G networks which have been talked about a lot lately, will effectively allow completely new applications which will concern the city, the smart city, the hospital, the transport networks, the energy networks. All of this, obviously, will mobilise absolutely considerable numbers of data, which will be processed more and more locally, where they are produced, with a whole new architecture that must be designed at the level of the European continent."	Thierry Breton, Internal Market Commissioner, Joint Declaration with Bruno Le Maire, 7.2.2020.
"The new Commission must therefore encourage the development of major European players who will allow the entire industry of yesterday to play on an equal footing with that of tomorrow. It is also necessary to promote artificial intelligence in all aspects of economic life to preserve our sovereignty and our competitiveness."	Thierry Breton, Internal Market Commissioner, quoted in Les Echos, 5.7.2019.
Gaia-X would be a "competitive, safe and trustworthy data infrastructure for Europe", said Mr Altmaier, adding that a Europe-run cloud system would "help restore our digital sovereignty" and serve as a "basis for a digital ecosystem".	Peter Altmaier, German Minister for Economy, quoted in Financial Times, 11.11.2019.

[7] Reding (2016, p. 1-2), for example, argues that the "EU is the largest economic and trading block in the world but is at risk of losing its digital sovereignty – its capacity to influence the norms and standards of the information technology that play a crucial role in 21st century development." She continues stating that "[s]overeignty 'is the capacity to determine one's own actions and norms'. It is easy to agree on this general definition. But the deep sense of sovereignty lies in our actions. We can use it to build borders and fences, thereby transforming ourselves into islands. That's what some European politicians risk doing, when they get lost in a maze of motley national prerogatives. If you think small, you stay small, giving up all possibilities to shape globalisation."

"Germany has a claim to digital sovereignty. That's why it's important to us that cloud solutions are not just created in the U.S."	Peter Altmaier, German Minister for Economy, quoted in Euractiv, November 2019.
"So we have both decided to create a European alternative for a sovereign data infrastructure".	Peter Altmaier, German Minister for Economy, quoted in Reuters, 19.9.2019.
"Here is how we avoid becoming a digital colony: after exchanges with civil society, private sector and politics, you can find my proposals on how to improve our digital life over the next 5 years. Protect our digital sovereignty with DSM 2.0."	Axel Voss, MEP, Twitter, 20.1.2020.
AWS cloud services are like a "soft drug. The more you take it, the more you like it."	Agnes Pannier-Runacher, French Deputy Minister for Economy, quoted in Atlantic Council, 11.12.2019.
"We need to have cloud infrastructure in Europe. And maybe in the near future we ask that European data to be stored, processed in European clouds ... Data should probably remain in Europe just because we want only European laws and rules to apply to it."	Guillaume Poupard, Chief Cybersecurity Official, France, quoted in Politico, 10.2.2020.
"[...]the third paradigm shift is technological: technology is an issue, as well as a disruptor and a referee in strategic balances. The deployment of 5G, data storage on the Cloud, as well as operating systems are strategic infrastructure in today's world. In recent years, we have too often considered that these were commercial solutions, simply industrial or private-sector issues, while what we are talking about here are strategic infrastructure, for our economies of course, and for our armed forces.	Emmanuel Macron, French President, Speech, 7.2.2020.
"European freedom of action requires economic and digital sovereignty. European interests, which Europeans alone should define, must be heard. It is Europe's job to define the framework for regulation that it imposes on itself, for it is a matter of protecting individual freedoms and economic data of our companies, which are at the core of our sovereignty, and of our concrete operational capacity to act autonomously.	Emmanuel Macron, French President, Speech, 7.2.2020.
"European digital sovereignty is the strongest tool for us to carve out a space for ourselves in the modern world," Cutajar said, adding that the dream of European digital sovereignty will remain a mere concept unless Europe is able to promote its digital champions "in third countries".	Joseine Cutajar, MEP, quoted in Euractiv, 5.11.2019.
"Today I've asked [the] next Commissioner for Internal Market for a true EU digital sovereignty and less protectionism to compete on a global scale. Europe cannot be a US or Chinese digital colony."	Esteban Gonzales Pons, MEP, Twitter, 14.11.2019.
"We cannot allow that the US seek to stop us taxing tech giants. A Digital Services Tax is key to ensure all pay their fair share. The EU should stay united behind France during this American assault – to defend our sovereignty."	Paul Tang, MEP, Twitter, 8.1.2020.
"We will look at all possibilities if any tariffs or measures are imposed by the United States. The European Commission will stand together with France and all other member states who wish to have the sovereign right to impose digital taxation on companies in a fair way".	Phil Hogan, Commissioner for Trade, Financial Times, 7.1.2020.
"We need a kind of Airbus for AI"	Peter Altmaier, German Minister for Economy, quoted in Reuters, 4.1.2018.
"Competition law should especially apply to tech giants because they are those who are monopolistic in the world... those who reach incredible levels of capitalization, who manage to combine activities which should normally be separated."	Bruno Le Maire, French Minister for Economy and Finance at Politico & Agefi Finance summit in Paris, 6.2.2020.
"My personal feeling is that we should not rule out dismantling [systemic platforms] ... at least to keep a means of pressure. We would be wrong to rule out structural remedies for diplomatic reasons," O said. The politician recommended focusing on the "three or four [companies] that really pose problems." Earlier in his speech, he mentioned Google, Amazon and Facebook. "If the Americans resolve the issue on their side with their legal framework and their values before we're able to set a European framework, it will be harder for us."	Cedric O, French Digital Minister, Politico, 24.2.2020.
"If we want technological sovereignty, we'll have to have to adapt our competition law, which has perhaps been too much focused solely on the consumer and not enough on defending European champions."	Emanuel Macron, President of France, Politico, 18.5.2020.

Source: ECIPE.

3.2.1. Classic Industrial Initiatives

Policy-makers pointing to the "need to create" truly European industrial champions tend to disregard that many EU-based companies still hold very strong global positions in a wide range of industries. Similar to the US, EU patterns of specialisation and R&D activity remained relatively stable over the past decade (European Commission 2019d). Industry intelligence shows that European companies are still particularly strong in the automotive sector, environmental technologies and machinery sectors. Moreover, political claims regarding the lack of "European champions" – a frequent reference in the debate about European technology sovereignty – also neglect to mention that many technology and Internet companies, which successfully operate across the EU and globally, are actually headquartered in the EU, e.g. France's Atos, Germany's SAP, Poland's Allegro, Sweden's Spotify, Finland's Wolt and many other (see, e.g. ECG 2020).

Companies in more traditional sectors such as carmakers are increasingly moving towards more digitised business models across their product and services portfolios. In the area of autonomous driving, for instance, numerous EU operators are partnering with international firms and taking part in autonomous vehicle (AV) testing abroad. The European Commission has welcomed such international cooperation for connected and autonomous vehicles. That, however, has not stopped some companies from proposing limits on AV competition and market access in the EU (see, e.g., El Referente 2019).

Despite these patterns and the general trend towards the digitalisation of traditional industries, the governments of France and Germany have taken the lead in shaping the design for new "all-EU" industrial policies. The influence has also shaped the Commission's recent policy communications. However, complaints by smaller states about the drive for a new industrial policy is often passing unnoticed in Brussels. A recently launched campaign, led by the government of Lithuania, aimed "to stop Brussels' focus on industrial strategy from stealing the show". Marius Skuodis, Lithuania's Vice-Minister for Economy, has said that the Single Market has been sidelined by discussions about the EU's industrial policy (Politico 2020c). The governments of nine smaller Member States have underlined the urgency of the Single Market as a response to big-ticket industrial policy. Lithuania was joined by Denmark, Finland, Sweden, Ireland, Latvia, Estonia, the Netherlands and the Czech Republic. They have a point. Attempts to defend national industries have always clouded European attempts to create competitive markets.

3.2.1.1. European Data Sovereignty: European Clouds

The German Chancellor, Angela Merkel, warned in a speech late last year about Europe having "dependencies" on foreign firms – predominantly US technology firms. Germany's Economic Minister, Peter Altmaier, has argued that Europe "is losing part of our sovereignty" when firms and agencies have to store their data on cloud platforms such as Amazon and Microsoft (CDU 2019). Gaia-X would be a "competitive, safe and trustworthy data infrastructure for Europe", said Altmaier, adding that a Europe-run cloud system would "help restore our digital sovereignty" and serve as a "basis for a digital ecosystem" (FT 2019). Gaia-X was created by the German Government and later supported by the French Government. It is however not (yet) an EU project and its outcomes remain unclear. This data governance project could potentially become a driver for cloud adoption, with high security and privacy standards, to the benefit of cloud services to public and private organisations.

Germany's recent federal cloud data initiative, which aims to become the "cradle of a vibrant European ecosystem" was mainly "conceived and drawn up" by representatives of Germany-based firms. France' Finance Minister Bruno Le Maire recently stated that France has enlisted tech companies Dassault Systemes and OVH to "break the dominance of U.S. companies in cloud computing" (Reuters 2019).

3.2.1.2. European Payments Sovereignty

Launched in November 2019, around 20 European banks from eight Eurozone countries are now supporting a new European payment system to challenge leading non-European payment services providers such as Visa, MasterCard, AliPay, Apple, Google and WeChat Pay. Banks headquartered in Germany and France make up a large share of this "European Payment Initiative" (EPI) project membership. A decision on whether or not to pursue the EPI is expected at the earliest in mid-2020.

The EPI project enjoys strong support from the European Central Bank (ECB), which for a long time has criticised the inability or unwillingness of European banks to develop a pan-European payment system. In 2010, 12 banks from eight countries joined the Monnet project, a consortium aimed at creating a European card scheme. The Monnet project was initially launched by major French and German banks but the project failed shortly after over lack of clarity on a sustainable business model.[8]

Renewed motivations for pursuing a regional European payments player with global reach are multi-faceted, with geopolitical considerations understood to be one of the key catalysts. On 26 November 2019, Benoît Cœuré, the former French Member of the Executive Board of the ECB, welcomed that Europe's banks are consolidating efforts to set-up a new pan-European payment system. Cœuré warned that

> [d]ependence on non-European global players creates a risk that the European payments market will not be fit to support our Single Market and single currency, making it more susceptible to external disruption such as cyber threats, and that service providers with global market power will not necessarily act in the best interest of European stakeholders.

He added that Europe's "[s]trategic autonomy in payments is part and parcel of the European agenda to assert the euro's international role." At the same time, Cœuré admitted that consumers increasingly demand payment services that work across borders and that are faster, cheaper and easier to use (ECB 2019).

Similarly, in March 2019 the European Commission was reported to be considering new regulations to support and accelerate the adoption of the ECB's new instant payments settlement system in an effort to challenge popular card and technology companies in Europe. In June 2019, the Commission formally announced that it was exploring policy options to strengthen the role of the euro and bolster its global relevance, and to "increase the autonomy of payment solutions in Europe and challenge the dominance of American and Asian apps and cards that Europeans use for their cross-border payments" (European Commission 2019). Similar to the ECB, Dombrovskis added in March 2020 that "[p]ayments matter because they are also a way to boost the international role of the euro".

However, an EU-only retail payment system will hardly reinforce the international role of the euro. Nor will it provide the EU with a new option, which already exists with Instex[9], to allow for some trade with countries when there is, for example, an EU-US divide over sanction policy. Also, retail banking or payment systems have not been subject to blanked prohibitions under US sanction policy.

[8] BNP Paribas, BPCE, Crédit Agricole, Crédit Mutuel, La Banque Postale, Société Générale, Deutsche Bank, DZ BANK, Postbank (French Banking Federation 2010).

[9] The Instrument in Support for Trade Exchange (Instex) is a European special-purpose vehicle established in January 2019. Its mission is to facilitate non-USD and non-SWIFT transactions with Iran to avoid breaking US sanctions.

Moreover, payment networks and users of payment services alike are interested in network security and resilience, data protection and trust as well as transactional efficiency and innovation. Users go to these networks partly because they offer resilience and high levels of security. Policy-makers promoting purely European infrastructure solutions, such as the EPI, need to be clear about this. International payment networks have the ability to route via multiple data centres around the world: local systems usually don't. International networks can rely on access to global data for cyber threat analysis, which allows for the detection of fraud outside of Europe in order to react faster to threats to Europeans. In a world where crime, especially cybercrime, travels across borders, national or siloed payment systems are more vulnerable to attacks because they lack global analytics and real-time global warning systems. Globally organised cybercrime, like cash-out attacks, are more likely to be detected and/or prevented through real-time analytics of big data, e.g. through a "rich global data lake of retail banking activity" leveraging machine learning and artificial intelligence (FICO 2018, Enisa 2016).

Consequently, a European payment initiative will not improve privacy or the security of payment data. The geographic location of data has no bearing on the security of that data, neither does it increase data privacy. Data security critically relies on the security systems and protocols that organisations have in place, regardless of where the data is stored.

Moreover, a purely European approach – in the name of technology sovereignty – would slow down innovation. For example, European FinTech players, such as Revolut and Klarna, benefit from their collaboration with global payment networks, particularly as it facilitates their expansion beyond European markets. The continued success of European FinTechs hinges on working collaboratively and interdependently with leading global companies.

If Europe wants to stay ahead in payment innovation and encourage the emergence of European FinTech players, it is better to promote innovation and set open standards that facilitate collaboration and exchange, rather than build new infrastructure and/or seek to regionalise the payment value chain. European regulation, such as the Payment Services Directive 2 (PSD2), through a focus on standard setting, has already paved the way for open finance to flourish and created new opportunities for innovations that consumers need and want to adopt. However, Europe's homegrown FinTechs all largely operate within their own national borders, without a Single Market in retail banking or payments. Therefore, attention should be given to removing obstacles to allow these EU FinTech players to develop across national borders and become pan-European players.

3.2.2. Protectionist Interpretations of Technology Sovereignty

Even though there is little detail about concrete policies, the EU's Industrial Policy Strategy seems to be guided by fears of being locked in a US-dominated cloud space without any European champion. It is therefore no surprise that some initiatives run the risk of stoking European protectionism. It is equally unsurprising that foreign governments have identified that threat.

However, the Covid-19 crisis has shown that reliance on foreign technologies is not a threat to European autonomy. First, during the confinement period technologies and tech companies made Europeans – and their governments – stronger. Technology kept Europe open for business despite the lock-down by enabling Europeans to work from home, access to computing power via cloud solutions, receive essential home deliveries, home schooling, online banking, etc. Europe's citizens became more sovereign with respect to accessing information and authorities used data to track and contain the spread of the virus.

Secondly, the crisis tested Europe's resilience and perceived dependency on (foreign) technology solutions. Early findings indicate that homemade solutions didn't fare better than existing European and international solutions. For example, a remote teaching tool by the French government failed to offer support for all those that needed online teaching. A few national prestige solutions

failed while existing European and global solutions, from cloud infrastructure to communications, payments to streaming services, all continued to work. Many tech companies have acted swiftly to address concerns, e.g. by reducing bandwidth consumption to avoid congestion.

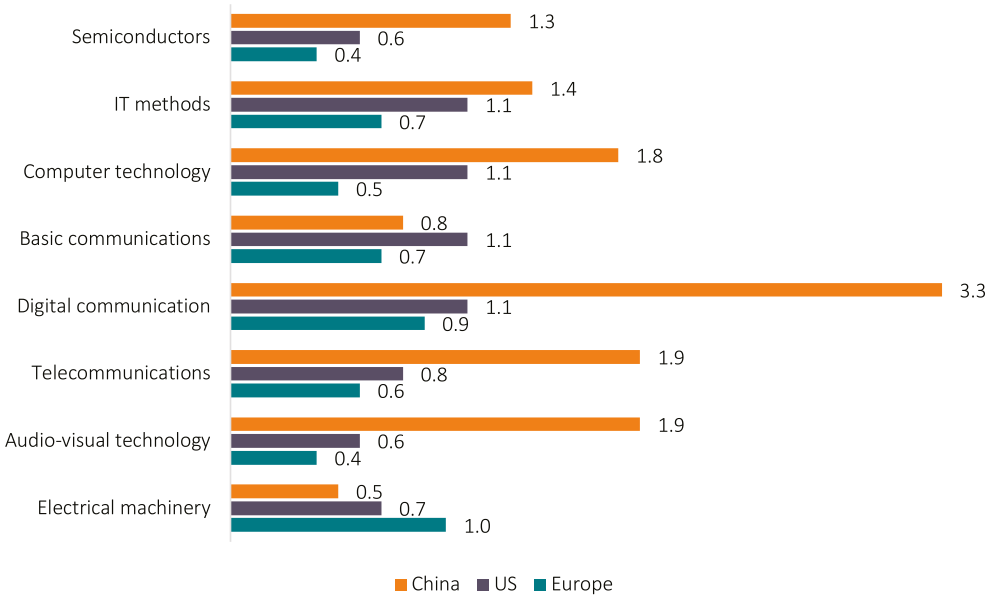
Obviously, some politicians might ignore this new evidence and capitalise on the crisis by calling for a more protectionist understanding of technology sovereignty. Policy-makers should however recognise that Europe benefits substantially from the technologies and services offered by innovative, domestic and foreign, technology companies. A misguided attempt to hinder access to the most popular foreign tech companies would leave Europe with less competition, less choice and less access to innovation.

A recently published report from the EU's Joint Research Centre (JRC) and the OECD, for example, comes to the conclusion that EU businesses are indeed significantly lagging behind in terms of their innovative capacities. Based on data for patents, trademarks and scientific publications of the world's top corporate R&D investors, JRC-OECD (2019) investigates the role of key industry players in shaping the future of technologies, and of AI in particular. It is shown that until 2016, businesses in the EU-28 and Switzerland continued to be specialised in largely the same fields of technology as in 2010-2012. It should be noted that the same pattern holds generally true for US-based companies, which continued to be specialised in the exact same technologies in which they were specialised in 2010-2012. As outlined by Figure 1, US (and Chinese) companies outperform European companies (EU-28 and Switzerland) in new (ICT and AI) technologies that are increasingly important for more traditional sectors.

These are sectors in which European companies are currently relatively strong, e.g. automobiles and parts, healthcare, environmental technologies and machinery equipment (as outlined by Figure 2 and Box 3). Europe's automotive and other transport sectors perform the largest proportion of their R&D activities within the EU. Based on the very strong past performance of the EU's automotive sector and the high specialisation of the EU, more than 90% of the research activities still take place in the EU. On the other hand, European companies show a significant technological disadvantage in semiconductors, IT methods, general computer technologies, basic communications technologies, digital communications technologies, telecommunications technologies, audio-visual technologies and electrical machinery.

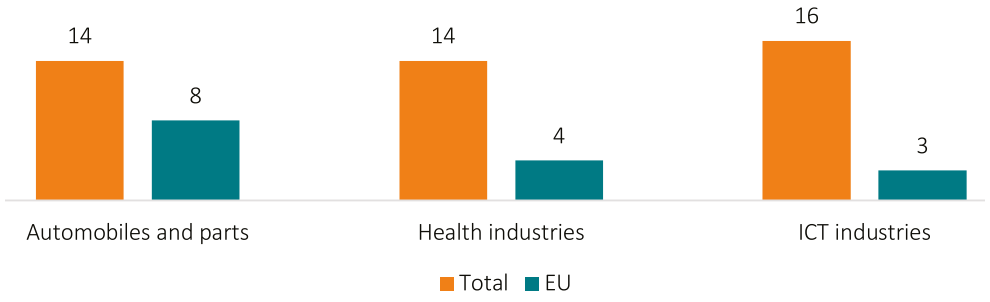
With regard to new technologies, as outlined by the EU's 2019 R&D Investment Scoreboard, "Big Data and AI can be broadly applied in most sectors [of the economy]". Looking at the sector level, AI and Big Data are also most widely considered as highly relevant for future competitiveness, with being among the top three technologies in six out of eight sectors. These technologies will have the most diverse application possibilities. This can also be seen in the joint study of the JRC and OECD on patents in the field of AI, where AI is both widely used but also developed in sectors that are traditionally low ICT-intensive. Other ICT-related technologies are considered as much less important for future competitiveness. The relevance of other technologies, such as I4.0 and Robotics, is much less widespread. ICT services and ICT hardware technologies are not mentioned amongst the most relevant technologies for future competitiveness in any of the sectors. Europe's current technology gap in many ICT or digital technologies may thus put at risk the international competitiveness of companies that are still strong in traditional, less digitalised industries, such as Europe's carmakers and machine manufacturers.

FIGURE 1: REVEALED TECHNOLOGY ADVANTAGE (RTA) OF WORLD'S TOP R&D INVESTORS, 2014-16, BY FIELD OF TECHNOLOGY AND GEOGRAPHICAL LOCATION OF HEADQUARTERS



Source: JRC-OECD (2019, p. 30). Note: RTA indices were compiled for the major economic areas where the top worldwide R&D investors have their headquarters. The index value is computed using the IP5 patent families. The RTA is defined as the share of patents in a field of technology for an economic area, divided by the share of patents in the same field at the global level. The index number is zero companies headquartered in an economic area hold no patent in a given technology. The index value grows with the increase of the patent share in the given technology.

FIGURE 2: DISTRIBUTION OF THE TOP 50 COMPANIES BY MAIN INDUSTRIAL SECTOR, 2018



Source: EU R&D Investment Scoreboard 2019.

BOX 3: EU-BASED COMPANIES HOLD A STRONG POSITION IN THE AUTOMOTIVE SECTOR AND IN ENVIRONMENTAL TECHNOLOGIES

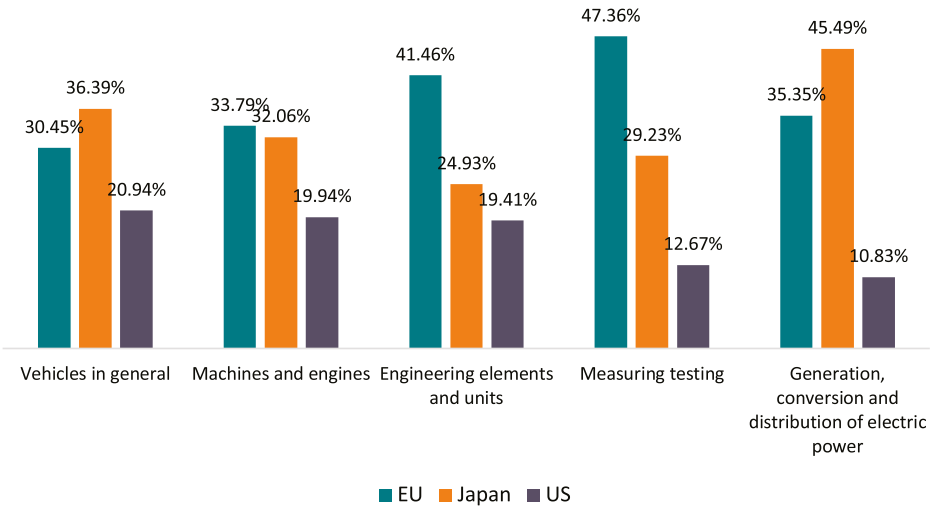
According to the EU's R&D Investment Scoreboard 2019, the automotive sector owns 13% of total patents belonging to the Scoreboard companies. EU companies hold 30%.

Most of these patents refer to current automotive technologies but an increasing proportion refers to green technologies, including electric and autonomous vehicles and newer components such as novel batteries and fuel cells. EU companies appear highly diversified and competitive in most technological fields, but in green technologies related to hybrid cars, batteries and fuel cells their Japanese counterparts are leading the race.

Yet, for new technologies, the EU's automotive companies are being joined in patent filing by companies from the software, IT hardware, electronics and chemicals sectors. This can become a major challenge for EU businesses, whose lead in the automotive sector may be eroded as digital technologies take a higher proportion of the value added in this sector. Several European carmakers are partnering with technology companies, e.g. in the development of autonomous vehicles.

As concerns environmental technologies in general, EU companies are strong innovators. According to the distribution of patent families on environmental technologies, EU-based firms own 27% of the respective patents, US companies hold 23% and Japanese companies hold 37% in total. Compared to Japan and the US, EU businesses are relatively strong in environmental technologies in the automotive sector, machines and engines, engineering elements and units, measuring testing, and the generation, conversion and distribution of electric power.

Share of patent families by world region, by number of patents



Source: EU R&D Investment Scoreboard 2019.

Industry data indicate that the EU performs poorly with respect to R&D activities and the number of companies that successfully commercialise digital technologies and business models. The European Commission is generally right in arguing that a different regulatory framework and new policies are needed to secure the competitiveness of key European sectors, including ICT and digital industries. However, current perceptions on a European technology sovereignty are unlikely to remain static. The next wave of technological innovation, which, according to ITIF (2019, p. 3), "holds the potential to reverse the 20-year productivity growth lag [in and beyond ICT industries] suffered by the EU", will alter political attitudes towards sector priorities and policies respectively.

Many Member States are already home to large Internet and technology companies and innovative start-ups. Europe's leading technology companies, e.g. France-based Atos and Criteo, Poland-based Allegro, Germany-based SAP, Finland's Wolt, Sweden's Spotify and others, ben-

efited considerably from the last technology wave, including Internet-based intermediations, mobile communications, cloud and online payment services. Many European information technology firms innovated and adapted. Others were successful entrepreneurial tech start-ups. At the same time, many of Europe's information technology firms were unable to scale up at the same speed as US technology firms and, to a somewhat lesser extent, successful Chinese Internet giants, which also strive for global market-leading positions.

Protectionist interpretations of technology sovereignty would add to existing tensions in international trade and investment policy, provoking retaliatory measures against Europe's strong export industries. The current debate about how to relax EU competition rules to support European industrial champions, while at the same time tightening them through ex-ante rules and mergers and acquisitions (M&A) scrutiny to limit foreign tech giants, is considered a major provocation by the EU's main trading partners. European politicians should abstain from picking winners and losers.

Picking politically well-connected companies would inevitably distort markets. Subsidies would have a crowding-out effect on private sector risk-taking and investment in the EU. Special taxes on digital services, aimed at foreign technology companies, are discriminatory by design. They would be largely borne by the users of digital services and unnecessarily provoke retaliatory measures (Bauer 2019).

3.3. European Responses to Internet Security Risks: Cybersecurity

The fourth C in the European debate about technology sovereignty is cybersecurity. European concerns about cybersecurity are generally about the safety of business and personal data in an increasingly global data environment. And these concerns are shared by governments, businesses and citizens across the EU. Cybersecurity threats are both big and increasing, and they are shared by each one of Europe's allies. These threats often tend to come from certain governments with little interest in freedom and democracy, with the aim of eroding current structures of international economic policy.

With regard to commercial data, the emergence and application of new technologies, such as cloud services, the Internet of Things (IoT) and 5G, has changed the strategic paradigm for protecting European commercial interests (Lee-Makiyama 2018). Critical commercial information, e.g. on contract negotiations, customer and marketing data, product designs and R&D, are commonly uploaded to clouds today. With respect to personal data and consumer protection, policy-makers are generally concerned about data privacy and potential harm to citizens and consumers caused by cyberattacks. These concerns have led to a number of regulations at EU and Member State level in recent years, e.g. the GDPR, the NIS Directive, the Cybersecurity Act, and the proposed e-Privacy Regulation proposal. However, European policy-makers wish to go further.

In its 2020 Digital Future Strategy, the European Commission highlights the risk of cyberattacks. It is argued that "malicious cyberactivity may threaten our personal well-being or disrupt our critical infrastructures and wider security interests (European Commission 2020b, p. 1). It is further stated that "[t]o tackle this growing threat, we need to work together at every stage: setting consistent rules for companies and stronger mechanisms for proactive information-sharing; ensuring operational cooperation between Member States, and between the EU and Member States; building synergies between civilian cyber resilience and the law enforcement and defence dimensions of cybersecurity; ensuring that law enforcement and judicial authorities can work effectively by developing new tools to use against cybercriminals; and last but by no means least, it means raising the aware- ness of EU citizens on cybersecurity." (p. 4)

In the case of consumer electronics and their rapid proliferation, policy-makers across Europe have already pushed for initiatives to improve consumer security, privacy and safety. Concerns about wider economic implications include risks from large-scale cyberattacks, e.g. concerted attacks launched from large volumes of insecure data storage applications and IoT devices. Policy-makers seek to address such risks through regulation and standardisation, e.g. the UK "secure by design" policies, Germany's IT Security Law and the EU's Cybersecurity Act, which (aim to) establish certification frameworks for ICT digital products, services and processes (DCMS 2018; BSI 2020; European Commission 2020).

Whether these measures help to make Europeans' data safer may be disputed. Regulatory actions may indeed contribute to safer devices and, perhaps more importantly, a more educated public with regard to the use of modern ICT devices and software applications. Harmonisation of Member State regulations on security standards would limit the regulatory burden imposed on businesses and consumers. At the same time, data residency and localisation requirements, e.g. within the scope of a "European Cloud", would neither increase the safety of Europeans' data nor allow Europeans to benefit from cutting-edge technologies and business solutions offered by superior foreign suppliers.

Europe's policy-makers need to ensure that citizens and businesses retain access and continue to benefit from new technologies and technology-based business models. At the same time, as highlighted by Lee-Makiyama (2018), cyber espionage is undetectable in most cases. Moreover, cyberattacks from government entities cannot be sanctioned under international law, so there is little potential for a UN-style solution. This situation is untenable to European policy-makers, and motivates calls for new diplomatic approaches, such as the proposal to condition market access on good government (no spying) behaviour by autocratic regimes.

Restrictions to market access might indeed serve as a workable lever to induce good government behaviour – after all, this is part of the rationale of economic diplomacy. However, such endeavours can also open the doors for new protectionist policies, and they can hurt EU allies whose support is needed in cybersecurity protection. Lessons can be drawn from the debate about the need to protect investments of strategic importance to Europe (see, e.g., Bauer and Lamprecht 2019). A sensible starting point could be the EU-US continuous dialogue on US law enforcement and national security laws during the Privacy Shield Framework annual review, and the potential prospect of a repeal of this data transfer tool should the Commission consider that US laws adversely affect EU citizens' data protection.

Similar to investment screening policies, the actual design of an EU cybersecurity framework needs to recognise the integrity of the EU's overarching economic policy objectives, particularly the EU's long-standing commitment to open markets and non-discriminatory policymaking (see, e.g., European Commission DG Trade 2015). With respect to China – whose government is a concern for Europe with respect to cyberattacks – policy initiatives on cybersecurity could seize the current moment of opportunity from the EU's negotiations of an investment agreement, committing China's government "not to spy", on the condition of sustained market access for Chinese trade and investment. If such a commitment were to be backed up by cooperation and review mechanisms, and restriction instruments used if other efforts fail, the chances of success would be higher.

Europe's policy-makers should recognise the risk of policy inconsistencies, e.g. the impacts of cybersecurity regulations on the integrity of the Single Market and international rules for trade and investment. New cybersecurity regulations need to be designed on the basis of scientific evidence regarding the actual impact on the safety of personal and commercial data rather than simplistic geopolitical considerations. European data localisation requirements, a frequently proposed policy (also pushed and enforced by the governments of China, India and Russia), would neither improve data safety nor reduce the number of cyberattacks from hackers and foreign

governments. Data localisation requirements would reduce Europe's technology sovereignty by reducing citizens' and businesses' access to trustworthy services. European data localisation requirements would also send undesirable signals to authoritarian governments, which do not share European values with respect to fundamental human rights, by empowering them to localise data to increase their capacities to spy on their own citizens. This would also contradict the goal of the GDPR and policymakers to export EU fundamental values to non-EU countries.

4. Recommendations Regarding Principles and Opportunities from Technology Sovereignty

The Covid-19 crisis has prompted Europe, and the world, to build resilient systems that draw on the energy, ingenuity and reliability of domestic and foreign firms. Given all that we have learnt from the pandemic, it points to a new ambition in Europe that puts less emphasis on independence and prescriptive policies towards a semi-autarkic EU. Defined in the right way, digital or technology sovereignty can improve the autonomy of Europe and its myriad of firms. An open approach to technology sovereignty can create new opportunities to compete at the frontier of technological development, with a positive impact on Europe's long-term global political influence.

Defined wrongly, the concept of technology sovereignty would reduce Europe's international competitiveness and saddle Europeans with technologies and businesses that are not globally competitive. A misguided form of technology sovereignty would only lead to notional sovereignty: while the EU would be free to adopt its "own" EU-originated technologies and standards, they would not provide the much desired economic and innovation benefits. In reality, such ambitions would render Europe obsolete in the shaping of international laws and norms that will guide the digital future.

The EU represents only 10% of the global population and most data in the world is therefore non-EU. Commission President von der Leyen rightly said that "we all know that the more data we have, the smarter our algorithms. This is a very simple equation. And therefore, it is so important to have access to data that are out there." While many people now are occupied by fears of exposing European data to foreigners, the future challenge will be for Europe to access the data of foreigners. Digital or data independence is not a realistic solution to achieve sovereignty with respect to technologies. Isolationist polices are attractive to those who think they will give them business advantages for a certain period of time. The reality is that it would undermine Europe's future ability to address specific concerns on data security and integrity. Protectionism and self-sufficiency in data or ICT technologies would reduce the global competitiveness of Europe's diverse industries, widening the EU's distinct investment and productivity gaps vis-à-vis the world's best performing jurisdictions.

By contrast, an autonomy-based approach to technology sovereignty needs to build on and improve Europe's ability to understand, access and use new technologies and technology-enabled business models, including technologies that emerge from the next wave of innovation in ICT. Such a programme will inevitably start with the provision of education and human capital. It also requires a strong, perhaps unprecedented emphasis of knocking down regulatory barriers in Europe's incomplete Single Market, which currently prevent the easy traverse of technologies, goods and services across borders. Importantly, conflicting national rules hinder European companies, including start-ups, to scale up and become globally relevant.

An autonomy-based approach will start from the acknowledgment that Europe is not a laggard on all accounts and that many European companies – small and large – bring goods, services and innovation to other regions. Like everyone else, Europe has strengths as well as weaknesses, and any policy programme to improve autonomy and effective sovereignty will have to start with addressing the specific weaknesses, without undermining the strengths.

Protectionist approaches like taxes on digital services or AI licensing obligations would generate negative market responses from other parts of the world. European firms – beyond those that provide technology and digital services – would be at risk of losing market access abroad simply because foreign governments would retaliate. European firms that sell goods and services abroad are at risk of being confronted with market-access restrictions because they have used inputs that are derived from a market that has been regulated to shut foreign firms out.

All of this should be obvious. Retaliatory responses are part and parcel of the reality of business politics and international economic diplomacy. For a Europe that runs a significant trade surplus with the rest of the world, especially in sectors that have high technology and data intensities, it should be a warning sign: protectionist policies would reduce both Europeans' future autonomy and prosperity. A Europe that cuts itself off from other advanced economies will ultimately lose its control over the future. It will also lose opportunities to set laws, regulations and norms together with like-minded countries. No part of the world could alone supply frontier technologies and services throughout the digital and technology supply chain. Just like in other parts of the economy, effective sovereignty – our ability to understand and access technology – comes from cooperation with others.

Finally, there is the important issue of trust. Command-and-control types of regulations have limited effects because the world of technology and data is complex and difficult to regulate in the same way as one can regulate steel or chemicals. A promising approach is to deepen efforts to cooperate with like-minded countries – countries that take fundamental rights seriously and that are on a similar quest to advance regulations that improve data security and integrity. There are many of them in the OECD community and collaboration with them is a necessary ingredient for a policy that will have the desired effect. It will also help to make European citizens and firms more autonomous and capable of using the opportunities technological change and globalisation can deliver.

To facilitate a more informed discussion about the merits of the EU's recently published digital, data, AI and industrial policy strategies, Table 7 outlines potential opportunities, policy inconsistencies and major pitfalls. The table outlines key aspects, which we assess against three potential policy inconsistencies at EU level: policy effectiveness (meeting the goals), efficiency (meeting the goals at minimum costs), and dynamic impacts (perspectives for Europe's future economic development).

TABLE 7: OPPORTUNITIES AND PITFALLS OF THE EU'S NEW INDUSTRIAL, ARTIFICIAL INTELLIGENCE AND DATA POLICY INITIATIVES

EU policy communication	Stated objectives (visions and goals)	Potential opportunities	Major pitfalls
European Commission: Europe fit for the digital age: Towards a truly European digital society	▪ European society empowered by digital technologies ▪ Digital technologies rooted in common values ▪ Regulatory framework that allows citizens to start up, grow, innovate and compete with large digital companies ▪ Digital environment that respects privacy, dignity and other rights	▪ A new industrial policy strategy can pave the way for a "Real European Single Market" for goods and services ▪ Given that Europe is still home to many knowledge-intensive industries and strong, research-oriented science organisations, a real Single Market could help Europe to catch up with more complete and thus much larger markets in China and the US ▪ Member States' corporate tax regimes negatively impact on investment. Policy proposals should generally aim for low corporate taxes and incentives for R&D investment. Corporate tax policies should be neutral to technologies and business models	Potential policy inconsistencies: ▪ Lessons need to be drawn from failed industrial policy initiatives at EU and Member State level, e.g. Quaero (a highly subsidised, but failed European search engine project) and Galileo (an overfunded European satellite system) ▪ New industrial policy (IPCEI type) state subsidies stand in opposition with the EU's state aid policies and may reinvigorate protectionist moods at Member State level ▪ New subsidies stand in opposition with the EU's trade policy agenda, which aims to contain disproportionate state aid, state interventionism and state-owned enterprises globally ▪ Changes in competition law could open doors for discretionary treatment of companies across industries (the picking of winners and losers), and empower Member State governments to combat proven competition EU practices and/or bypass EU competition law through a loose application of s tandards ▪ The aim to create European champions stands in opposition to the EU's "enabling" SME polices and the European Commission's commitment to a "Trade Policy for All", which is guided by the principle of non-discrimination Effectiveness (meeting the goals): ▪ New subsidies or exemptions in competition policy are inappropriate with regard to the objective to structurally increase international competitiveness across EU Member States ▪ The creation of a "Real European Single Market" for goods and services would be the most effective way to stimulate private sector investment (including FDI from abroad), innovation, economic activity and cross-border trade Efficiency (minimum costs): ▪ Europe's research-intensive companies were in the past very successful in applied research and innovation, but less successful in commercialising innovative technologies. A more complete – real – single market would increase the commercialisation of innovative technologies, in which European companies (as innovators and adopters) show a structural disadvantage ▪ New forms of subsidies are costly for taxpayers. Subsidies increase bureaucracy, lobbying and tie otherwise productive resources in businesses and governmental institutions Dynamic impacts (perspectives for future economic development): ▪ New forms of subsidies, exemptions in competition policy and government-supported European champions would discriminate against innovative companies and crowd-out private-sector activities, including SMEs ▪ Recognising the adverse impacts of subsidies on innovation and competitiveness, a subsidy-based industrial policy would likely result in an internationally less competitive European economy; lessons should be drawn from the poor innovation track record of European companies that are fully or partly owned by the state, e.g. in financial services and network industries

EU policy communication	Stated objectives (visions and goals)	Potential opportunities	Major pitfalls
European Commission: White Paper on Artificial Intelligence – a European Approach	▪ Make the EU a global leader in innovation in the data economy and its applications ▪ More innovation in manufacturing, healthcare, transport, energy, environmental services, public services ▪ Human-centric approach to AI ▪ Ecosystem of trust that generally welcomes AI	▪ Encourage take up of AI solutions by European authorities and private sector ▪ Prioritise the need to develop and attract AI ▪ With the exception of security-related business models, AI policies should not demand ex-ante conformity assessments, but instead require companies to do assessment during development ▪ Ex-post evaluations/ audits would allow European companies to continue to invest and grow in EU Member States, without having to relocate to non-European jurisdictions for R&D activities and market launch ▪ Ex-post assessments would increase Europe's attractiveness to foreign technology companies, which would be more inclined to invest and expand in Europe. ▪ Cooperation should be sought with like-minded third countries	Potential policy inconsistencies: ▪ Licensing and ex-ante restrictions stand in opposition to the EU's trade policy agenda, which aims to facilitate market access by lowering barriers imposed by licencing regulations ▪ Licensing and ex-ante restrictions stand in opposition with the EU's SME agenda, which aims to encourage SMEs to access and adopt new innovation; SMEs lack the financial resources available to large companies and are thus ill-equipped to familiarise with and overcome licensing requirements Effectiveness (meeting the goals): ▪ Licensing and ex-ante conformity assessments would contradict the objective to become "a global leader in innovation in the data economy"; licensing requirements would contradict enabling regulatory frameworks, e.g. IPR protection and tax exemptions for R&D-intensive companies ▪ Licensing and ex-ante conformity assessments would decrease Europe's attractiveness to both European and foreign technology innovators/companies; R&D-intensive companies would divest or abstain from investing in Europe ▪ Divestment would adversely impact on future skills and qualifications with respect to the development and handling of ICT, data, AI and other technologies; divestment would result in less private-public partnerships in basic research and applied R&D Efficiency (minimum costs): ▪ Ex-ante conformity assessments are expensive and delay access to products and services ▪ A process of ex-ante testing of AI applications risks becoming a time-consuming affair that will slow down the market entry of technologies; it would in turn undermine the productivity and international competitiveness of downstream sectors in Europe Dynamic impacts (perspectives for future economic development): ▪ Conformity assessments slow down market access; AI conformity testing procedures could open the door for discriminatory treatment, i.e. the denial of market access for applications from foreign companies; this would undermine European companies' capacity to quickly adopt the best technologies available, with adverse implications for international competitiveness

EU policy communication	Stated objectives (visions and goals)	Potential opportunities	Major pitfalls
European Commission: A European Strategy for Data	▪ EU to become a leading role model for a society empowered by data, incl. businesses and organisations ▪ Maximisation of the benefits of the data-driven economy based on Europe's values ▪ To grow data volumes and facilitate technological change	▪ The EU's data strategy could reiterate Europe's commitment to the free flow of data and commitments not to impose data localisations policies, which prevent Europeans from accessing cutting-edge and low-cost data services ▪ The data strategy should recognise the positive economic impacts of trade secrets and intellectual property rights (IPRs), but at the same time increase public access to unutilised public data ▪ Policy-makers should codify their commitment to open markets and non-discriminatory data policies ▪ European cloud-computing markets should remain open to competitive foreign companies. Foreign market access should not be restricted to (only large and politically well-connected) European companies	Potential policy inconsistencies: ▪ The European data strategy paints a Europe-centric, potentially isolationist picture, which stands in opposition to the EU's stated trade policy objectives ▪ The focus on "European Cloud" and/or "European Data Space", potentially data localisation policies, stand in opposition with the EU's SME policies and the recently published industrial policy strategy; localisation policies would deprive European businesses, including SMEs, from low-cost and easy-to-access ICT services, e.g. data storage and processing services and payment services Effectiveness (meeting the goals): ▪ Government-led cloud initiatives and/or data localisation requirements and data-sharing obligations, which undermine intellectual property rights and trade secrets, would have a strong deterrent effect on investment and innovation and are thus inappropriate to render the EU "a society empowered by data" and digital opportunities Efficiency (minimum costs): ▪ Forced data localisation distorts markets and deteriorates the allocation of productive resources ▪ Liability rules would have a deterrent effect on innovation and the development of digital business models; they would prevent structural change and effectively sustain the use of outdated and relatively unproductive business models and technologies. ▪ Data-sharing obligations, which undermine IPRs and trade secrets, would have a deterrent effect on investment and thus contribute to the sustained use of outdated and less productive business models and technologies Dynamic impacts (perspectives for future economic development): ▪ Government-led cloud schemes, forced data localisation and data-sharing polices would crowd-out private sector investments and deprive European businesses of low-cost and easy-to-access data storage and processing services; European companies would in turn face higher costs, reducing the capacity to invest in innovation and business growth ▪ Government-supported cloud schemes, forced data localisation and data-sharing polices would have a deterrent effect on foreign investment across industries, which slow down innovation and structural economic change in Europe

Source: ECIPE.

REFERENCES

Access Partnership (2020). How Will COVID-19 Impact EU Tech Policy? Webinar. 13 May 2020. Available at http://info.accesspartnership.com/en/how-will-covid-19-impact-eu-tech-policy?utm_campaign=EU%20Digital%20Policy%202020&utm_source=hs_email&utm_medium=email&utm_content=87945901&_hsenc=p2ANqtz-9SQKv0oKRukiGfPCCjUssOl8jhuw8MaqJUYjutU3vyUOiu3IUPBhuRe7zklmaAEQK5YFmBubjn5aF3nVx4kEvqp2n26w&_hsmi=87945901.

Bauer, M (2019). Submission to USTR Section 301 Investigation of France's Digital Services Tax. Available at https://ecipe.org/wp-content/uploads/2019/08/2019_08_07_ECIPE-Submission-to-USTR.pdf

Bauer, M. and Lamprecht, P. (2019). Investment Openness in Europe: Investment Screening and Implications for EU-China Investment Relations. November 2019. Available at https://ecipe.org/publications/investment-openness-in-europe/

Bauer, M. (2018). Online Platforms, Economic Integration and Europe's Rent-Seeking Society: Why Online Platforms Deliver on What EU Governments Fail to Achieve. ECIPE Policy Brief 9/2018. Available at https://www.econstor.eu/handle/10419/202508

Bauer, M. (2017). Right Direction, Wrong Territory. Why the EU's Digital Single Market Raises Wrong Expectations. March 2017. Available at https://www.aei.org/research-products/report/right-direction-wrong-territory-why-the-eus-digital-single-market-raises-wrong-expectations/

Barker, T. (2020). Europe Can't Win the Tech War It Just Started. Article in Foreign Policy. 16 January 2020. Available at https://foreignpolicy.com/2020/01/16/europe-technology-sovereignty-von-der-leyen/, accessed on 3 February 2020.

Berger, A. (2010). The United Nations, National Sovereignty and the "Responsibility to Protect". 22 March 2010. Available at https://www.die-gdi.de/en/the-current-column/article/the-united-nations-national-sovereignty-and-the-responsibility-to-protect/

Benhamou, B. (2018). Digital Sovereignty and European Data Regulation – Prospects of the GDPR in the Aftermath of the Cambridge Analytica Crisis. Institute of Digital Sovereignty. 19 May 2018. Available at http://www.netgouvernance.org/DigitalSovereigntyandEuropeanDataRegulation.pdf, accessed on 4 February 2020.

Besson, S. (2011). Sovereignty. Oxford Public International Law. Available at https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1472

Bellanger, P. (2011). De la souveraineté en général et de la souveraineté numérique en particulier. LesEchos.fr, 30 August 2011. Available at http://archives.lesechos.fr/archives/cercle/2011/08/30/cercle_37239.htm

Bitkom (2019). A sovereign cloud and data infrastructure for Germany and Europe. 15 November 2019. Available at https://www.bitkom.org/sites/default/files/2019-11/20191115_keypoints-for-a-sovereign-cloud-infrastructure-in-germany-and-._.pdf

Bitkom (2018). Towards European Leadership on Innovation – Recommendations for the next Digital Single Market. Available at https://www.bitkom.org/sites/default/files/2019-01/Towards%20European%20Leadership%20in%20Innovation.pdf, accessed on 4 February 2020.

Bonenfant, M. (2018). Trust – the foundation of Europe's digital sovereignty. Article on Stormshiled. 17 December 2018. Available at https://www.stormshield.com/news/trust-the-foundation-of-europes-digital-sovereignty, accessed on 4 February 2020.

BSI (2020). Das IT-Sicherheitsgesetz. Available at https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/it_sig_node.html

CashEssentials (2019). Will PEPSI displace Visa and MasterCard? 15 November 2019. Available at https://cashessentials.org/news/will-pepsi-displace-visa-and-mastercard/

CDU (2019). Peter Altmaier: Technologische Souveränität der EU erhalten. 18 March 2019. Available at https://www.cdu.de/artikel/peter-altmaier-technologische-souveraenitaet-der-eu-erhalten

Christensen, C. M. and Bower, J. L. (1996). Customer Power, Strategic Investment, and the Failure of Leading Firms. Strategic Management Journal, Vol. 17, No. 3 (March 1996), pp. 197-218. Available at https://www.jstor.org/stable/2486845?seq=1

Couture, S. and Toupin, S. (2018). What Does the Concept of 'Sovereignty' Mean in Digital, Network and Technological Sovereignty? GigaNet: Global Internet Governance Academic Network, Annual Symposium 2017. 30 January 2018. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3107272, accessed on 4 February 2020.

DCMS (2018). Secure by Design: Improving the cyber security of consumer Internet of Things Report. 7 March 2018. Available at https://www.gov.uk/government/collections/secure-by-design

Drent, M. (2018). European strategic autonomy: Going it alone? Clingendael – Netherlands Institute of International Relations. August 2018. Available at https://www.clingendael.org/sites/default/files/2018-08/PB_European_Strategic_Autonomy.pdf

DigitalGipfel (2018). Plattform Innovative Digitalisierung der Wirtschaft: Fokusgruppe „Digitale Souveränität in einer vernetzten Gesellschaft", Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen. Available at https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2018/p2-digitale-souveraenitaet-und-kuenstliche-intelligenz.pdf?__blob=publicationFile&v=5

ECB (2019). Towards the retail payments of tomorrow: a European strategy. Speech by Benoît Cœuré, Member of the Executive Board of the ECB, at the Joint Conference of the ECB and the National Bank of Belgium on "Crossing the chasm to the retail payments of tomorrow". 26 November 2019. Available at https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp191126~5230672c11.en.html

ECG (2020). 12 leading marketplaces in Europe. Article published by Ecommerce Germany. Available at https://ecommercegermany.com/blog/12-leading-marketplaces-europe

EDPB (2019). EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection. 12 July 2019. Available at: https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en The annex is available at https://edpb.europa.eu/sites/edpb/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf

El Referente (2019). Goggo Network levanta 44 millones con el apoyo de SoftBank y Axel Springer Digital Ventures. 16 December 2019. Available at https://www.elreferente.es/tecnologicos/goggo-network-levanta-44-millones-con-el-apoyo-de-softbank-34622

Enisa (2016). Big Data Threat Landscape and Good Practice Guide. January 2016. Available at https://www.enisa.europa.eu/publications/bigdata-threat-landscape

Erixon, F. and Lamprecht, P. (2018). The Next Steps for the Digital Single Market: From Where do We Start? Policy Brief No 2/2018. Available at https://ecipe.org/wp-content/uploads/2018/10/ECI_18_5F_TheNextStepsfortheDigital_2-2018_03.pdf

Euractiv (2020). Leak of draft Communication on Europe fit for the digital age: Towards a truly European digital society. February 2020. Available at https://www.euractiv.com/wp-content/uploads/sites/2/2020/02/Europe-fit-for-the-digital-age-LEAK.pdf

Eurobarometer (2019). Spring 2019 Standard Eurobarometer. Available at https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4969

European Commission (2020a). Communication from the Commission: A New Industrial Strategy for Europe. 10 March 2020. Available at https://ec.europa.eu/info/sites/info/files/communication-eu-industrial-strategy-march-2020_en.pdf

European Commission (2020b). Communication from the Commission: Shaping Europe's digital future. 19 February 2020. Available at https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

European Commission (2020c). Communication from the Commission: A European strategy for data. 19 February 2020. Available at https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

European Commission (2020d). Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence. Press Release. 19 February 2020. Available at https://ec.europa.eu/digital-single-market/en/news/shaping-europes-digital-future-commission-presents-strategies-data-and-artificial-intelligence

European Commission (2020e). White Paper on Artificial Intelligence – A European approach to excellence and trust. 19 February 2020. Available at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

European Commission (2020f). Communication from the Commission: Identifying and addressing barriers to the Single Market. 10 March 2020. Available at https://ec.europa.eu/info/sites/info/files/communication-eu-single-market-barriers-march-2020_en.pdf

European Commission (2020g). Communication from the Commission: Long term action plan for better implementation and enforcement of single market rules. 10 March 2020. Available at https://ec.europa.eu/info/sites/info/files/communication-enforcement-implementation-single-market-rules_en_0.pdf

European Commission (2019a). Criminal justice: Joint statement on the launch of EU-U.S. negotiations to facilitate access to electronic evidence. 26 September 2019. Available at: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_19_5890

European Commission (2019b). Security Union: Commission receives mandate to start negotiating international rules for obtaining electronic evidence. 6 June 2019. Available at https://ec.europa.eu/commission/presscorner/detail/en/ip_19_2891

European Commission (2019c). EU R&D Investment Scoreboard. The 2019 EU Industrial R&D Investment Scoreboard. Available at: https://op.europa.eu/en/publication-detail/-/publication/bcbeb233-216c-11ea-95ab-01aa75ed71a1/language-en

European Commission (2019d). The 2019 EU survey on industrial R&D investment trends. Available at https://op.europa.eu/en/publication-detail/-/publication/05d409ba-216f-11ea-95ab-01aa75ed71a1/language-en

European Commission (2019e). Mergers: Commission prohibits Siemens' proposed acquisition of Alstom. Press Release. February 2019. Available at https://ec.europa.eu/commission/presscorner/detail/en/IP_19_881

European Commission (2019f). Instant payments. 28 June 2019. Available at https://ec.europa.eu/newsroom/fisma/item-detail.cfm?item_id=654172&utm_source=fisma_newsroom&utm_medium=Website&utm_campaign=fisma&utm_content=Instant%20payments%20&lang=en

European Commission (2018). State of the Union 2018: The Hour of European Sovereignty. 12 September 2018. Available at https://ec.europa.eu/commission/news/state-union-2018-hour-european-sovereignty-2018-sep-12_en

European Commission (2018a). Commission Decision of 30 January 2018 setting up the Strategic Forum for Important Projects of Common European Interest, 2018/C 39/03. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOC_2018_039_R_0003

European Commission (2018b). Minutes Strategic Forum for Important Projects of Common European Interest, 30 May 2018, Brussels. Available at https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vkln6uke5czr

European Commission (2015). Communication from the Commission: A Digital Single Market Strategy for Europe. 6 May 2015. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192

European Commission (2008). State aid: Commission authorises aid of €99 million to France for QUAERO R&D programme. 11 March 2008. Available at https://ec.europa.eu/commission/presscorner/detail/en/IP_08_418

European Commission DG Trade (2015). Trade for all – Towards a more responsible trade and investment policy. October 2015. Commitment to tackle digital protectionism.

European Parliament (2019a). Fact Sheets on the European Union: The principle of subsidiarity. Available at https://www.europarl.europa.eu/factsheets/en/sheet/7/the-principle-of-subsidiarity

European Parliament (2019b). EU industrial policy at the crossroads – Current state of affairs, challenges and way forward. December 2019.

European Parliament (2019c). How to tackle challenges in a future-oriented EU Industrial Strategy? Volume I. June 2019.

European Parliament (2019d). How to tackle challenges in a future-oriented EU Industrial Strategy? Volume II. June 2019.

European Parliament (2018). European Parliament resolution of 30 May 2018 on the future of food and farming (2018/2037(INI)). Available at https://www.europarl.europa.eu/doceo/document/TA-8-2018-0224_EN.html

Friends of Industry (2018). Joint statement by France, Austria, Croatia, Czech Republic, Estonia, Finland, Germany, Greece, Hungary, Italy, Latvia, Luxembourg, Malta, Netherlands, Poland, Romania, Slovakia, Spain. 6th Ministerial Meeting, 18 December 2018. Available at https://www.gouvernement.fr/sites/default/files/locale/piece-jointe/2018/12/929_-_declaration_finale_-_6eme_reunion_des_amis_de_lindustrie-en.pdf

FMIBC (2019). BMI intensiviert Aktivitäten zur Stärkung der digitalen Souveränität in der öffentlichen Verwaltung. German Federal Ministry of the Interior, Building and Community. Press release of 19 September 2019. Available at https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2019/09/digitale-souveraenitaet-oeff-verwltg.html, accessed on 4 February 2020.

FICO (2018). New Analytics for Real-Time Payments Fraud. With a view to stopping real-time payments fraud, FICO recently released the Retail Banking Consumer fraud model. 2 November 2018. Available at https://www.fico.com/blogs/new-analytics-real-time-payments-fraud

Financial Times Editorial Board (2019). Digital sovereignty does not need EU champions. Opinion on The FT Views. The Editorial Board of the Financial Times. 14 November 2019. Available at https://www.ft.com/content/2762d7dc-0607-11ea-a984-fbbacad9e7dd, accessed on 3 February 2020.

Fiott, D. (2018). Strategic autonomy: towards 'European sovereignty' in defence? European Union Institute for Security Studies (EUISS). November 2018. Available at https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2012__Strategic%20Autonomy.pdf

Fraunhofer (2019). Challenges and Potentials of A Logistics Data Space. 2019. Joint publication of Fraunhofer and International Data Spaces Association. Available at https://www.internationaldataspaces.org/wp-content/uploads/2019/10/IDSA-LC-position_paper.pdf, accessed on 4 February 2020.

Fraunhofer (2016). White Paper on Industrial Data Space – Digital Sovereignty Over Data. Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Munich. Available at https://www.fraunhofer.de/content/dam/zv/en/fields-of-research/industrial-data-space/whitepaper-industrial-data-space-eng.pdf, accessed on 4 February 2020.

French Banking Federation (2010). About twenty European banks plan to create a new card scheme for Europe. 6 May 2010. Available at http://www.fbf.fr/en/means-of-payment/monnet/about-twenty-european-banks-plan-to-create-a-new-card-scheme-for-europe.

FT (2019). Germany calls on EU to tighten grip on Big Tech. 11 November 2019. Available at https://www.ft.com/content/2d538f22-048d-11ea-a984-fbbacad9e7dd

Fulton, S. (2020). Continental Drift: Is Digital Sovereignty Splitting Global Data Centers? Article published on Data Center Knowledge on 2 January 2020. Available at https://www.datacenterknowledge.com/regulation/continental-drift-digital-sovereignty-splitting-global-data-centers, accessed on 4 February 2020.

Galles, G. (2019). Remembering Gustave de Molinari: Individual sovereignty, not government sovereignty. 7 March 2019. Available at https://www.ocregister.com/2019/03/07/remembering-gustave-de-molinari-individual-sovereignty-not-government-sovereignty/

German Advisory Council for Consumer Affairs (2017). Digital Sovereignty Report by the Advisory Council for Consumer Affairs. June 2017. Available at https://www.svr-verbraucherfragen.de/wp-content/uploads/English-Version.pdf, accessed on 4 February 2020.

German Federal Ministry for Economic Affairs and Energy (2019). Project GAIA-X. A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem. October 2019. Available at https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/project-gaia-x.pdf?__blob=publicationFile&v=4

Gueham, F. (2017). Digital Sovereignty – Steps towards a new system of internet governance. Le Fondation pour l'innovation politique, a French think tank for European integration and free economy. Available at https://euagenda.eu/upload/publications/untitled-77045-ea.pdf

Goujard, C. (2018). France is ditching Google to reclaim its online independence. Article published by wired.co.uk on 20 November 2018. Available at https://www.wired.co.uk/article/google-france-silicon-valley, accessed on 4 February 2020.

Hamilton, D. S. (2014). The Geopolitics of TTIP: Repositioning the Transatlantic Relationship for a Changing World. Center for Transatlantic Relations, Paul H. Nitze School of Advanced International Studies Johns Hopkins University. Available at https://archive.transatlanticrelations.org/wp-content/uploads/2016/08/Complete_book.pdf

Henderson, R. and Clark, K. (1990). Architectural Innovation: The Reconfiguration of Existing Product Technologies and the Failure of Established Firms. Administrative Science Quarterly, 35(1), March 1990. Available at https://www.researchgate.net/publication/200465578_Architectural_Innovation_The_Reconfiguration_of_Existing_Product_Technologies_and_the_Failure_of_Established_Firms

Hogan Lovells (2019). Demystifying the U.S. CLOUD Act: Assessing the law's compatibility with international norms and the GDPR. January 2019. Available at https://www.hoganlovells.com/~/media/hogan-lovells/pdf/2019/2019_01_15_whitepaper_demystifying_the_us_cloud_act.pdf

International Data Spaces Association (2018a). Sharing Data While Keeping Data Ownership. White Paper. October 2018. Available at https://www.internationaldataspaces.org/wp-content/uploads/2019/07/Whitepaper-2018.pdf

International Data Spaces Association (2018b). Jointly Paving the Way for a Data Driven Digitisation of European Industry. Position paper. October 2018. Available at https://www.internationaldataspaces.org/wp-content/uploads/2019/07/IDSA-Position-paper-2018.pdf

ITIF (2019). Promoting European Growth, Productivity, and Competitiveness by Taking Advantage of the Next Digital Wave. March 2019. Available at https://itif.org/publications/2019/03/26/promoting-european-growth-productivity-and-competitiveness-taking-advantage

Järvenpää, P., Major, C. and Sakkov, S. (2019). European Strategic Autonomy Operationalising a Buzzword. October 2019. International Centre for Defence and Security. Available at https://www.kas.de/en/web/estland/single-title/-/content/european-strategic-autonomy-operationalising-a-buzzword

JRC-OECD (2019). World Corporate Top R&D Investors: Shaping the Future of Technologies and of AI. Joint publication of the European Commission's Joint Research Centre (JRC), the European Commission's science and knowledge service and the Organisation for Economic Co-operation and Development (OECD). Available at https://ec.europa.eu/jrc/en/science-update/shaping-future-technologies-and-ai

KPMG (2019). Implication of the U.S. Cloud Act on Privacy Aspects. 20 March 2019. Available at https://blog.kpmg.ch/implication-of-the-u-s-cloud-act-on-privacy-aspects/

Krasner, S. D. (2001). Sovereignty. Foreign Policy. January/February 2001. Available at http://www.columbia.edu/itc/sipa/S6800/courseworks/sovereignty_krasner.pdf

Lee-Makiyama, H. Stealing Thunder: Cloud, IoT and 5G will Change the Strategic Paradigm for Protecting European Commercial Interests. Will Cyber Espionage be Allowed to Hold Europe Back in the Global Race for Industrial Competitiveness? February 2018. Available at https://ecipe.org/publications/stealing-thunder/

Leonard, M., Pisani-Ferry, J., Ribakova, E., Shapiro, J. and Wolff, G. (2019). Redefining Europe's economic sovereignty. Joint publication of Bruegel and the European Council on Foreign Relations. June 2019. Available at https://bruegel.org/wp-content/uploads/2019/06/PC-09_2019_final-1.pdf, accessed on 4 February 2020.

Leonard, M. and Shapiro, J. (2019). Strategic Sovereignty: How Europe can Regain the Capacity to Act. European Council on Foreign Relations. June 2019. Available at https://www.ecfr.eu/page/-/ecfr_strategic_sovereignty.pdf

Linklaters (2019). U.S. CLOUD Act and GDPR – Is the cloud still safe?. Article published on 13 September 2019. Available at https://www.linklaters.com/en/insights/blogs/digilinks/2019/september/us-cloud-act-and-gdpr-is-the-cloud-still-safe

Lippert, B., Ondarza, N. v., Perthes, V. (2019). European Strategic Autonomy Actors, Issues, Conflicts of Interests. SWP Research Paper 4. German Institute for International and Security Affairs. Available at https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2019RP04_lpt_orz_prt_web.pdf

McKinsey (2019). Asia's Future is Now. McKinsey Global Institute. July 2019 Discussion Paper. Available at https://www.mckinsey.com/featured-insights/asia-pacific/asias-future-is-now?cid=other-eml-nsl-mip-mck

McKinsey (2012). Evolution of the earth's economic center of gravity. McKinsey Global Institute analysis using data from Angus Maddison; University of Groningen. Available at https://globaltrends2030.files.wordpress.com/2012/07/nic-blog-mgi-shifting-economic-center-of-gravity.pdf

Pohlmann, N., Sparenberg, M., Siromaschenko, I. and Kilden, K. (2014). Secure communication and digital sovereignty in Europe. Securing Electronic Business Processes, Springer Vieweg 2014, pp. 1-15.

Popp. K. (2019). Waving the flag of digital sovereignty. Article on the Atlantic Council. 11 December 2019. Available at https://www.atlanticcouncil.org/blogs/new-atlanticist/waving-the-flag-of-digital-sovereignty/, accessed on 3 February 2020.

PWC (2018). Data exchange as a first step towards data economy. PricewaterhouseCoopers. March 2018. Available at https://www.internationaldataspaces.org/wp-content/uploads/2019/07/Data-exchange-PWC-study.pdf, accessed on 4 February 2020.

PWC (2017). The World in 2050. The long view: how will the global economic order change by 2050? Available at https://www.pwc.com/gx/en/issues/economy/the-world-in-2050.html#downloads

Reding, V. (2016). Digital Sovereignty: Europe at a Crossroads. New European Debates article by Viviane Reding. European Investment Bank Institute. Available at http://institute.eib.org/wp-content/uploads/2016/01/Digital-Sovereignty-Europe-at-a-Crossroads.pdf, accessed on 4 February 2020.

Reuters (2019). France recruits Dassault Systemes, OVH for alternative to U.S. cloud firms. 3 October 2019. Available at https://www.reuters.com/article/us-france-dataprotection/france-recruits-dassault-systemes-ovh-for-alternative-to-u-s-cloud-firms-idUSKBN1WI189

PCM (2019). PEPSI: A European payment system to rival Visa and Mastercard? 12 November 2019. Available at https://www.paymentscardsandmobile.com/pepsi-a-european-payment-system-to-rival-visa-and-mastercard/

Perrit, H. H. Jr. (1998). The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance. Chicago-Kent College of Law, Illinois Institute of Technology. Spring 1998. Available at https://pdfs.semanticscholar.org/06fb/60988985680367095fcb21e9ccc96336efba.pdf, accessed on 4 February 2020.

PEW (2017). Few see EU as world's top economic power despite its relative might. Available at https://www.pewresearch.org/fact-tank/2017/08/09/few-see-eu-as-worlds-top-economic-power-despite-its-relative-might/

Pinto, R. A. (2018). Digital Sovereignty or Digital Colonialism. New tensions of privacy, security and national policies. SUR 27, Vol. 15, p. 15-27. Available at https://sur.conectas.org/wp-content/uploads/2018/07/sur-27-ingles-renata-avila-pinto.pdf, accessed on 4 February 2020.

PMR (2019). Payment Methods Report 2019. June 2019. Available at https://www.europeanpaymentscouncil.eu/sites/default/files/inline-files/Payment%20Methods%20Report%202019%20-%20Innovations%20in%20the%20Way%20We%20Pay.pdf

Politico (2020a). The Achilles' heel of Europe's AI strategy – Europe's strategy is all about companies sharing their data. That's easier said than done. March 2020. Available at https://www.politico.eu/article/europe-ai-strategy-weakness/

Politico (2020b). Vestager touts AI-powered vision for Europe's tech future. 17 February 2020. Available at https://www.politico.eu/article/margrethe-vestager-touts-ai-artificial-intelligence-powered-vision-for-europe-tech-future/

Politico (2020c). Lithuania marshals 'like-minded' defenders of internal market. 27 February 2020. Available at https://www.politico.eu/pro/lithuania-marshals-like-minded-defenders-of-internal-market/?utm_source=POLITICO.EU&utm_campaign=7feef998e0-EMAIL_CAMPAIGN_2020_02_27_07_30&utm_medium=email&utm_term=0_10959edeb5-7feef998e0-190178425

Rinas, S. (2016). Digitale Souveränität – eine Perspektive. Article on Digital Society Blog of Humboldt University's Institut für Internet und Gesellschaft. 5 February 2016. Available at https://www.hiig.de/digital-sovereignty-a-prospect/, accessed on 3 February 2020.

Scott, B., Heumann, S. and Lorenz, P. (2018). Artificial Intelligence and Foreign Policy. Publication by Stiftung Neue Verantwortung. January 2018. Available at https://www.stiftung-nv.de/sites/default/files/ai_foreign_policy.pdf, accessed on 4 February 2020.

Stackfield (2019). 8 secure cloud storage services from Germany. Available at https://www.stackfield.com/blog/8-secure-cloud-storage-services-68

Stiker, T. (2019). European Organizations Committed To Digital Sovereignty. Blog published on Kopano on 10 October 2019. Available at https://kopano.com/blog/european-organizations-committed-to-digital-sovereignty/, accessed on 4 February 2020.

Supreme Court (2017). In the Supreme Court of the United States. Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of Neither Party. Available at https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf

Thieulin, B. (2019). Towards a European digital sovereignty policy. Opinion of the Economic, Social and Environmental Council presented by Benoît Thieulin, rapporteur, On behalf of the Section for European and International Affairs. Official Journal of the French Republic. Available at https://www.lecese.fr/sites/default/files/travaux_multilingue/2019_07_souverainete_europeenne_numerique_GB_reduit.pdf, accessed on 4 February 2019.

Thornhill, J. (2019). The people, not governments, should exercise digital sovereignty. Opinion on EU tech regulations. Financial Times. 25 November 2019.

USDJ (2019a). U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online. 3 October 2019. Available at https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists

USDJ (2019b). Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton. 7 October 2019. Available at https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us

Vestager, M. (2019). Hearing of Margrethe Vestager, Executive Vice President "Europe fit for the Digital Age", Opening statement. 8 October 2019. Available at https://multimedia.europarl.europa.eu/en/hearing-of-margrethe-vestager-executive-vice-president-designate-europe-fit-for-the-digital-age-opening-statement-bymargrethe-vestager_I178158-V_v

von der Leyen, U. (2019). A Union that strives for more. My agenda for Europe – Political Guidelines for the Next European Commission 2019-2024. Available at https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf, accessed on 4 February 2020.

von der Leyen, U. (2019a). Mission Letter to Margrethe Vestager, Executive Vice-President-designate for a Europe fit for the Digital Age, Brussels. 1 December 2019. Available at https://ec.europa.eu/commission/sites/beta-political/files/mission-letter-margrethe-vestager_2019_en.pdf

von der Leyen, U. (2019b). Mission Letter to Thierry Breton, Commissioner for Internal Market, Brussels. 1 December 2019. Available at https://ec.europa.eu/commission/commissioners/sites/comm-cwt2019/files/commissioner_mission_letters/president-elect_von_der_leyens_mission_letter_to_thierry_breton.pdf

von der Leyen, U. (2019c). Mission Letter to Phil Hogan, Commissioner for International Trade, Brussels. 1 December 2019. Available at https://ec.europa.eu/commission/sites/beta-political/files/mission-letter-phil-hogan-2019_en.pdf

von der Leyen (2019d). My agenda for Europe, By candidate for President of the European Commission Ursula von der Leyen, Political Guidelines for the Next European Commission 2019-2024. 8 November 2019. Available at https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

Voss, A. (2020). A manifesto for Europe's digital sovereignty and geo-political competitiveness. Available at https://www.axel-voss-europa.de/wp-content/uploads/2020/01/AVoss-Digital-Manifesto-2020-english-1.pdf, accessed on 3 February 2020.

Weber, A., Reith, S., Kasper, M., Kuhlmann, D., Seifert, J. P. and Krauß, C. (2018). Security. Safety and Fair Market Access by Openness and Control of the Supply Chain. White Paper V1.0. March 2018. Available at https://www.itas.kit.edu/pub/v/2018/weua18a.pdf, accessed on 3 February 2020.

Weinrib, J. (2017). Sovereignty as a Right and as a Duty: Kant's Theory of the State. 1 June 2017. In Claire Finkelstein and Michael Skerker (eds) Sovereignty and the New Executive Authority (Oxford: University Press, Forthcoming). Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2976485

Williams, B. (1998). The Sovereign State in the 21st Century: Some Implications of Economic Globalization and New Technologies for Political Organization. Senior Thesis Projects, 1993-2002. Available at https://trace.tennessee.edu/cgi/viewcontent.cgi?article=1033&context=utk_interstp2, accessed on 3 February 2020.

WTO (2019). World Trade Report 2019. The Future of Trade in Services. Available at https://www.wto.org/english/res_e/booksp_e/00_wtr19_e.pdf

ZDNet (2020). New Bill to prepare Australian law enforcement for the US CLOUD Act. 5 March 2020. Available at https://www.zdnet.com/article/new-bill-to-prepare-australian-law-enforcement-for-the-us-cloud-act/

References to legal text:

US Cloud Act: https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf

EU GDPR: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX-:32016R0679&from=EN

EU-US Privacy Shield: https://www.privacyshield.gov/servlet/servlet.FileDownload?-file=015t00000004qAg