ADVANCING A EUROPEAN TECH AGENDA

ITI's Policy Recommendations for 2020 - 2024

ITI Promoting Innovation Worldwide

Table of Contents

2 March 2020

Policy Recommendations for a European Tech Agenda

Europe’s opportunity to preserve an enabling environment for innovation and ensure its global competitiveness and security

The Information Technology Industry Council (ITI) is the premier advocate and thought leader for the global technology industry. ITI’s membership comprises 70 of the leading technology and innovation companies from all corners of the information and communications technology (ICT) sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity, and Internet companies.

The technological innovations of ITI’s members, and the digitalisation of the economy more broadly, bring innumerable benefits to European industry and society. The tech sector empowers European companies of all sizes and across industries – from agriculture to education, financial services to manufacturing, healthcare to energy and transportation – to leverage frontier innovations towards competition and success in the global marketplace. Whether it is sensors that detect health and safety hazards for workers in real time, or artificial intelligence that allows doctors to analyse complex medical data faster than ever, technology allows us to address some of the most challenging issues of our time and improve the quality of everyday life for Europeans. The tech sector is also already taking significant steps to help prepare the workforce of the future for the shifting skills and competencies that are required in the 21st century.

Tech policy is a crucial priority in the 2019-2024 EU term, one on which Europe has an opportunity to play an international leadership role on policy issues that are increasingly global. ITI and its members believe that building trust and fostering the public interest in the era of digital transformation are essential. Our companies have made great strides in bringing the positive societal benefits of transformative technologies to fruition and remain committed to upholding the fundamental principles of privacy, inclusivity, transparency, and democracy that underpin European society. We believe in the importance of preserving an enabling environment for innovation to ensure Europe’s global competitiveness and security. Europe’s digital infrastructure is the foundation for that. 5G is a core element to support digital transformations in industry and society, estimated to enable more than €2.2 trillion worth of economic output in Europe by 2030.

ITI has developed recommendations outlining concrete steps that policymakers can take, in partnership with industry, academia, civil society, and other stakeholders, to effectively implement the ambitious agenda for **“Shaping Europe's Digital Future”** launched by the European Commission in February 2020. Our recommendations address the economic and social implications of technology and the role of our industry, in a manner that supports innovation, while recognising the public interests at stake. They focus on the following key policy areas:

International Cooperation

Global cooperation and open competition are essential to advancing innovation

Amid calls to boost Europe's "technological sovereignty" in response to concerns about the bloc's diminishing contribution to global value chains and its significant dependence on foreign technologies, we embrace the Commission's statement that this notion is not about protectionism, but about developing stronger players on key technologies in Europe (e.g. artificial intelligence, 5G, quantum computing, cybersecurity, blockchain, data sharing and data usage etc.), and we believe that together we can increase Europe's global competitiveness.

Maintaining and increasing the ability to develop key technologies and ensure their availability to the EU in the future is an unquestionable aim for the EU, as it would be for any government. Our industry acknowledges the sincere public interest objectives the EU is pursuing, and we want to be an active and constructive partner of the EU in achieving those aims.

The notion of technological sovereignty is closely intertwined with that of "strategic autonomy," addressed by the European Commission's own think tank - the European Political Strategy Centre (EPSC) – in its note on strategic autonomy in the digital age (July 2019) noting how digital technologies affect all dimensions of strategic autonomy. We welcome the European Commission's statement made in its *Shaping Europe's Digital Future* Communication of February 2020 to not define technological sovereignty *against* particular actors but rather to use it as a way to advance the European technology industry while excluding protectionism and discrimination. Any other approach could harm European interests, and negatively affect larger societal and economic goals, such as the pursuit of innovation, prosperity, peace, and security.

Our Recommendations

1. **Ensure Europe remains committed to free trade and multilateralism.** Europe can strengthen its ability to shape the digital revolution by embracing globalisation; recognising the significance of its mutual interdependence with like-minded democratic countries like the U.S., Japan, Australia, Singapore and others; and building on the benefits and successes of global collaboration. Moreover, the EU is well placed to benefit from increased international trade, given its companies' high levels of global competitiveness. Since the beginning of the century, EU goods exports have almost tripled, increasing by approximately EUR 1.5 trillion.[1]

2. **Embrace openness as a key driver of innovation.** Many people have put forth suggestions to achieve "technological sovereignty" through new approaches to trade, data and other issues. Most of these ideas can be implemented in ways that are compatible with Europe's longstanding commitments to free trade and open markets and should not be based on the false premise that excluding or otherwise treating foreign entities differently is the way to strengthen Europe's technological autonomy. An open EU economy is in fact a major source of productivity gains and private investment, which in turn foster new technologies, research, and innovation. One cannot and should not forget that globalisation benefits European innovation.

3. **Recognise globalisation's contribution to the European economy.** We encourage the Commission to maintain its long-standing commitment to collaborating with like-minded democracies and

[1] *See* European Commission Communication - Trade for All, Towards a more responsible trade and investment policy, 2015

economic partners. The global nature of many companies is a crucial element of their innovation strategies, their contributions to Europe's goal of maintaining and increasing the ability to develop key competences and technologies and ensure their availability in the future, their efforts to create jobs and enhance competitiveness in Europe, and their commitments to European values, regardless of where they are headquartered.

4. **Maintain a global leadership role in fostering innovation by relying on global industry-led standards.** In a context of globally integrated markets and value chains, the EU will maintain a leadership role in fostering innovation and interoperability by deepening its international engagement in a broad range of standards development organisations, as well as advancing its legislative agenda. GDPR and the EU Cybersecurity Act are recent examples of Europe's global influence. As the EU moves to implement these measures, it will be important to support international, industry-led, consensus-based standards development bodies. These bodies will develop the most appropriate voluntary standards, which can serve as ways for companies to meet regulatory or other requirements; however, governments should resist the temptation to prescriptively select specific standards that shall fulfill regulatory requirements. As technology and consumer demand changes, so too will standards, allowing companies to adopt the newest and most appropriate standards. This supports the ongoing rethinking of regulation's impact on domestic innovation, industry's competitiveness overall, and Europe's goal of developing new technological capability, resiliency, and influence on the development and deployment of new technologies globally.

Artificial Intelligence

Global convergence will benefit the people, society and economy of Europe

Europe has an opportunity to take an international leadership role on Artificial Intelligence (AI). In view of the publication of the European Commission's White Paper on AI on 19 February 2020, ITI offers the following recommendations **for a successful European AI agenda**, addressing the economic and social implications of technology and the role of our industry, in a manner that supports innovation, while recognising the public and individual interests at stake.

Technological innovations bring innumerable benefits to the European economy and society. We are already experiencing the benefits of AI in an array of fields. **Promoting these advances is no less important than managing any potential challenges.** Stakeholders globally are aware of and addressing the main challenges posed by AI. For instance, there is a recognition of the need to mitigate bias, inequity, and other potential harms in automated decision-making systems.

The tech industry shares the goal of **responsible AI use and development**. As technology evolves, we take seriously our responsibility as enablers of a world with AI, including seeking solutions to address potential negative externalities and helping to train the workforce of the future.

Our Recommendations

1. **AI policy should be flexible to match the rapid pace of technological development**. AI is a suite of technologies capable of learning, reasoning, adapting, and performing tasks in ways inspired by the human mind. The technology is constantly evolving and improving, as are the tools to address some of the challenges around explainability, bias, and fairness. The potential benefits of AI development are enormous and premature legislation should be mindful of the fast pace of technological advancement.

2. **Context is key in identifying appropriate policies.** Our industry is committed to partnering with relevant stakeholders to develop a reasonable accountability framework for AI. As leaders in the AI field, ITI members recognise their important role in making sure technology is built and applied for the benefit of everyone. We support the EU's "human centric" approach which underlines ethical aspects in AI deployment. But **approaches must be context- and risk-specific and should take into account that not all applications require an all-encompassing fundamental rights-based approach**. Some basic AI uses have little or no impact on individuals' rights, such as in the context of industrial automation and analytics to streamline automobile manufacturing or to improve baggage handling and tracking at busy European airports. Many other uses – e.g. in medicine, financial services or transport – are subject to sectoral regulation already. A proper assessment of applicable laws should precede new legislation that could lead to conflicts of law.

3. **Prioritise an effective and balanced liability regime**. AI presents great opportunities for society in different fields yet raises valid concerns around responsible and safe deployment. The clarification of rules around liability, currently designed for physical products, is an appropriate area of focus. There are also important considerations about finding the appropriate balance of ex-ante, preventive rules and ex-post remedies. We support a framework that adequately compensates victims for damages and provides a clear path for redress. In many cases the current regime will be easily applied in an AI/software context, but there might be cases where rules may have to be reviewed or amended. **Any review will have to take into account use cases that can have an effect on liability**. Digital products are developed through a trial and error process aimed at constantly improving products and services,

including their safety and security, even after they are made available to the public. If a vulnerability or a harmful exploit is detected in a product or service in the market, developers send out patches to mitigate such risks, giving a new dynamic to the liability framework as users can choose not to install patches, raising questions around responsibilities between producer and user. In that sense, applying the exact same rules to AI as for other types of products might be hard.

4. **The EU should further the development and use of AI *globally* by cooperating with its international partners**. As the AI ecosystem is global and the technology is not developed in regional siloes, the most effective means of advancing Europe's AI agenda is to expand the discussion beyond national borders. Europe should move away from an 'AI made in Europe' narrative – many AI products and services used in Europe are comprised of both European and non-European elements developed in different locations and in line with international standards. The EU should work towards trustworthy AI for its citizens by ensuring its approach fosters the region's global competitiveness, in turn helping Europe shape global AI governance.

5. **Recognise the significance of Europe's mutual interdependence with like-minded democratic countries, and the importance of shared common values** like trust, fairness, explainability, effectiveness, safety, and human oversight - the core principles that need to guide future policy action on AI. There is a valuable opportunity in working together to shape balanced solutions in situations where the application of some of these values conflicts in practice – for example, when explainability (through simpler algorithms) can conflict with accuracy, or human intervention reduces quality results (e.g. in misreading medical scans).

6. **Assessing the need for upgrading the regulatory framework to enable AI to fulfil its potential in Europe is crucial** to identify what legislative gaps exist and the extent to and manner in which any such gaps should be filled. We value the evaluation of sector-specific legislation that is being carried out by the European Commission. Many ITI members have also engaged in the European Commission's High-Level Expert Group (HLEG) on AI and helped create the ensuing ethics guidelines and policy recommendations; several of our members have also partaken in the AI piloting phase. We encourage the European Commission to continue involving stakeholders in the crafting of the European AI approach, including any regulation.

7. **Availability of and responsibility for securing personal data** is key, as many promising uses of AI rely on personal data. By leveraging large and diverse datasets and increased computing power and ingenuity, AI developers and other stakeholders innovate across industries to find solutions that will meet the needs of individuals and society in unprecedented ways. AI-driven medical diagnostics can alert doctors to early warning signs to more capably treat patients. Increasingly intelligent systems are capable of monitoring large volumes of financial transactions to more efficiently identify fraud. SMEs can gather new insights and improve their businesses by using AI and data analytics made available to them through cloud services.

8. **Support global, voluntary, industry-led standardisation**. Standardisation can help form a bridge between AI regulations and practical implementation. The EU should support and safeguard the work and processes of international standards development bodies. Global AI standards can help establish global consensus around technical aspects, management, and governance of the technology, as well as frame concepts and recommended practices to establish trustworthiness of AI inclusive of privacy, cybersecurity, safety, reliability, and interoperability. Standards must not establish market access barriers or preferential treatment; rather, they should work for the benefit of the international community and be applicable without prejudice to cultural norms and without imposing the culture of any one nation in evaluating the outcomes/use of AI.

9. **Ideas for new ex-ante conformity assessments that include independent audit and testing by public authorities to ensure that high-risk AI applications adhere to EU rules should carefully consider the practicability and added value of such an approach, taking into account existing sectoral certification processes.** While we appreciate the need for strong assurances, it is not at all clear that the existing conformity assessment infrastructure could effectively carry out prescribed testing on what are often among the most socially valuable applications of AI. For instance, the lack of expertise needed to evaluate datasets or algorithms in sufficient depth as well as the volume of requests would create significant practical and capacity challenges, particularly if such evaluations could only be undertaken by Notified Bodies. Finally, giving an independent assessment body access to the underlying data used to train a model, including algorithms, source code, or other proprietary information, could also lead to conflicts of laws.

Privacy

Individual and enterprise trust is key to innovation

ITI prioritises the goal of protecting personal privacy. We believe in empowering people through a strong, uniform, and consistent set of privacy protections, no matter where their data is located.

Europe has developed an extensive framework for privacy, and the GDPR is having a global impact on many governments' efforts to update privacy legislation or pass privacy laws for the first time. These developments will help foster the trust of individuals and businesses in digital products and services. The continuing implementation of the GDPR should focus on deep harmonisation within the EU, while being flexible to accommodate the ongoing tech evolution that brings benefits to individuals, businesses, and society in sectors like healthcare or mobility.

Individual trust in market rules and market players is crucial. Ensuring users' access to and control over personal data enhances trust and transparency, leading to increased consumer welfare in the form of innovative products and services at lower prices or free of charge. Strong privacy protections are not in opposition to innovation; in fact, robust privacy rules, combined with strengthened data governance, can jumpstart innovation. Big data and AI applications generate substantial innovations and efficiency gains that are passed on to consumers, augment human capability and enable advances in education, healthcare, transportation, sustainability, and many economic efficiencies in innumerable fields. Independent of the specific country or region, companies must manage data responsibly to earn users' trust and fulfil their expectations with regard to privacy.

In the world of digital transformation, the full potential of the modern economy cannot be realised without increased trust. Privacy violations hinder innovation and growth by eroding public trust in digital goods and services. Effective privacy and data protection safeguards can help maximise individuals' participation in the economy and harness the full potential of the ecosystem. While there is no single approach to privacy that works for all jurisdictions, stronger and more coherent principles on data protection globally mean people have more control over their personal data, and that businesses can benefit from greater confidence and trust.

As business models and applications change rapidly, it is important to avoid creating artificial boundaries and limitations on the use of data. Inflexible and overly prescriptive regulation or excessive compliance burdens may stifle innovation, undermine the development of new growth-enhancing businesses, impact the personalised services consumers benefit from, or even run counter to the privacy interests they purport to serve. Businesses rely on their ability to operate globally and transfer data across borders. Global approaches to privacy should encourage the adoption of innovative security and privacy best practices, recognising the benefits of techniques and controls that obstruct re-identification and better enable research and innovation in areas that rely on data use such as machine learning and AI. Fragmented approaches to privacy across the globe create unnecessary costs, and onerous requirements that degrade the user experience, or deter innovation and SMEs' participation in the digitally-enabled economy. In an effort to better inform ongoing privacy discussions globally, ITI developed the "Framework to Advance Interoperable Rules (FAIR) on Privacy" (FAIR on Privacy), a roadmap toward the goal of protecting privacy and personal data to advance the interests of individuals, businesses, and governments.

Our Recommendations

1. **Emphasise the importance of global collaboration and promote interoperability between regional mechanisms for international data transfers.** Article 42 of the GDPR on recognising and approving certifications creates the perfect opportunity to identify commonalities between the approaches of

the EU and other regions, particularly the Asia-Pacific, by exploring potential interoperability through certification pursuant to GDPR Article 42 and APEC Cross-Border Privacy Rules (CBPR).

2. **Continue implementation work to provide legal clarity for businesses on GDPR compliance.** Our companies have embraced the GDPR as a milestone in safeguarding privacy and trust. Ensuring consistent application across the EU will help bring clarity for regulators, businesses and individuals, including by checking its interaction with other rules. We urge the European Data Protection Board to continue to publish guidance on key aspects of GDPR, in particular on data subject rights.

3. **Encourage global partners to commit to ongoing dialogue in official forums on international transfer mechanisms**, while providing robust and future-proof mechanisms for data transfers. We stand ready to support greater interoperability in privacy rules and data flows globally. **Privacy Shield** remains a crucial mechanism to ensure secure data transfers between the U.S. and the EU. We welcome the Advocate General's Opinion in the *Schrems II* case regarding standard contract clauses (SCCs) and hope that the Court will also uphold the Privacy Shield in the *La Quadrature du Net* case.

4. **Ensure seamless data flows between the EU and the UK post Brexit.** We encourage the EU and UK to prioritize the negotiation and adoption of an adequacy decision by the end of 2020 to ensure that data continues to flow freely between the EU and the UK, avoiding unnecessary business interruptions or impacts on EU companies and others doing business with the EU and UK.

5. **Cybersecurity is essential to ensure privacy**. The EU has a great track record in this area, and we hope that critical cybersecurity measures will be encouraged as part of any efforts to improve privacy protections, including by recognising security as a legitimate interest for processing personal data in the proposed e-Privacy Regulation.

6. **Clarify interplay between e-privacy and GDPR.** After lengthy negotiations, uncertainty still remains around the proposed e-Privacy Regulation, including its scope, definitions, legal bases and the relationship with the GDPR and new technologies like AI. This new legislative term provides the opportunity to reconsider the proposal, avoiding the introduction of overly strict rules on consent for data processing that would duplicate efforts made under GDPR, or unnecessarily restrict the processing of non-personal data essential to Europe's digital innovation and competitiveness. We stand ready to support the EU' efforts to enhancing privacy while avoiding unintended consequences.

7. **Advocate against forced data localisation globally.** Governments around the world are increasingly seeking to enact data localisation measures, normally due to misconceptions that they strengthen security, privacy or allow for easier government access to data. We urge EU policymakers to **engage closely with international partners – particularly China, Vietnam, Indonesia, India, and South Korea – to deter them from introducing data localisation** requirements and encourage international cooperation to identify solutions balancing privacy, security and economic growth.

8. **Enhance law enforcement cooperation in an effort to establish efficient mechanisms and protocols for threat information sharing and data access requests**. We welcome the EU e-evidence proposal that will improve intra-EU cross-border data sharing and lays the groundwork for improved global cooperation. Moving forward, the proposal should ensure stronger privacy safeguards and further avenues for service providers and enforcing authorities to challenge data requests – both are necessary to protect the fundamental rights of users. The U.S. CLOUD Act is another mechanism to potentially facilitate cooperation between the EU and the U.S. in this space. Skepticism about the CLOUD Act prevails in many jurisdictions, owing to misunderstanding of its intent and impact, and a lack of appreciation regarding the increased safeguards it requires of executing parties. The EU should also be cognizant that its approach to government access to data will set an important precedent that could impact individual privacy rights globally.

Data Governance

A balanced framework is key to innovation

Digital innovation relies on the availability of large and diverse datasets from the private and the public sectors, enabling technology developers to innovate across industries and meet the needs of individuals and society in unprecedented ways. For example, analysing data and producing customised recommendations based on learning from a large pool of similar cases can revolutionise the delivery of healthcare and facilitate a new wave of personalised modern conveniences for European citizens. Much of this functionality will be built upon insights gleaned from non-personal data sets – that is, data which is anonymised or not directly relatable to a specific individual.

To realise this potential, it is critical to ensure that technology developers are able to access high quality public data sets. Allowing businesses and the general public to reuse data can help boost economic development within the EU as well as transparency within the EU institutions. Open government data is a tremendous resource that is as yet largely untapped. There are many areas where open government data can be of value to many different groups of people and organisations, including EU governments themselves. The benefits of more available open data sets lie in the creation and delivery of new products and services.

In addition, open data can be used to help transform businesses across industry sectors from within as they embrace the digital world. We appreciate the European commission's focus on data governance with the adoption of **Europe's Data Strategy** in February 2020, and put forth the below recommendations for the EU to realize its fullest potential by continuing to invest in and prioritizing the institution of effective data governance initiatives, which encourage digital transformation across sectors.

Our Recommendations

1. **Business-to-business data sharing should remain voluntary.** Voluntary agreements between companies constitute today the main tool for business-to-business data sharing, and several consultations at the EU level in the past few years seem to confirm that there is no demand to create legal obligations in this area. We caution against blanket sharing obligations that would threaten investment in research and could stifle innovation.

2. **Make public data more accessible.** Facilitating a robust government data access and data sharing environment will be critical for the EU in the coming years. The EU should continue to catalyse economic growth through digital transformation by publishing public data under an open license and applying an 'open by default' principle. The EU should also continue to facilitate the removal of other barriers to widespread open data use. These barriers include lack of awareness, lack of knowledge, and poor data quality.

3. **Business-to-government data sharing should be encouraged on a voluntary basis.** We strongly support the claim that requests for the reuse of privately held data by public bodies should be proportionate, balanced and limited to the minimum extent necessary for the performance of their functions, based on a voluntary system.

4. **Opportunities to collect and distribute data responsibly can be created through data-sharing agreements**. The EU should incentivise investment in tools to monitor and improve AI as data is collected and ages, and also play a leading role in collecting data that will improve core supply chain issues such as predictive maintenance and safety. The EU framework has proven that most issues can

be solved by adequate application of existing rules. Interoperability, transparency and non-discrimination should be the key principles for the future.

5. **The EU can encourage global partners to commit to similar efforts to make open data more readily available via dialogue in official forums.** We stand ready to support these efforts towards promoting greater innovations and digital transformation across industry sectors and public institutions.
6. **Data portability should be enhanced.** Considerations related to switching, access to data and portability should take into account specific situations and contexts and avoid a one-size-fits-all approach. IP and trade secrets should be respected and safeguarded. Imposing rigid standards to enable data portability could have unintended consequences by hardwiring the status quo, forestalling innovation, and precluding future portability.
7. **High-quality training data can enhance research.** Sharing and making more high-quality training data available would enable better training of AI algorithms, and the EU could maximise AI's development in Europe and the value of its digital assets by allowing open access to machine-learning friendly datasets for R&D, provided that sufficient privacy and security protections remain.
8. **The EU should take a thoughtful approach to data sharing for law enforcement purposes.** Europe should work towards a clear framework for businesses when it comes to law enforcement cooperation. Efficient information-sharing and data access request mechanisms need to be established at an EU level. The EU should bear in mind that its approach to government access to data will set a precedent impacting individual rights globally, including in countries with fewer rule-of-law and fundamental rights safeguards.

Cyber and Supply Chain Security

Policy should reflect shared responsibility and the changing nature of cyberspace

ITI's members are global companies with complex supply chains, including both producers and users of cybersecurity products and services. Cybersecurity risks have intensified as the world's digital infrastructure has become increasingly interconnected and magnified by major technological shifts like cloud, IoT, AI, and 5G. We support the EU's continuous work with its international partners to strengthen cybersecurity.

Cybersecurity is integral to the EU's economy and competitiveness. While cyberspace holds great benefits for society, it also presents opportunities for misuse and exploitation. Cybersecurity concerns hinder innovation and growth, jeopardise trust, and threaten national security, economic growth, and individual rights. Increasingly sophisticated adversaries target European governments, organisations, and citizens, and attack the **global supply chains** of essential products in the EU's digital infrastructure. While both ICT companies and governments are focusing on managing supply chain risks and the security of networks, malicious behavior is an increasing and ever-evolving threat for both the public and private sectors. Industry is in the process of building security into products, services, *and* supply chains, along with providing security solutions, while governments play a key role in advancing cybersecurity best practices. The EU has acknowledged that cybersecurity is crucial to Europe and identified cybersecurity as one of its top priorities. As cybersecurity threats diversify, malicious cyber activities not only threaten the global economy (and the Single Market), but also Europe's democracies, freedoms, and values. The tech industry's interests in and shared goal of improving cybersecurity are fundamentally aligned with those of the EU.

Cybersecurity policy must reflect a shared responsibility and the changing nature of cyberspace. Security is a continuous process of risk management, technology development, and process improvement that must evolve with today's highly complex and dynamic environment. Cybersecurity is a shared responsibility – neither governments nor companies can address it alone. A range of policy tools and approaches is available to meet our shared security objectives, including risk management, threat information sharing, technological innovation, education, and raising awareness. These tools and approaches must be manageable and interoperable – too many silos can create a risk of overlooking or failing to connect the dots between incidents and events across networks. Static or overly prescriptive rules will not provide a lasting solution to cybersecurity concerns, since they quickly become outdated as business models and technology change and cyber adversaries evolve.

Data localisation measures weaken cybersecurity by creating a single point of failure in a given jurisdiction. Still, often due to misconceptions about improving security or access to data, some governments continue to pursue data localisation measures, creating attractive hacking targets and making data vulnerable to natural disasters and technical failures. The EU should discourage such policies.

Our Recommendations

1. **Promote international best practices in cybersecurity.** We recommend that Europe's future cybersecurity policies support and align with international industry-backed approaches to risk management, such as the ISO/IEC 27000 family of information security management systems standards. Other tools providing a common language to manage cybersecurity risks (such as the U.S. NIST Cybersecurity Framework) should also be considered in the upcoming NIS Directive review.

2. **Align EU cyber certification with international standards.** The EU Cybersecurity Act's certification framework should be implemented in a way that is adaptive and risk-based. Existing international standards should be the basis for developing certification schemes – including in the ongoing SOG-IS framework, the cloud security working group and potential schemes regarding IoT or 5G security. Continuous support for countries in developing capacity will also be crucial to enhance cyber hygiene and best practices.
3. **Develop a multi-stakeholder, public-private approach to cybersecurity.** As many countries launch multi-stakeholder initiatives to address cybersecurity vulnerabilities with different sectors, such as IT, finance and telecoms, we recommend the EU continue to seek active participation of the private sector, including in the form of consultation or comment, in order to direct its resources where cyber risk is most critical and imminent, as well as active partnership to facilitate mechanisms to deal with the complex nature of global cybersecurity challenges.
4. **Address supply chain security collaboratively**. Supply chain security will be critical as the EU moves to deploy 5G networks, and the EU should promote the adoption of baseline security requirements in the supply chain aligned with international best practices, encompassing risks in both product and service-oriented suppliers. A risk-based approach to supply chain security, which extends to network security and therefore 5G security, in which evidence-based risk assessments are conducted throughout the supply chain is another important fundamental. The EU should seek to develop incentives to encourage ICT vendors, including in 5G and consumer and industrial IoT, to adopt supply chain and cyber hygiene, including for example transparency in how organisations manage supply chain risks. Lastly, public-private partnerships can be an efficient way to help companies implement cyber hygiene and mitigate supply chain risks.
5. **Advance policies to recognise the growing complexity of emerging technologies.** To realise the tremendous promise and digital transformation of new technologies, we need equivalent security transformation and policy solutions. The EU clearly understands the cybersecurity risks resulting from emerging threats and should cultivate cooperation with the private sector and global partners, and also participate in the development of global, voluntary, and consensus-based standards and best practices.

Taxation

Ensuring a strong, functioning and dependable international tax system

The tech sector seeks to be a critical and constructive voice in conversations about cross-border taxation and strengthening the global tax system. Ensuring a strong, functioning and dependable international tax system is a priority for our industry. In recent years, a number of EU Member States have launched their own approaches to taxing digital services, spurred by arguments around tax fairness. Similar efforts are also being explored in other parts of the world. Unilateral measures are ill-suited to address broader underlying challenges related to taxing online activities. Any individual-economy approach that targets companies on the basis of revenue thresholds and specific business models has the potential to violate existing tax treaties, risk double taxation, and present continuing trade implications. These measures are also likely to cause increased fragmentation of the international tax system resulting from conflicting and overlapping policies.

ITI therefore supports multilateral engagement at the Organisation for Economic Cooperation and Development (OECD) as the best approach to grapple with the complex cross-border taxation policy issues related to the digitalization of the global economy. Beginning with the Base Erosion and Profit Shifting (**BEPS**) project in 2013, major economies have been at work to comprehensively address a number of tax policy issues through discussions led at the OECD. These and more recent conversations reflect the need for a cooperative, global approach to an inherently international set of issues. We have long engaged in dialogue at the OECD and in capitals, providing input to policymakers about the impacts of proposed policies and feedback about technical design features, with the primary purpose of strengthening the international taxation system.

Discussions at the OECD continue to push forward and intensify as countries look to find a global solution by mid-2020. These efforts have led to agreement on many design characteristics of an updated international tax system that would allocate more profits to market jurisdictions and create a framework to ensure that entities pay a minimum level of tax. This process has continued to move forward with the objective of reaching political agreement on all aspects of a new system’s design by July 2020. We hope that this multilateral process will achieve a result that builds on the success of BEPS, and stand ready to work with policymakers to facilitate such an outcome.

Our Recommendations

1. **Working towards a global solution.** We encourage the EU and its Member States to rely on the OECD as the vehicle for contemplating and agreeing upon reforms to the international tax system. Any reforms should be comprehensive and income tax-based, avoid double taxation, and include appropriate dispute resolution mechanisms that will provide certainty.

2. **Avoiding discriminatory, unilateral policies.** Many of the proposals under consideration or already in place are discriminatory in their current form, raising trade policy concerns while creating a precedent for potential taxes affecting a broad range of digital revenues. There must be a clear, continuing commitment that unilateral measures that have already been put into place will be reversed once an OECD solution is found.

3. **Curbing a fragmented policy approach.** A patchwork of inconsistent policies should be avoided, given the negative impacts on economic growth and innovation. If countries implement significantly divergent approaches, companies will face the possibility of similar but incompatible policies across

multiple jurisdictions, which is likely to impose multiple layers of taxation on the same income without effective avenues for relief and discourage innovation, investment and IT-related job creation in the EU.

4. **Seeking stakeholder input.** It is essential to include the broader global business community and seek buy-in. Policies under contemplation will create equities for all multinational businesses across economic sectors and geographies.

Trade

Promoting 21st Century commitments for Europe and the global economy

Amid turbulence in the international trading system, the EU is positioned to further its standing as a champion of multilateralism and open markets through leadership both at the World Trade Organisation (WTO) and in its domestic policies. Europe can demonstrate to economies around the world that open economic policies facilitate productivity gains and investment, which in turn foster new technologies, research and innovation. The ICT sector shares the view that a rules-based trading system provides the necessary stability to ensure continued growth, development and inclusivity in the global economy. Global trade challenges demand meaningful international cooperation, and ITI will support the EU's efforts to drive the reforms necessary to ensure that global trade rules remain relevant, effective and enforceable.

The last decade has seen a fundamental shift in the way global trade is conducted. **Globally competitive companies across all sectors rely on a vast array of data-driven digital technologies to produce, export, market, and sell goods and services**. Global cross-border data flows grew by 45 times from 2005 to 2015, and 75 percent of the value created by cross-border data flows accrues to traditional industries. Technology products and services drive growth and job creation in virtually every sector of the economy. EU manufacturers of automobiles and aircraft depend on real-time access to global data as a means of conducting their day-to-day operations, driving innovation in the implementation of new technology, and improving product performance and safety. EU small businesses of all types leverage technology platforms to reach new customers in foreign markets – an impossible feat only a decade ago.

However, commitments in trade agreements have not kept up with the rapid pace of change in global trade. Companies are increasingly subject to conflicting and restrictive national policies governing digital services and emerging technology, driving the need for strong trade policy tools. **Updated digital trade rules at the WTO and in future free trade agreements (FTAs)** are necessary to ensure that companies can continue to grow, innovate and create jobs. As the EU continues its active engagement in WTO E-Commerce Negotiations, it should seize the opportunity to lead in the advancement of trade provisions that meaningfully combat barriers to digital trade, including discriminatory data governance policies in order to uphold, while advancing best practices for regulatory frameworks that serve the public interest and allow for the transparent and non-discriminatory transfer of data across borders.

At the same time, the EU's efforts to expand its trade and investment relationships with key trading partners provide important opportunities to advance commercially meaningful, high-standard outcomes and foster regulatory compatibility in areas of emerging technology. This remains crucial in the context of the **transatlantic commercial relationship, the largest bilateral trade and investment relationship in the world.** The U.S. is the largest non-EU consumer of EU digitally enabled services exports, accounting for $179.6 billion in 2017, more than all comparable EU exports to Asia and Oceania. Through deepening engagement, the EU and the U.S. have the opportunity to establish a model for the promotion of regulatory compatibility across sectors, including through increased reliance on global, industry-driven, voluntary consensus standards. Convergence on these solutions is increasingly important as both governments pursue fit-for-purpose approaches to regulating digital services and emerging technology. In addition, working with the U.S., Japan and others, the EU can build on recent successes (like the Joint Statement of the Trilateral Meeting of the Trade Ministers of Japan, the United States and the European Union (14 January 2020) by **fostering consensus on new rules to address unfair trading practices.**

Elsewhere, we support the EU's efforts utilize existing bilateral initiatives with countries like Indonesia to **directly confront barriers to trade in ICT goods and digital services**, including the potential imposition of tariffs on electronic transmissions. Similarly, the EU should seek to advance strong, non-discriminatory intellectual property protections, including through provisions that curb counterfeiting and piracy.

Finally, as the EU engages the UK to establish the parameters of **the future economic relationship**, we strongly support its efforts to pursue a mutually beneficial, forward-looking bilateral arrangement that prioritises the **continued cross-channel movement of data**, as well as **pragmatic, flexible approaches to regulatory compatibility** that facilitate innovation, the open exchange of goods and services, and strong protections for privacy, security, safety, and the environment.

Our Recommendations

1. **Pursue a vision of free trade and open markets.** Through political prioritisation and continued intergovernmental cooperation, we call upon the EU to safeguard and revitalise a multilateral trading system that continues to provide a stable, predictable, and effective framework for companies of all sizes across the world. This will help economies grow and prevent the risk of trade disputes.

2. **Advance the EU-US trade relationship.** ITI strongly supports a **structured dialogue between the U.S. and EU** to deepen trade engagement and facilitate greater cooperation on areas of common concern. This dialogue could serve as a venue to facilitate greater collaboration on unfair trade practices of common concern, including subsidies, state-owned enterprises and barriers to digital trade; facilitate greater collaboration on security challenges of common concern, including through alignment of, i.e. export control policies; and engage on emerging digital policy initiatives with a view to fostering interoperability and limiting the emergence of market access barriers.

3. **Develop a forward-looking framework for economic partnership with the UK.** In near-term engagement with the UK on the terms of the EU-UK future economic relationship, we encourage the EU to pursue a mutually beneficial, forward-looking bilateral arrangement that prioritises the continued cross-channel movement of data, as well as pragmatic, flexible approaches to regulatory compatibility that facilitate innovation, the open exchange of goods and services, and strong protections for privacy, security, safety, and the environment.

4. **Craft a balanced approach to data flows in trade agreements.** We encourage the EU to work with industry and like-minded governments to craft a balanced approach to data flows in trade agreements that allows data to flow freely across borders while safeguarding strong privacy protections. Trade agreements should not be used to regulate or circumscribe appropriate privacy or cybersecurity practices. They should rather contain narrowly tailored exceptions to digital trade provisions to allow participating countries to adequately protect data while preventing the imposition of overly restrictive or discriminatory measures.

5. **Advocate for fair and open trade relationships vis-à-vis global partners.** In collaboration with industry and like-minded governments, Europe should address policies and practices of third countries (e.g. China, Vietnam, South Korea, India, Indonesia) that unjustifiably restrict the movement of data, disregard intellectual property protections, create unfair competitive conditions and hinder the development and use of innovative technologies, including market-distorting subsidies, forced data localisation measures, and other requirements to use local servers and software, rather than best available technology.

6. **Advance engagement in the WTO E-Commerce Initiative.** The EU should seek to secure the strongest possible commitments for eliminating or reducing barriers to trade and facilitating the development of strong, interoperable regulatory frameworks in areas like privacy and cybersecurity. These include commitments to facilitate the flow of data across borders; prohibit localisation of data and forced disclosure of source code, algorithms, and encryption keys; expand market access commitments in

sectors key to e-commerce, and simplify and expedite customs clearance procedures. The EU should continue to lead in seeking a permanent moratorium on customs duties on electronic transmissions.

7. **Pursue strong digital trade chapters in FTA negotiations.** We encourage Europe to factor the commitments noted above into its work on bilateral and regional FTAs. Doing so is particularly important in bilateral engagements where such commitments would serve to directly address existing **barriers to trade in ICT goods and digital services.**

8. **Continue to advance the Better Regulation agenda.** The European Commission should do so with respect to proposed regulatory approaches to digital services and emerging technology, with a view toward increasing regulatory transparency, ensuring coherence across legislative acts, improving WTO notification practices and preventing the emergence of technical barriers to trade.

Digital Services

Policies for internet intermediaries should encourage innovation and resolve proven market failures

The internet has greatly incentivised the development and deployment of a wide variety of innovative content, applications, and services. Online platforms play an indispensable role in driving innovation and growth in the economy, creating market opportunities and access for businesses of all sizes. In parallel, policymakers around the world are grappling with real challenges caused by the scale, speed, and complexity of platforms and their ability to shape public opinion. At ITI, representing the tech industry as a whole, we understand and recognise our shared responsibility to maintain a safe, inclusive, and innovative online environment. As in every public space, harmful and illegal content may be found on platforms. Policymakers in Europe and around the world have rightfully committed to ensuring the safety of their citizens and economies and to respecting fundamental rights. Our companies are aware of their transformative role in society and are committed to take responsibility that the Internet stays a safe and open place for all. It is also paramount that all relevant players work together to ensure a functioning online market and sufficient protections for users, consumers, smaller businesses and brands.

We understand one of the central goals of the Digital Services Act is to increase **legal certainty,** including by updating the 2000 e-Commerce Directive (ECD) to clarify roles and responsibilities for all actors in the online context. We support this objective and are committed to work with the European Institutions to forge a **balanced framework** for a well-functioning online ecosystem.

Recently, there have been efforts around the world to develop regulatory frameworks for platforms. These have come in the form of EU platform-to-business regulations, content moderation efforts in Europe, the U.S., and Southeast Asia, and initiatives involving anti-piracy or anti-sex trafficking in the U.S.. Because of the complex and dynamic nature of platforms, setting comprehensive regulation is complex – this is why ITI encourages the EU to scope its initiatives on resolving proven market failures and gather robust stakeholder input to develop well-tailored solutions for specifically identified challenges. Under the previous European Commission, new regulations affecting platforms such as the platform-to-business Regulation and the Copyright Directive have been adopted. A careful review of the impact of these laws as they come into force will be critical in understanding which additional aspects need additional horizontal or sector specific regulatory approaches.

Our Recommendations

1. **Differentiating between illegal and harmful content is important.** Regulatory efforts should focus on illegal content as defined by existing laws governing the offline world. Harmful, but not illegal, content should continue to be addressed separately through voluntary or co-regulatory approaches. The decision as to whether content is harmful and /or should be removed is greatly influenced by regional or national cultural context, and assessments of what content is appropriate may vary based on company type or services provided. Policymakers should collaborate with companies to develop solutions that fit specific societal contexts through self-regulatory or co-regulatory approaches that promote trust between companies, policymakers and users, and support innovation.

2. **Content moderation should be led by digital economy players best suited to do so.** The digital economy allows consumers to increasingly benefit from fully integrated products and services, but it also creates complex relations between suppliers. Removal of content in such a complex system affects more than one business in the majority of cases. Any future initiative on content moderation should focus on the relevant activity and a company's interaction with content, identifying those

companies best placed to moderate content while relieving others whose role makes them ill-suited to do so.

3. **Types of platforms and services rather than size should matter.** A new regulatory approach should factor in the vast landscape of platforms, activities, interactions with users and user content, and technical capabilities. Any initiative should carefully define the scope to clarify what activities, rather than what companies, would be subject to the guidelines. It is important to consider where companies may have the ability to moderate content as opposed to merely technical control.
4. **Legal fragmentation in the European Single Market needs to be avoided.** National governments have surged ahead with legislative approaches to online content moderation (such as NetzDG in Germany). Further, new collaborative economy services struggle to set foot in many European markets, due to diverging national and at times even municipal rules. Legal fragmentation hinders the ability of start-ups to scale up and compete globally. Europe is well placed to lead discussions around challenges that policymakers, industry, and civil society need to address head on. A thoughtful approach should take account of existing legislation when identifying needs for horizontal or sector-specific approaches. Any reform of the ECD should take the opportunity to harmonise the horizontal aspects via a Regulation, to ensure the avoidance of fragmented national approaches.
5. **Update the ECD to reflect new business models.** There are countless types of digital platforms, and definitions in the ECD could be updated to reflect this new, constantly changing landscape. A new approach to the current active and passive host differentiation could provide additional legal certainty needed to promote innovation. The transition between active and passive hosting can also change over the course of businesses' lifespan. Potential new legislation should take into account the difference between various business models and the degree of knowledge or control a service has over the content. Online service providers who act as a mere conduit, caching or hosting service like cloud infrastructure would have different responsibilities from more specific applications that involved those services, such as social media, online marketplaces, or sharing economy services for example, given the different degrees of involvement in the activities concerned. A more principle-based approach would provide the needed flexibility to better determine a company's role in content moderation. Similarly, activities such as actively taking down content that is either harmful or illegal, should be incentivised through provisions such as a 'Good Samaritan' clause, that protects and supports work that companies are doing to advance online safety.
6. **The Commission should retain proven instruments under the ECD**. Notably, the country-of-origin principle ensures that providers of online services are subject to the law of the Member State in which they are established. This is a fundamental principle that has helped spur the uptake of online services by reducing regulatory barriers and addressing fragmentation. Efficient notice and takedown (N&T) processes are further key to advancing this debate. We strongly urge policymakers to retain these key principles in the upcoming legislative overhaul.
7. **Intermediary liability needs to be clear, stimulate innovation and protect citizens.** The liability regime is central to the effectiveness of the legal framework. Yet questions around the existing liability regime for internet intermediaries are creating uncertainty. Attempts to advance technological solutions to facilitate content moderation online could be developed at a faster pace than they are currently. A roadblock here is uncertainty about the interplay between proactive monitoring and intermediary liability. Tackling the proliferation of illegal content must be a shared responsibility of the entire eco-system (e.g. platforms, authorities, users on- and offline) including ensuring an effective N&T process is equally important. Whilst platforms have the responsibility to make N&T processes efficient, accessible and transparent, notifiers must be willing and able to use the tools

provided responsibly. Frivolous, unsubstantiated or vague notices are counterproductive, and the framework should not incentive these behaviors.

8. **User trust is central to the interests of our members and drives industry commitments to address content issues.** Our members want to maintain trustful relations with all of their stakeholders. In order to do so, Internet companies have an interest in providing information to users and governments in a transparent manner regarding their content moderation tools and measures. However, consideration of potential reporting obligations should take into account the significant burden on the companies of all sizes involved. Existing self-regulatory and co-regulatory efforts and memoranda of understanding have shown success and should be part of the ongoing dialogue between Internet companies and policymakers.

9. **The EU can play a central role for global policy leadership on content moderation.** Moving beyond the EU level, we also observe a heightened risk of fragmentation at global level that we need to address and avoid. The EU is in a prime position to inspire other jurisdictions and their approaches towards regulating content and setting up intermediary liability protections. This is an area where global regulatory convergence would make sense, as it would help protect citizens around the world more evenly, while allowing companies to deploy consistent actions addressing these challenges worldwide. As the EU debate moves ahead, it should aspire to lead a global-by-design approach, taking into account the importance of the final result to attract international convergence.

Competition

Free competition focusing on consumer welfare is key to promote innovation

ITI strongly supports free and undistorted competition as key to promoting innovation and consumer welfare. The tech community is committed to addressing challenges arising from technological change globally and in the EU. Europe is a leader in several segments of the technology industry, such as app development, which creates revenues in the EU for about a third of the global market.

Consumers' trust in market rules and players is crucial. Companies are providing more and more relevant and innovative products and services at lower prices, thereby increasing consumer welfare. Big data and AI applications generate substantial efficiency gains that are passed on to consumers. By reducing entry barriers and making it easier for small suppliers to reach new customers, innovative technologies and businesses benefit consumers by increasing competition and creating new services, augment human capability and enable advances in education, healthcare, mobility, sustainability, and many economic efficiencies in innumerable fields. By doing so, they offer major opportunities to start-ups and SMEs, who can grow more and faster than they would otherwise do, underpinning future European prosperity.

Grasping differences in business models and user interaction across **digital platforms** is key to gauging potential non-competitive conduct and properly addressing any challenges. As business models and applications change rapidly, regulation should not create artificial boundaries that may stifle innovation and the creation of new businesses. Artificially constraining the size of a company or network may appear to increase competition, but it could also reduce consumer welfare. Policymakers should consider how to ensure that new market entrants are able to succeed, while not imposing rigid rules that disrupt the consumer experience or value that they receive from a platform. Strong **network effects** may disincentivize switching platforms and impact choice and competition. Whilst network effects may be offset by multi-homing and increased competition across platforms, they can be reinforced by lack of interoperability or gatekeeper applications. These factors should be considered, but only together with others like a company's conduct and market behaviour.

Proportionate instruments that ensure a consistent policy approach and fair competition should be considered wherever necessary. Consideration of issues related to switching, access to data and portability would necessarily have to **focus on the specific data concerned**, and the available alternatives. It would be difficult to enact a one-size-fits-all approach to these issues across all types of situations.

There are discussions on several significant potential changes to EU and national competition laws, including concepts such as **transcendence** (declaring a company as being of paramount significance for competition across markets and subjecting it to specific obligations); or broadening the **essential facility** concept, e.g. as regards access to data; extending concepts of **relative/significant market power** to intermediaries; or still introducing an **intermediation power** criterion, broadening the notion of dominance by looking at how significant an intermediary's services are for access to supply and sales markets, and whether sufficient and reasonable alternatives exist. Some of the above ideas would constitute a major shift from the current setting - when considering them, it is paramount to avoid undue discrimination against specific business models and account for the positive impacts of intermediaries. Consideration of these ideas should be based on rigorous application across sectors so that any potential benefits (e.g. wider access to data) spread across society. One should also take into account other rules (like the P2B regulation), parallel regulatory initiatives that are meant to address similar concerns (e.g. the announced data act), and finally the limitation posed by applicable, conflicting provisions such as GDPR.

Our Recommendations

1. **The EU should lead an international dialogue.** Given the intersection between competition and other policies in an increasingly digitalised global economy, international dialogue is needed on these policies, focusing on the complementarity between competition, consumer welfare and innovation.

2. **Competition enforcement should be separate from other policy issues.** The boundaries between **privacy and competition** enforcement must remain clear – antitrust rules ensure that markets function well, whilst data protection laws address privacy concerns. This will help ensure that both objectives are met, and avoid the risk of assessing data protection through the prism of market power or similar competition law constructs that are extraneous to privacy. Conversely, privacy and security are becoming a competitive element in their own right. Raising consumer awareness and making switching across competing applications easier, e.g. by allowing them to port their data while ensuring it does not lead to additional security risks, will encourage competition in providing services featuring greater privacy protections, thereby lowering the cost for more secure and privacy-friendly products.

3. **Consumer welfare should drive competition policy.** While the EU competition law framework is sufficiently flexible to address new challenges, the underlying principles for the debate on its future should be **interoperability**, **transparency**, **non-discrimination** and consumer **choice**, ensuring at the same time the protection of IP rights and avoiding hurdles for innovation. Regulators should in particular focus on **consumer welfare**, not on protecting competitors.

4. **Competitive dynamics need close assessment.** Market definitions should better reflect competitive dynamics, and recognise that digital platforms compete globally. Deeper analysis of **network effects** is needed – markets will not necessarily be less competitive or less innovative, as medium and smaller platforms continue to help customers reach a wide range of goods and services. Competitive dynamics across platforms offering different core services to the same customers should also be assessed.

5. **Company conduct matters.** Data should be assessed under competition law as any other asset that companies compete with in the market but taking into account how it differs from other assets due to its non-exclusive nature. Enforcement should focus on a company's conduct and not on structural issues, like the amount of data a company holds, or its size. Policymakers should particularly consider potential unintended consequences of an unduly strict approach to big data, avoiding new rules for every new product or business model, which might stifle more innovative or effective models. This is particularly true for **AI applications** – as these vary widely, policymakers should recognize the importance of sector/application-specific approaches; one approach will not fit all AI applications.

6. **Data portability should not be dealt with in a one-size-fits-all approach.** Consideration of issues related to **switching, access to data and portability** should take into account the data at play, the operator concerned and available alternatives. Every case should be assessed on its own merits, avoiding a one-size-fits-all approach. In order to increase competition in the markets and avoid lock-in effects and switching barriers, portability of data should be enhanced, provided this does not affect IP and trade secrets. Imposing rigid standards to enable data portability could however have unintended consequences, hardwiring the status quo, forestalling innovation and precluding future portability.

7. **Considering platforms' enabling capacities for consumers and other businesses.** As the notion of **platform** refers to very different models, policymakers should consider the role that specific platforms play in the markets they operate, the value they create, their relationship to customers and competitors, and the possible alternatives – ensuring markets remain open to innovative challengers, and keeping consumer welfare and economic efficiency as final objectives.

2 March 2020

Sustainability

The technology industry supports Europe's climate ambitions and urges for industry-led, collaborative policies

In its December 2019 Communication 'The European Green Deal', the European Commission has outlined its ambition to become the first climate-neutral continent by 2050. With this strong commitment, the European Commission is viewing different industrial sectors and assessing them for their energy performance.

While tech is a fundamental enabler for achieving society's sustainability goals, our industry also has an important direct role to play in the green transition, and many companies are already taking action and committing to ambitious goals related to their respective activities. The technology industry is for example developing ways to efficiently handle rapidly growing data volumes from data storage to data flows to data analytics. Further, the transition to 5G will catalyse energy efficient solutions across all industry sectors, thereby reducing carbon emissions.

Our Recommendations

1. **Digital technologies are recognised as a crucial means to achieve the transition towards a climate-friendly Europe.** Our industry embraces this important role wholeheartedly and stands ready to support the Commission's efforts. We encourage greater investment in and use of technologies that can help facilitate the green transition in order to for example better manage the electricity grid or save energy via smarter management of freight.

2. **Mandating a certain charging technology would risk innovation and thereby limit consumer welfare while not leading to significant waste reduction.** Ideas to mandate a common charger have been much debated in Europe. While we applaud the goal of reducing electronic waste while increasing consumer convenience, we do not believe that mandating a certain technology would be the right way to achieve this goal or promote innovation. The marketplace has shifted significantly since debate on this topic began: in 2009, there were thirty different mobile chargers on the market, now there are three (USB-C, micro USB, and lightning). The European Commission has noted in the past that mandating the use of a specific technology would have ultimately been counterproductive in fostering this convergence. E-waste and consumer convenience have been cited as key components of any voluntary or regulatory approach to a common charger. We share these priorities, and encourage EU policymakers to carefully consider how any solution might actually achieve these goals. We favor a fact-based approach that fosters innovation and continued interoperability in the market. We look forward to the publication of the Commission's impact assessment, and encourage the Commission to decide on the most suitable approach based on the available evidence.

3. **Repairability should not come at the expense of product quality.** One of the key areas of focus for the new European Commission will be advancing **repairability, recyclability and reuse of electronic products** with a view to increasing product lifespans and enabling certified third-party repairs. Our industry has long been pursuing these objectives, has advanced professional repairability of electronic products and believes in the need of appropriate repair strategies. While we stand ready to support these efforts, repairability should not come at the expense of ensuring product longevity through (build) quality and durability. We encourage a balanced approach that considers all the needs of the customer including function, durability, safety, and security. We stand ready to jointly explore with the Commission how design requirements, e.g. on component accessibility, can strike the right balance without having unintended negative design or durability impacts.

4. **Data centers are a key vehicle for energy-efficient data storage.** Data centers enable the most innovative companies in the world to store their data, compute it, execute and deliver services. Tremendous energy efficiency gains have been made by the transition from local data storage within companies to outsourcing of data storage to trusted providers. A whole new industry has emerged from this need of the technology industry in the past decades. Data centers are working hard to meet growing demands for storage space while using state-of-the art technology to support energy-efficient handling of data for the benefit of the environment but also to meet economic considerations. The previous European Commission has implemented ambitious mandatory standards for server energy efficiency (Commission Regulation 2019/424), which are taking effect on 1 March 2020. We seek to embark on a path of positive collaboration with stakeholders in the European institutions moving forward.

5. **The transition to a circular economy requires a harmonised approach at EU level**, where all Member States abide by the same rules and enable a more sustainable Single Market for digital products and services. While we understand the ambitions, some countries may have to go further than EU law and adopt more restrictive measures, we would favor an EU-level regulatory framework based on sound scientific analysis and justified regulation. This would avoid risks of creating barriers to trade and fragmenting the EU's Single Market, and it would bring all EU countries to a higher environmental standard.

Member Companies

ITI

accenture
High performance. Delivered.

Adobe

Akamai

amazon

AMD

ANALOG DEVICES

AUTODESK.

Canon

Cognizant

CORNING

Dropbox

ebay

EQUINIX

ERICSSON

EY

facebook

FUJITSU

Google

Hewlett Packard Enterprise

Honeywell
THE POWER OF CONNECTED

hp

IBM

intel

intuit

IRON MOUNTAIN

JUNIPer
NETWORKS

KEYSIGHT
TECHNOLOGIES

Lenovo

Lexmark

logitech

mastercard

McAfee

Microsoft

MOTOROLA
SOLUTIONS

NCR

NetApp

nielsen

ORACLE

paloalto
NETWORKS

pwc

QUALCOMM

RAPID7

Red Hat

Sabre

salesforce

SAMSUNG

SAP

Schneider Electric

servicenow

Snap Inc.

SoftBank
Group International

SWIFT

SYNOPSYS

TATA
TATA CONSULTANCY SERVICES

tenable

teradata.

Texas Instruments

TOSHIBA
Leading Innovation >>>

TOYOTA

tsmc

twilio

VERISIGN

verizon media

VISA

vmware

xerox

zt Systems