AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Towards a digitalised Single Market (2019 -2024)

Recommendations for the next digital policy agenda of the European Commission

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €2 trillion in 2017, directly supports more than 4.7 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Table of contents

Executive summary

Europe can reap tremendous benefits from a digitalised economy and society. Digital technologies improve connectivity in rural areas, support environmental sustainability and peoples' health, safety, mobility and overall quality of life. They stimulate economic growth and jobs by increasing industrial productivity and efficiency, creating new business opportunities and expanding consumer choice.

Ahead of the next European Commission and European Parliament's mandate (2019-2024), the American Chamber of Commerce to the European Union (AmCham EU) has identified the following key priority areas to build a competitive European digital economy:

- **Better regulation**: Policy and regulatory frameworks in the EU should aim to foster investment in digital technologies, innovation and entrepreneurship, while adequately protecting citizens and users from possible risks. In particular:
  - ✓ Before introducing new rules, policy-makers should carefully assess whether existing legislation is fit for purpose. Multi-stakeholder dialogues are essential to design the right policy solutions to identified challenges.
  - ✓ New legislation should be principle- and risk-based and should take into account the diversity of applications and users for digital technologies, instead of applying one-size-fits-all rules.
  - ✓ The European Commission's political and institutional structure should reflect the fact that all sectors of the economy are undergoing various degrees of digital transformation and should streamline digital across policy fields.
- **Emerging technologies**: Europe should boost the development and make the most of new emerging technologies such as Artificial Intelligence (AI), Blockchain, Internet of Things (IoT) and 5G and enable their integration in sectors like mobility and health. In particular:
  - ✓ The free flow of data and availability of open and public data is essential for digital technologies to emerge and scale-up. In addition, the principle of contractual freedom needs to be protected when it comes to access of non-personal data. Open solutions should be promoted through a market-driven approach to prevent lock-in effects in the data economy.
  - ✓ The EU and Member States, in a coordinated effort, should boost strategic investments in AI, while ensuring its uptake across different economic sectors. The development of guidelines on ethics in AI will encourage companies to self-regulate.
  - ✓ The broader adoption of Blockchain will require a clear and stable legal framework and will considerably benefit from the implementation of use cases and pilot projects in the public sector, as well as the participation of governmental agencies in private projects.
- **Investment, innovation and entrepreneurship:** The successful digitalisation of the economy and society will depend on enabling factors such as incentives for research and development (R&D) and the ability of businesses to scale-up and to protect their investments. In particular:
  - ✓ It is crucial to incentivise investments in research, development and the application of emerging technologies. Third-country participation and international cooperation in R&D will contribute to reaching Europe's technological ambitions and should remain valued.

- ✓ International standards and practices should be prioritised wherever possible. The role of the EU Multi-Stakeholder Platform (MSP) should be strengthened in international fora and consortia to develop specifications for information and communications technology (ICT).

- ✓ Lifelong learning programs for employees should be developed. Academic institutions should adapt their curriculum to equip students with digital skills and meet the specific needs of a digital technology-powered economy.

- **Trust:** For all businesses, governments and people to reap the full benefits of digital technologies, they need to be trusted by their users. The complexity of value chains and diversity of business models and application sectors, as well as the fast-developing digital environment, requires strong public-private partnerships to tackle complex challenges such as ethics in AI and cybersecurity in IoT. In particular:

  - ✓ Data protection and privacy is a long journey which requires continuous and open dialogue between relevant stakeholders and data protection authorities. Any future rules on confidentiality of communication data (e-privacy) should be fully aligned with the General Data Protection Regulation (GDPR).

  - ✓ The requirements for IoT cybersecurity call for proportionate and risk-based solutions which take into account specificities of different markets and applications. Any future EU security certification should align on existing international security standards and practices.

  - ✓ A new European framework and EU-US agreement on access to electronic evidence (e-evidence) is essential to provide clear procedures and safeguards in cross-border cases.

- **International cooperation**: Governments need to cooperate to ensure free flow of data, the scale-up of start-ups and technologies and to effectively address challenges such as cybersecurity.

  - ✓ The EU-US Privacy Shield agreement will continue to be a fundamental mechanism to ensure and safeguard the transfer of personal data, and as such the provision of digitally-enabled services across the Atlantic.

  - ✓ EU trade agreements need to include provisions to prevent unjustified data localisation requirements and other market access restrictions such as forced technology transfers.

  - ✓ Negotiations on e-commerce rules need to be launched in the framework of the World Trade Organization (WTO) to make global trade more inclusive and to promote a free and open internet.

Introduction

Digital technologies are profoundly transforming the economy and society, bringing tremendous benefits to businesses, citizens and governments.

For **business**, the intense competition on cutting-edge innovation in the digital economy has offered opportunities to boost productivity and reduce transaction costs thanks to access to innovative digital products and services that help optimise processes, supply chains, production and distribution. All of this enables companies to participate in global value chains and directly access customers in markets in ways previously only feasible for larger and more established companies.

For **citizens and consumers**, the benefits are associated with access to a wider and better range of goods and services at competitive prices. Digital services offer new opportunities for entrepreneurship, job creation, education and interaction with family and friends located across the world. Digital technologies can also help people live a more sustainable and healthier life through expanded access to medical services which improve patient outcomes, reduce doctor and hospital visits and improve accessibility for people with disabilities.

Governments benefit from the digital economy because they have access to technologies that help them deliver more efficient and better public services, become more closely connected to citizens, improve governance, evaluate policies and deliver better results overall.

We must simultaneously recognise that, in addition to the benefits, the integration of technologies into our lives and business operations has also raised concerns over its impacts on society and the economy, such as the protection of people's privacy, the spread of illicit content, unfair competition and job losses. These are critical issues that need to be addressed proactively by companies and relevant stakeholders to create a trusted and safer environment.

To tap the full potential of digital technologies and keep investment flowing, governments should enact policies and regulations that promote trust and competitiveness. Long-term commitment to a forward-looking policy framework – characterised by effective regulatory models and supported by multi-stakeholder engagement between regulators, elected officials and private businesses – will help ensure the continued growth of the European digital economy.

This paper outlines AmCham EU's vision for the EU's next digital agenda (2019-2024), and is divided into five main sections:

Section 1 highlights the importance of Better Regulation, how adopting a new way of doing policy can create the right regulatory environment to encourage innovation and entrepreneurship in the digital space.

Section 2 focuses on emerging technologies which Europe can better embrace, such as AI, Blockchain, IoT and 5G.

Section 3 outlines key pillars to create an enabling environment for innovation and entrepreneurship to flourish: incentives to boost investment, interoperable solutions for new technologies to scale-up and opportunities for people to gain new skills.

Section 4 tackles the challenge of building trust in the digital economy. Consumer and citizen needs should be at the centre of the digital transformation, making them feel safe and protected online is key to boosting the usage of digital services. Each society has the power and the responsibility to decide how to shape its digital transformation and this should be through an inclusive and informed debate.

Section 5 emphasises the importance of global cooperation for a competitive European digital economy. European and international data flows are essential to cross-border trade and trade agreements need to effectively tackle market access barriers.

1. Key principles for Better Regulation in the digital economy

The complexity, speed of development and horizontal nature of digital technologies require a new way of policy-making which should be based on a strong public-private partnership. Multi-stakeholder dialogues are essential to design the right regulatory and policy solutions. Furthermore, in order to avoid EU legislation acting as a barrier to future technological developments, any new regulatory or policy framework needs to take into account existing legislation and the diversity of application areas and type of users of digital technologies.

Time for implementation

Before initiating new legislative proposals, policy-makers should give time to existing initiatives and legislation to be implemented and to show concrete results. For example, the e-Privacy proposal (published in January 2017) does not fully align with the GDPR which entered into force in May 2018, and thus has brought considerable uncertainty in terms of data protection compliance. Furthermore, recently launched initiatives in the data economy space deserve greater attention before taking any further action, such as: the Support Centre for data sharing, the Expert group on business-to-government (B2G) data sharing principles and the European Commission guidelines on business-to-business (B2B) data sharing.

Priority to quality over time

Before introducing any new rules, existing policy frameworks should be carefully assessed to see if they are fit for purpose, giving priority to quality over time. Throughout the regulatory process, impact assessments are essential to ensure that regulatory environments encourage innovation and entrepreneurship while protecting consumers. Rushing through decision-making procedures could risk creating unclear and non-future proof rules that would need to be re-evaluated after a relatively short period of time, generating legal uncertainty for companies.

No one-size-fits-all

Legislation needs to be technology-neutral and distinguish different applications area for digital technologies. Today's emerging technologies are global, interconnected and reliant on a broad variety of information sources, both directly collected and indirectly observed, as well as on highly variable data such as real-time sensor inputs. Data can be personal and/or not linked to natural persons (for example, where industrial IoT solutions are concerned). Finally, technologies are applied in a wide range of sectors (with different risk scenarios) and across diverse business models.

Whenever policy-makers draft new rules, they should bear in mind the difference in users of services, be it consumers or enterprise mass markets. Enterprise and professional customers have bilateral and extensively negotiated contracts, including specific rules and provisions that are negotiated between two commercial partners. In most cases, rules designed for consumers would not be relevant or applicable to an enterprise and professional customers and could even have the unintentional result of obstructing the principle of contractual freedom.

Principle-based solutions

Technologies advance at such a fast pace that solutions need to be principle-based, market-led and risk-based in order to keep a framework relevant. Frameworks should set the overall objectives to be reached rather than prescribing how to do it. For example, a policy that has the goal of protecting networks and information would be more effective if it is based on 'what' must be protected rather than 'how' it must be protected, taking into account the risk profile of a given product or service. Having very prescriptive rules could create unintended consequences and could considerably increase the burden of implementation.

A multi-stakeholder approach

A good step towards Better Regulation would be to stimulate more systematically proactive multi-stakeholder engagement to design policy solutions to an identified challenge. Public consultations should be combined with targeted workshops, roundtables and expert groups. One interesting example is the on-going European Commission High-Level Expert Group (HLEG) on AI, which has gathered stakeholders from all impacted sectors to draft guidelines on ethics.

Strong leadership

The Commission's political and institutional structure should reflect the fact that all sectors of the economy are undergoing various degrees of digital transformation. Although it is not in our remit to comment on the future institutional structure, we do believe that:

- Digitalisation should be embodied in each policy field and needs to be reflected in the institutional structure.
- Overall coordination of initiatives relevant to the digital economy through a European Commission Vice-President is essential to ensure consistent initiatives and provisions.
- A Better Regulation process should continue to be at the heart of the procedures of the next Commission and co-legislators.

2. Fostering emerging technologies

Advancement in science and research leads to the emergence of new technologies with tremendous economic and social potential. The most promising technologies currently include AI, Blockchain, IoT and 5G. These can bring huge benefits but also challenges, as they profoundly transform the way of using certain products and services, such as connected mobility and eHealth. Scientists, developers, industry and policy-makers must maximise the benefits from new technologies whilst minimising possible risks.

Data economy

For the last several years, machines – from tractors to production lines to airplane engines – have generated an increasingly significant volume of data. This data, in turn, has enabled better services and more follow-on innovation by the producer, which feeds into the supply chain and creates opportunities for new suppliers and brings value to the end-customers. However, this new business model has also raised concerns of who will have 'access' to such (non-personal) data. While today the data economy is functioning well, with a high degree of innovation and competition, these questions are legitimate. Going forward, the following factors are crucial to boost the data economy:

- The principle of **contractual freedom** is essential when it comes to access of non-personal data. The Commission has rightly recognised that there will be cases in which industry players will need to prevent disclosure of data to lawfully protect themselves against competitors. Unique solutions require time and investment and these investments are undermined if competitors can easily glean strategies or technology from data disclosed to third parties, without commensurate effort on the competitors' part (leading to so-called 'free-riding'). Several initiatives presented in 2018 aim at stimulating the data economy through a market-driven approach, such as the Support Centre for data sharing, B2G expert group recommendations, and B2B data sharing guidelines. Further guidance from the Commission to some specific sectors would be useful.

- **Availability of public and open data** is a key success factor for the uptake of emerging technologies, like AI. A good step was made with the agreement reached between the EU co-legislators on the revision of the Public-Sector Information Directive. Public authorities should be incentivised to open up new types of public data, such as data from public undertakings.

- The implementation of the EU **Free Flow of Data** Regulation will remove and prevent unjustified data localisation requirements. This will make it easier for start-ups to scale-up and for companies across sectors to benefit from new technologies that enable them to store and analyse data more efficiently and cost-effectively.

- The Commission should continue to promote **open solutions** to prevent lock-in in the data economy through a market-driven approach. There is a role for the development of self-regulatory codes of conduct for businesses to facilitate data porting and switching between cloud service providers based on established open governance models. The Commission should also promote the development of procurement guidelines for open source technologies, thus driving uptake not only through regulations, but also through market incentives.

Artificial intelligence

There is no doubt that AI will transform every aspect of our society and economy. Already, AI is commonly used in many of our daily actions with features that make our lives safer, more convenient and more productive. Breakthroughs in areas such as vision, speech, translation and knowledge in recent years have proven AI is a technology that is transformative and has unprecedented potential. Key factors to boost AI in Europe include:

- **Uptake**: Stimulate the uptake of AI within priority industry sectors that can greatly benefit from digital transformation, such as automotive, healthcare, telecommunications, manufacturing and retail. This should include supporting R&D as well as facilitating access to computing power, skills, advice and mentoring.

- **R&D**: Policy-makers should boost private and public investment in R&D, such as through EU funds (Horizon 2020, Future and Emerging Technologies, future Horizon Europe and Digital Europe), public-private partnerships and cross-border testing. The ambition should be to create an innovation-friendly environment with incentives for investment in research, development and the application of AI, including greater collaboration and co-development.

- **Data**: Availability and free flow of data are essential to AI. Therefore policy-makers should: make non-sensitive public-sector data available for research to boost data available for training AI systems; support the creation of AI ecosystems and public-private partnerships; unleash the potential of the data economy in Europe by making sure data can move freely across borders with Europe and internationally; facilitate text and data mining; and avoid creating prescriptive rules for data ownership or data access.

- **Ethics:** The development of voluntary ethical guidelines in consultation with a broad group of stakeholders will help to develop a common understanding on key issues and encourage companies to self-regulate. These guidelines should be both holistic and proportional, so that they are pertinent to a wide range of businesses that are using AI in different ways.

- **No one-size-fits-all**: AI is a fast-evolving domain with different applications depending on markets and business models. Diverse uses of AI pose different risks and require tailored responses. Policy-makers should assess existing regulatory frameworks to see if they are fit to address AI and adapt the current legal frameworks rather than create new AI laws. It is also essential to make sure that future legislation addressing issues other than AI do not undermine AI's development.

Blockchain

Blockchain is an emerging technology which has the potential to transform the way we interact and exchange information in a faster, more secure and more transparent way. At policy level, a good understanding of what blockchain is and does is essential for the development and broader adoption of distributed ledger technology (DLT), together with a clear and stable legal framework for its application in Europe. In particular, the key factors to boost Blockchain in Europe could include:

- **Legal certainty** in areas such as the legal status of smart contracts, GDPR compliance and classification of digital assets and tokens. This does not necessarily require new legislation, but rather guidelines and clarifications to ensure that the existing framework is fit for the blockchain era.

- **Experimentation**: the implementation of use cases and pilot projects in the public sector and the participation of governmental agencies in private projects would be the best way to test the technology in a large number of areas and promote its use.

- **No-one-size-fits-all**: the potential uses for DLT are numerous and diverse. Therefore, any regulatory framework needs to be sufficiently cognisant of the variety of potential applications of DLT which are adaptable to operating across multiple activities and services.

Internet of Things

The multplication of connected devices – 20.4 billion by 2020 according to Gartner[1] – raises legitimate needs from users for privacy, security, resilience, transparency and interoperability. At the same time, the IoT is still an emerging technological area in the earliest days of its development and growth. The EU must enable an environment that allows for safe innovation without unintentionally limiting or hindering market access or undermining the competitiveness of the EU market in comparison to the rest of the world.

- **Apply existing legislation**: Full use should be made of already existing instruments to address any concrete and proven issues or market failures that may arise in the IoT space. For instance, generic or blanket cybersecurity labelling of IoT products could result in counter-productive technology mandates. Such 'IoT security labels' would result in new market access barriers or roadblocks to innovation without bringing any real cybersecurity or privacy benefits which could otherwise be achieved on the basis of already existing instruments.

- **Risk-based approach**: Any policy framework for the IoT should be risk-based and incoporate industry standards and best practices.

- **Contractual freedom**: We understand the Commission's decision to further study whether new rules are needed to handle issues relating to liability in connection with the 'data economy' (particularly in the context of enterprise IoT). It is important that no 'gaps' in liability exist for consumers and identifying fault in the connected device economy may at times be difficult given the number of different hardware and software suppliers involved in individual products. However, contract terms are the best way to handle liability issues, as they provide predictability and certainty for businesses engaged in the supply chain.

5G

For emerging technologies to succeed, the rollout of 5G will be essential. As rightly acknowledged by the European Commission, the fifth generation of telecommunication systems, or 5G, will be one of the most critical building blocks of our digital economy and society in the next decade.[2] The connectivity benefits of 5G will give consumers access to more information faster than ever before and will make businesses more efficient. Autonomous cars, smart communities, industrial IoT, immersive education and eHealth will all rely on 5G. The successful rollout of ultra-fast 5G services in Europe will require several factors, including but not limited to:

- Swift adoption and implementation of **EU Member States' 5G roadmaps**.

- Quick and consistent implementation of the **Electronic Communications Code** by EU Member States.

- Greater **consistency of 5G spectrum** and regular consultation and coordination among all relevant stakeholders.

[1] https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016 (retrieved on 12 February 2019)

[2] https://ec.europa.eu/digital-single-market/en/towards-5g (retrieved on 12 February 2019)

Connected mobility

Connected, automated and autonomous vehicles are starting to revolutionise how vehicles interact with each other, with road infrastructure and other third operators. They have the potential to increase the efficiency of road use and improve both the safety and the environmental performance of vehicles. Key measures are needed to enable this transformation:

- **Legal framework**: The timely adaptation and harmonisation of statutory framework conditions, that enable technological development and allow for connected, automated and autonomous vehicles across borders is an essential prerequisite for the successful development and introduction of such vehicles.

- **Social acceptance**: A broad discussion and a continuous dialogue with society is required for automated and autonomous driving to be accepted.

- **Security and privacy**: It is essential that privacy, security and liability are a priority to allow the digital ecosystem to thrive. Security by design must be central to all Intelligent Transport System (ITS) technologies, supported by a voluntary, market-driven and risk-based cybersecurity certification framework to protect road users.

- **Needed infrastructure**: Infrastructure for connected mobility entails above all the blanket and cross-border installation of an intelligent infrastructure and consistent, high-performance and reliable network coverage.

Digital health

Digital health (eHealth) is an emerging and rapidly developing field which has the potential to transform healthcare to support a variety of health-related services along the continuum of care, increasing its quality and efficient and empowering patients. This technology should be harnessed to support a new healthcare paradigm that is capable of responding to the greatest challenges in this sector by fully exploiting the most innovative solutions. To realise the potential of eHealth, the areas that should be addressed are:

- **Health data ecosystem:** The EU should transition to a healthcare 'data ecosystem' across Europe by adopting a 'holistic' approach to interoperability which will enable healthcare systems to share electronic health records (EHRs) more easily across providers and citizens. A streamlined adoption of international standards will ensure the 'building blocks' on which EHRs are based (eg. standard coded data elements and order sets for medical history) can interoperate across borders and healthcare settings. The Commission should support a wide dissemination of information regarding the benefits and use of common standards for EHRs and to promote their adoption across Europe.

- **Training:** The Commission should lead a debate about the need to reskill and upskill the healthcare workforce, including suggestions to improve educational and professional training systems and helping the understanding and uptake of digital technologies.

- **Reimbursement**: eHealth solutions are currently not covered by traditional reimbursement models. The Commission should foster a change in reimbursement models (eg, through an expert group) to ensure effective, cross-border eHealth services for patient safety and quality of care.

- **EU funding**: The EU should reinforce supporting measures to accompany the digital transformation of the healthcare sector primarily through Connecting Europe Facility (CEF), Horizon 2020/Europe and European Social Fund Plus (ESF+), which can support the development of core infrastructure, the investment in capital equipment and the upskilling of the workforce.

3. Enabling investment, innovation and entrepreneurship

Europe should accelerate the realisation of a genuine Digital Single Market (DSM) and thereby foster an enabling environment for European entrepreneurship to flourish. We need harmonised and interoperable solutions for new technologies to scale-up, incentives for investment in technologies, a boost in digital talent, strong protection of Intellectual Property Rights (IPR)s and continued enforcement of EU competition policy.

Investments

Continued and targeted public and private investments are essential to foster Europe's competitiveness. We welcome the ambitions of the current Commission to boost investments in technologies, such as AI, Blockchain, IoT and 5G.

- **R&D incentives**: Incentives for investment in research, development and the application of emerging technologies need to be put in place to keep Europe competitive. The public sector has a key role to play in fostering and co-developing the best technological solutions. Public procurement based on open standards and strong sustainable requirements presents an essential tool in this regard.

- **Openness**: Third-country participation in EU funding programmes is an important part in Europe's technology ambitions in R&D. In 2016, US industry R&D investment totalled €27.6 billion, representing 58% of total global US affiliate R&D.[3] This includes R&D labs invested by US companies with a long-standing presence in Europe. It is fundamental that international cooperation and third-country participation remains valued and possible without administrative burden and legal uncertainty.

Standards and interoperability

The development and use of global and open standards and interoperability frameworks are instrumental to ensuring an international scale in cybersecurity, smart grids, smart cities, intelligent transportation, IoT, advanced manufacturing and 5G. Therefore:

- We need an strengthened role for the **EU MSP** (Regulation 2012/1025) in international fora and consortia to develop global ICT standards. Interoperability will also be improved by the creation of a public procurement helpdesk for technology purchasing as part of the MSP initiative.

- If there is a need to define new standards, EU institutions should consider in the first place if **international standards** exist, which may, if needed, be transposed into European standards.

- The development of standards should follow requirements and recommended practices under the WTO Technical Barriers to Trade (WTO TBT) Agreement. European standards should be defined through the existing **European standardisation system** embodied in Regulation 1025/2012.

[3] The Case for Investing in Europe 2018: http://www.amchameu.eu/publications/case-investing-europe-2018 (retrieved on 22 February 219)

Talent

More than one-third of skills that will be needed in the future are not considered crucial today.[4] Governments and industry need to work together and re-think current policies to equip the workforce and the broader population with the skills needed in a digitalised economy and society. In particular, governments can build on the numerous successful private sector initiatives, such as those in the area of gender equality and integration or under-represented minorities. The following actions seem essential to adapt to the changing skills demand:

- **Invest in education, life-long learning and reskilling** to ensure our workforce is ready for the jobs of tomorrow. Vocational trainings, apprenticeships and corporate academies and work-ready certifications will continue to play an important role. Furthermore, systems should be developed that enable workers to expand their applied skills throughout their professional career beyond classic academic institutions.

- **Better align education with in-demand skills** to best prepare citizens for the job market of tomorrow. Education in Science, Technology, Engineering and Mathematics (STEM) is crucial. However, emerging technologies such as AI require multi-disciplinary skills, and ethics, arts and creativity will be just as important. Therefore, governments should work with academic institutions to create curriculums that meet the specific needs of a digital technology-powered economy, such as ethical training for engineers and technology training for lawyers or healthcare professionals.

Intellectual property

Strong protection of IPRs is crucial to encourage innovation and investment and thereby a flourishing digital economy in Europe. Recent figures from the EU Intellectual Property Office (EU IPO) have shown that IPR-intensive industries account for around 42% of EU GDP, generate 38 % of all jobs and contribute as much as 90% of EU exports.[5] There is a need to ensure strong protection of IPRs both offline and online, including by making progress towards a cost-effective, high-quality, flexible, rapid and predictable patent litigation system in Europe alongside a unitary patent protection.

Competition policy

Continued enforcement of the EU competition policy in markets that are being reshaped by the growth of the digital economy will remain essential to maintain the robust competition in these markets and promote innovation. Antitrust authorities in the EU and elsewhere have repeatedly confirmed that existing antitrust tools can be applied effectively in these markets in a fact-based, case-by-case manner to ensure that appropriate actions are taken in each case. The Commission has appropriately launched a major study on ways in which the digitisation of the economy may affect EU competition policy and AmCham EU has been an enthusiastic participant in this process. In any initiative stemming from this study, it will be essential to ensure that competition policy tools evolve in such a way that they can continue to address the challenges of the digital economy. Competition tools need to be applied in preference to regulation in view of the highly differentiated and competitive nature of digital markets and at the risk that regulatory approaches may inadvertently chill competition rather than stimulating it.

[4] AmCham EU Future of Skills Briefing: http://www.amchameu.eu/system/files/position_papers/amchameu-future-skills-briefing_note.pdf

[5] EU IPO: https://euipo.europa.eu/ohimportal/en/web/observatory/ip-contribution#ip-contribution_1

4. Building trust

For all businesses, governments and society to reap the full benefits of digital technologies, they need to be trusted by their users. The ability of technical systems to handle and protect personal data and sensitive business data is a key reputational factor for companies, and it is essential to ensure users' safety. The complexity of value chains and diversity of business models and application sectors, as well as the fast-developing digital environment, requires strong public-private partnerships to tackle complex challenges such as IoT cybersecurity or disinformation.

Data protection and privacy

Data protection and privacy is a long journey and discussions will continue on the interpretation of the **GDPR** and its application in new areas, such as Blockchain. Therefore, it is essential that data protection authorities consult regularly with stakeholders, ensure a strong dialogue with industry and guarantee a harmonised interpretation of the GDPR rules across Europe. The European Data Protection Board (EDPB) has an essential role to play in this regard.

While the application of the GDPR is under way, the proposal for an **e-Privacy Regulation** (published in January 2017) which regulates confidentiality of communication has brought considerable uncertainty in terms of data protection compliance. It is important that data, including communications data, is protected in a way that is consistent with the GDPR. The proposed e-Privacy regulation, however, goes far beyond regulating third-party access to communication data in transmission. The proposal exceeds the GDPR by adopting a very strict consent-only approach to the processing of electronic communication data, including all types of metadata.

The scope combined with this strict approach is also problematic: It suggests the inclusion of machine-to-machine communication and a variety of devices, as well as IoT applications as it was recognised by the Commission's non-paper (February 2019)[6]. Communications data and data from IoT solutions do not require the creation of new or specific rules for privacy or security; instead, the GDPR provides a robust framework for the processing of all personal data.

Before moving ahead in the legislative process, full alignment with the GDPR should be ensured and the impacts on the data economy should be carefully understood and considered. Any future rules on confidentiality of communication should be fully aligned with the GDPR.

Ethics in artificial intelligence

Building a common understanding around ethics, transparency and accountability in the area of AI is essential to foster the uptake of this technology. The following considerations are important for future and on-going work:

- Any guidelines should be developed through an **inclusive and market-driven approach**. The future European Commission HLEG guidelines on ethical principles for AI are meant to be updated on a regular basis, a process which should be carried out through the same multi-stakeholder approach.
- Focusing on **use cases** will allow companies to start implementing these guidelines in their research, development and deployment of AI systems.
- The EU should encourage a consistent approach to the development of ethical principles at an **international level**.

[6] https://data.consilium.europa.eu/doc/document/ST-5934-2019-INIT/en/pdf (retrieved on 26 February 2019)

Cybersecurity

Cybersecurity is a responsibility of government and industry alike and the most effective way of advancing it is through public-private partnerships, harmonisation and global cooperation.

With the exponential growth of connected devices, cybersecurity has become a major concern both for the online and physical world. When addressing **security in the IoT space**, the following principles need to be considered:

- **Risk-based approach**: Requirements should be established to secure networks and information based on 'what' must be protected rather than 'how' it must be protected, taking into account the risk profile (ie, smart lights do not need to fill the same security requirements as power plants). On the contrary, pushing for generic or blanket cybersecurity labelling of IoT products could result in counter-productive technology mandates without necessarily bringing any real cybersecurity or privacy benefits.

- **Proportionate approach**: Government procurement, consumer markets and enterprise markets all have unique characteristics and should be appropriately managed in accordance with those differences. The benefits of a 'proportionate' approach will allow the unique characteristics of each market to be addressed with their respective relative risk.

- **International industry standards and organisations**: Globally developed industry standards can be used in order to incorporate industry best practices as well as to ensure a globally interoperable approach that is technology-neutral. Most international standards (both formal bodies and fora/consortia) include voluntary certifications that companies can meet using objective criteria and benchmarks. These certifications are updated on a regular basis, ensuring that companies continue to provide the highest level of protections while meeting an ever-changing environment. Any future EU security certification should strongly align on existing international standards and practices.

In addition, **harmonisation** is essential to increase Europe's cyber resilience. The transposition and implementation of the Network and Information Security (NIS) Directive should be as harmonious as possible. Furthermore, care must be taken not to undermine the light-touch approach agreed by the legislators. Too detailed one-size-fits-all rules and thresholds may not be suitable for every situation.

Finally, cyber threats cross borders and jurisdictions and therefore call for **global cooperation**. The cyber resilience of the DSM will greatly depend on the EU's ability to work effectively and efficiently with foreign partners in particular the US, to adopt common approaches to detecting, mitigating and managing cyber risk at the international level. It is fundamental that the EU continues to strengthen its efforts to drive the international promotion of confidence building measures and the development of norms of acceptable state behaviour in cyberspace. On top of this, we urge the Commission, the European External Action Service (EEAS) and Member States to work closely with international partners and allies on these issues, especially the US.

Law enforcement access to electronic evidence

A new framework on access to electronic evidence (e-evidence) is essential, both within Europe and in the transatlantic context. For important purposes of public safety in the course of criminal investigations, law enforcement authorities (LEAs) across Europe increasingly need digital evidence that is stored or managed in different jurisdictions. However, when requesting access to users' data, LEAs must follow clear rules and procedures that fully safeguard users' privacy and other fundamental rights – especially in cross-border cases where the service provider is established or the data is stored in a different jurisdiction and would involve the interests of foreign citizens or governments. In addition, the EU should ensure that the responsibility for protecting users' rights and compliance with the law is not disproportionately bestowed on private companies.

The **e-evidence proposals** presented by the Commission in April 2018 have the potential to significantly increase legal certainty in this space and provide a basis for an international agreement. However, for the EU to set the right international precedent and create a workable framework, it should respect existing jurisdictional standards and contain strong procedural and material safeguards. The extremely high fines proposed in the Council's general approach[7] are disproportionate and, as the European Parliament's latest working documents[8] point out, they may not even be legal under the Treaties.

Last but not least, long-term solutions can only be achieved with an **EU-US Agreement on law enforcement access**. We welcome the Commission's proposed mandate and encourage the swift start and conclusion of the negotiations.

Tackling illegal content online

The online environment offers tremendous possibilities to distribute content and goods across markets, but also presents challenges as it allows for much wider and faster proliferation of illegal items, such as terrorist content or content infringing IP. Illegal content in all its forms constitutes an obstacle to the creation of a safe and sustainable DSM. A sound and robust enforcement regime is essential for the protection of our members' incentives to continue investing in even more innovative and creative products and services.

[7] https://data.consilium.europa.eu/doc/document/ST-15020-2018-COR-1/en/pdf (retrieved on 22 February 2019)

[8] http://www.europarl.europa.eu/committees/en/libe/working-documents.html?ufolderComCode=LIBE&ufolderLegId=8&ufolderId=12854&source=&linkedDocument=true&urefProcYear=&urefProcNum=&urefProcCode (retrieved on 22 February 2019)

5. Strengthening international cooperation

Digitally-enabled trade represents huge potential for all sectors of the economy[9] and depends on the ability for businesses to transfer data across borders. In the same way, poorly designed policies that increase data processing costs can have a severe economic impact. EU trade policy and the WTO need to modernise and take into account the realities of market access restrictions in the area of digital trade.

Free flow of data

The flow of data between the EU and US – by far the highest in the world – is 50% higher than the data flows between the US and Asia in absolute terms, and 400% higher on a per capita basis.[10] Cross-border data flows are essential to the growth and competitiveness of many segments of European industry such as manufacturing, financial services, retail and healthcare. The **EU-US Privacy Shield** agreement will continue to be a fundamental mechanism to ensure personal data flows across the Atlantic. Today, more than 4,450 companies from both sides of the Atlantic are certified under this mechanism, which safeguards the transfer of personal data.[11]

In addition, as more and more countries adopt privacy regulations with more or less similar approaches to the GDPR, it is essential to foster discussions and alignment on key data protection principles (ie, rules for data breach notification) to avoid fragmentation. The Commission should continue its work to ensure the interoperability of the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules system with Binding Corporate Rules (BCRs) under the GDPR.

Public policy regimes

To facilitate trade in innovative digital services, public policy regimes that minimise regulatory impediments to such services and recognise the trade-enhancing value of market competition should be promoted wherever possible. In order to minimise regulatory impediments and avoid unintended consequences, policies should support regulations that:

- Are limited to specific and legitimate public policy objectives consistent with international treaties.
- Promote data flows and eliminate data localisation mandates.
- Are established pursuant to transparent procedures allowing for comments by all interested parties.
- Do not constitute unnecessary barriers to trade in services, such as impediments to integrated services and complex supply chains.

Procedures should be available to allow for parties to review and eliminate regulations, or forbear from their application in situations where competitive market forces are present to achieve the regulatory objective. In general, when competitors are subject to diverging regulatory obligations, parties should seek to facilitate trade by applying the least burdensome regulatory obligation to all such competitors.

[9] Excluding intra-EU trade, EU member states exported $569.6 billion and imported $418.0 billion in digitally-enabled services, resulting in a surplus of $151.6 billion for these services in 2014 (Transatlantic Economy Study 2018 available at: http://www.amchameu.eu/publications/transatlantic-economy-2018 (retrieved 15 February 2019)

[10] Transatlantic Economy Study 2018

[11] https://www.privacyshield.gov/list (retrieved on 19 February 2019)

Trade policy

EU trade agreements are a key instrument to enhance the cross-border flow of services and to cut costs and administrative barriers. As data becomes a strategic asset to every economy, exporters increasingly face protectionist data localisation requirements and other market access restrictions. Restrictions on data flows may impose a substantial economic burden on small and medium-sized enterprises (SMEs) that provide goods and services with the help of foreign infrastructure such as cloud computing. Newly negotiated trade agreements between the EU and its trade partners need to reflect these new economic realities. Therefore, chapters related to cross-border trade in services should include provisions to:

- Prohibit quantitative restrictions for service providers.
- Support the free flow of data and strengthen the digital economy.
- Restrict localisation requirements for computer infrastructure, manufacturing or service facilities.
- Prohibit forced disclosure of source code or transfers of technology.
- Enable the use of global technology standards.
- Ensure license-free export of dual-use items.
- Reinforce cybersecurity cooperation.

These principles should be leveraged at multilateral and bilateral levels (for instance the future EU-US and EU-UK agreements). The WTO is an important venue for the development of e-commerce rules that will ensure that companies can grow, innovate and create jobs across the globe. Negotiations need to be launched to define cutting edge e-commerce rules that make global trade more inclusive and promote a free and open internet.

Conclusion

There is a strong case to unlock the potential of digital technologies in Europe and ensure their successful uptake across economic sectors. Businesses, governments and citizens can all benefit from the digital transformation. With this in mind, AmCham EU calls on the EU institutions to consider the following priorities for the next EU digital strategy:

1. Rethink the way of doing policies and designing rules by adopting a more principle-, risk-based and market-driven approach.

2. Enact an ambitious agenda on emerging technologies by promoting targeted investments that foster their development and promote uptake across economic sectors and society.

3. Create an enabling environment for investment, innovation and entrepreneurship to flourish by supporting R&D investments, international standards, skills, IP and competition.

4. Build trust in the use of technologies by building strong public-private partnerships and applying existing regulatory frameworks.

5. Allow for businesses of all sizes to scale-up and to trade at the global level by ensuring data flows and tackling unjustified market access restrictions.

This ambitious agenda can only be achieved through strong EU leadership, cooperation with industry and all relevant stakeholders and continued transatlantic and global cooperation. AmCham EU looks forward to continuing to contribute to creating a competitive European digital economy which benefits everyone.