ITI's 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 around the world for the technology industry. ITI's membership is comprised of more than 60 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 and healthcare to energy and transportation – to leverage frontier innovations towards competition and success in the global marketplace. Whether it is an internet connection that opens new business opportunities for rural communities, sensors that detect health and safety hazards for workers in real time, or artificial intelligence that allows doctors to analyze complex medical data faster than ever, technology allows us to address some of the most challenging societal issues of our time and improve the quality of everyday life for Europeans. The tech sector is also already taking significant steps – likely more than any other sector – to help prepare the workforce of the future for the shifting skills and competencies that are required in the 21st century.

Tech policy will remain a crucial priority in the 2019-2024 EU term. Europe has an opportunity to take an international leadership role on policy issues that are increasingly global. ITI and its members share the firm belief that building trust and fostering the public interest in the era of digital disruption are essential. As such, 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 democratic values that underpin European society. We also strongly believe in the importance for policy-makers to preserve an enabling environment for innovation to ensure Europe's global competitiveness and security.

With both of these critical yet complementary objectives in mind, ITI has developed recommendations outlining concrete steps that policymakers can take, in partnership with industry, academia, civil society, and other stakeholders, to advance a compelling European tech agenda for the 21st century. Our specific recommendations, which can be found on the subsequent pages of this document, address the economic and social implications of technology and the role of our industry, in a manner that supports innovation, while recognizing the very real public interests at stake. They focus on the following key policy areas:

- Global convergence on Artificial Intelligence – page 2;
- Interoperable privacy rules – page 4;
- Global cyber and supply chain security – page 6;
- Governance of non-personal data – page 8;
- Digital trade and data flows – page 10;
- The international tax system – page 12;
- An innovation-friendly framework for internet intermediaries – page 14; and
- Competition policy and digitalisation – page 16

ITI Recommendations for Artificial Intelligence

Global Convergence on AI policy will benefit the people, society and the economy of Europe

Artificial Intelligence (AI) is a suite of technologies capable of learning, reasoning, adapting, and performing tasks in ways inspired by the human mind. We are already experiencing the benefits of AI in an array of fields. Startups, SMEs, and larger tech companies have all developed AI systems to help solve some of society's most pressing problems. Many others are using AI to improve their business, provide better public services and advance ground-breaking research. The AI ecosystem is global and multifaceted. ITI supports the EU's multi-stakeholder engagement approach to AI and encourages the EU to bolster its global engagement on AI policy to ensure it is prospering for the benefit of our societies.

AI developers and other stakeholders innovate across industries to find solutions that will meet the needs of individuals and society in unprecedented ways. By leveraging large datasets, increased computing power and ingenuity, AI-driven medical diagnostics can alert doctors to early warning signs to more capably treat patients. AI-enabled sports evaluations are able to make personalized training recommendations to players. Increasingly intelligent systems are capable of monitor large volumes of financial transactions to more efficiently identify fraud. SMEs can gather new insights and improve their business by using AI and data analytics made available to them through cloud services.

While the potential benefits of AI development are enormous, it is impossible to fully predict the future impact. Stakeholders globally are aware and addressing the main challenges. For instance, they recognize they must find ways to mitigate bias, inequity, and other potential harms in automated decision-making systems. Further, while AI's full impact on jobs –either in creation or displacement– is not yet clear, preparing the EU's future workforce to adapt to rapid technological change is critical. The tech industry shares the goal of responsible AI use and development. As technology evolves, we take seriously our responsibility as enablers of an AI world, including seeking solutions to address potential negative externalities and helping to train the workforce of the future.

Our Recommendations

AI remains an active area of research. The technology is constantly evolving and improving, as are the tools to address some of the challenges around explainability, bias, and fairness. The best way for the EU to maximize the development of AI within Europe and the value of its digital assets in such a dynamic environment is by leveraging public-private cooperation and making progress in the following areas:

1. Prioritise Europe's competitiveness as a way to weigh in with its values and principles in the global AI race. As AI is not developed in regional siloes, the EU should move away from an 'AI made in Europe' narrative, which contradicts the global perspective the European Commission has endorsed. Many AI products and services are the combination of European and non-European elements developed in different locations. The most reliable way for Europe to ensure trustworthy AI for its citizens is to ensure its approach to innovative technologies like AI fosters its global competitiveness and allows Europe the opportunity to shape the global debate on AI governance.

2. Engage in promoting international responsible and ethical AI practices. AI presents great opportunities for society in a variety of different fields. It also raises valid concerns around responsible and safe development and use. As leaders in the AI field, ITI members recognize their important role in making sure technology is built and applied for the benefit of everyone. We support the EU's focus on embedding ethical aspects in the approach to AI. The EU should aim to promote the ethical development and use of AI *globally* via collaboration with its international partners to promote a shared understanding and common norms, and a dialogue with other geographies when it comes to responsible development. In particular, the following aspects need to be taken into consideration:

- The approaches must be context- and risk-specific, and a multi-stakeholder approach is required to identify solutions that work for all actors involved;
- Technology and research can help address some of the challenges (e.g. fairness and interpretability);
- As the AI ecosystem is global, the most effective debate goes beyond national borders. Pitting Europe against other geographies will not help local players harvest the potential of technology to the fullest;
- As many promising uses of AI rely on personal data, responsible use of data is key. AI use will have to respect existing laws around data protection and privacy, such as the GDPR. In addition, it is important for developers, users, and regulators to incorporate privacy considerations in their approach to the technology. Key principles of responsible personal data use in the AI context are: *Transparency*, *Privacy-by-Design*, *Risk Assessment and Mitigation*, and *Redress*.

3. Prioritise an effective and balanced liability regime. EU policymakers recognise the clarification of rules around liability as a subsequently important area of focus. We encourage the Commission to continue the engagement with multi-stakeholder expert groups. The right solution can only come from an open exchange with all actors in the chain. We believe in many cases the current regime will be easily applied in an AI context. However, there might be cases where rules will have to be amended. We support a framework that adequately compensates victims for damages and provides a clear path for redress. Such framework will have to take into account the legal and technical specificity of different use cases. As with AI in general, context is key to identify the right policies. Industry is committed to partnering with relevant stakeholders to develop a reasonable accountability framework.

4. Consider supporting international, technology neutral, industry-led standardisation. As governments and industry are considering the best path forward regarding laws, regulations, and policy for AI, the role of standardisation is a key factor that can help form a bridge between written rules and practical implementations. However, no horizontal standard can reasonably cover the technology as a whole. Standards would need to be specific to different sectors and use cases. With rapid technological change, overreliance on a set of fixed standards will prevent innovative solutions from entering the market. Any AI-related policy considerations adopt the long-standing principles of voluntary, industry-led standardisation, and consensus-based international standards.

Appropriate development of AI standards – *standards should*:

- Establish global consensus around technical aspects, management, and governance; frame concepts and recommended practices to establish trustworthiness of AI inclusive of privacy, cybersecurity, safety, reliability, and interpretability; be sector and application-specific when used for AI evaluation.
- Enable non-discriminatory market access, reduce barriers to market entry, spur innovation to the benefit of society, and be performance-based when enabling technical interoperability.
- Work for the net benefit of the international community and be applicable without prejudice to cultural norms, without imposing the culture of any one nation in evaluating the outcomes/use of AI.

Inappropriate development of AI standards – *standards should not*:

- Establish barriers to trade, be designed to only advance industries or objectives of a single nation or bloc; or be used to replace the development or update of national regulations applicable to AI.
- Limit the pace of AI innovation.

ITI Recommendations on Interoperable Privacy Rules

Privacy is crucial to consumer and enterprise trust which is key to innovation

ITI prioritizes the goal of protecting the privacy of our consumers and enterprise users, and our interests are fundamentally aligned with the EU institutions in this area. Since our members are global companies with complex supply chains around the world, we understand the importance of individuals being able to rely on a uniform and consistent set of privacy protections principles no matter where their data is located.

Europe has developed an extensive framework for privacy and the General Data Protection Regulation is having a global impact on many governments' efforts to update their own privacy legislations and enable their businesses to trade more easily with European markets. These developments will help foster the trust of consumers and businesses in digital products and services critical to the adoption of new technology in the EU. The implementation of the data protection framework should focus on deep harmonisation within the EU, and flexibility to take into account the ongoing tech evolution, allowing the EU to meet the needs of individuals, businesses, and society and innovate across many industries in unprecedented ways, from revolutionising the delivery of healthcare to facilitating a new wave of modern conveniences while ensuring privacy rights are safeguarded.

Consumer trust in market rules and market players is crucial. Ensuring consumers' access to and control over their personal data is key to ensure their trust that data will be used in a transparent manner, leading to increasing consumer welfare in the form of better, more relevant and innovative products and services, at lower prices or free of charge. In this manner, strong privacy protections are not in opposition to innovation; in fact, robust privacy rules, combined with strengthened data governance can jumpstart innovation. Among a wide scope of uses, 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. The right privacy and data protection safeguards can maximize 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 coherent principles on data protection globally mean people have more control over their personal data and our businesses can benefit from increasing levels of confidence and trust.

As business models and applications change rapidly, it is important to avoid creating artificial boundaries, inflexible and overly prescriptive regulation or excessive compliance burdens that may stifle innovation, undermine the development of new growth-enhancing businesses, 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, recognizing the benefits of techniques and controls that obstruct reidentification and better enable valuable research and innovation in areas that rely on the use of data 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 otherwise deter innovation and SMEs' participation in the digitally-enabled economy. In an effort to better inform the ongoing privacy discussion , 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. This effort continues as we work with governments to advance robust privacy norms globally.

Our Recommendations

- We encourage the EU to emphasise the importance of **global collaboration and to promote interoperability between regional mechanisms** for international data transfers. The General Data Protection Regulation's Article 42 provisions on recognizing and approving certifications creates the perfect opportunity to identify commonalities between the approaches of the EU and other regions of the world, particularly the Asia-Pacific, by exploring potential interoperability through certifications pursuant to GDPR Article 42 and APEC CBPRs.
- Our companies have embraced the **GDPR** as a significant milestone in safeguarding privacy and trust the EU will ensure consistent application across member states, along with clarity for regulators, businesses, and individuals by checking its interaction with other rules. Moving towards the GDPR's first year, the EU should also assess its impact on consumers' trust, companies' behavior, quantity/impact of infringements, and on the economy.
- We urge the EU to continue to encourage global partners to commit to ongoing dialogue in official forums related to **international transfer mechanisms**, while providing robust and future-proof mechanisms for data transfers. We stand ready to support these efforts towards promoting greater interoperability in privacy rules and data flows globally.
- There can be no privacy without security. The EU has a great track record in this area, and we hope that **critical cybersecurity and other beneficial activities be encouraged** as part of any efforts to improve privacy protections, including by recognizing security as a legitimate interest for processing personal data in the e-Privacy regulation.
- Governments around the world are increasingly looking 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, and South Korea – to deter them from data localisation** and encourage international cooperation that will help identify solutions to balance privacy, security, and economic growth.
- Furthermore, we encourage the EU to **work on law enforcement cooperation multilaterally or bilaterally in an effort to establish efficient mechanisms and protocols for threat information sharing and data access requests**. The U.S. CLOUD Act is one such mechanism to facilitate bilateral cooperation between the EU and the U.S. in this space. The EU should also be cognizant that its approach to government access to data will set an important international precedent that could impact individual privacy rights globally. It is essential for the EU and its Member States to adopt internal practices that it would welcome being replicated by third countries, which could have substantially different rule-of-law and fundamental rights safeguards.

ITI Recommendations on Data Governance

Access to quality non-personal data sets is key to innovation

ITI companies recognize that digital innovation in the modern age will rely on the availability of large datasets from the private and the public sectors, enabling technology developers to innovate across many industries and meet the needs of individuals and society in unprecedented ways. For example, by analyzing data and producing customized recommendations based on learning from a large pool of similar cases, the EU can revolutionize the delivery of healthcare and facilitate a new wave of personalized modern conveniences for its citizens. Much of this functionality will be built upon insights gleaned from non-personal data sets – that is, data which is anonymized or not directly relatable to a specific individual.

To realise this potential, it will be critical to ensure that technology developers are able to access high quality public data sets. **The EU has started off on strong footing to make this a reality by setting up its EU Open Data Portal in 2012.** Allowing business 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. Between 2016 and 2020, the market size of Open Data is expected to increase by 36.9% to a value of 75.7 billion EUR.[1]

In addition, open data can be used to help transform businesses across industry sectors from within as they embrace the digital world. We 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

- We suggest the EU continue to catalyze the growth of the economy through digital transformation **by publishing open data under an open license and encourage it to apply an ‘open by default’ principle**.

- **As business models and applications change rapidly, it is important to avoid creating artificial boundaries**, inflexible and overly prescriptive regulation, or excessive compliance burdens that may stifle innovation or undermine the discovery of new growth-enhancing insights. Businesses rely on their ability to operate globally and transfer data across borders. The EU has been forward thinking in this regard in passing its free flow of non-personal data regulation. Future EU policies should continue to encourage innovation by recognizing the benefits of techniques and controls that better enable valuable research and innovation in areas such as machine learning and AI that rely on the use of data.

- Data localisation requirements run converse to the above motivations, so we suggest the EU make efforts to continue to discourage such policies at the member state level and to **vigorously**

[1] http://thegovlab.org/open-data-index-2018-edition/

enforce its recently adopted EU-wide free flow of data regulation and prohibit data localisation measures other than for clearly defined national security exceptions.

- Similarly, as governments around the world are increasingly looking to enact data localization 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, and South Korea – to deter them from data localization** and encourage international cooperation that will help identify solutions to balance privacy, security and economic growth and help facilitate the ready access to more high quality public data.

- It will be critical in the coming years that the EU **facilitate a robust government data access and data sharing environment.** Many AI research fields and practical applications require high-quality training data. Sharing and making more data available would enable better training of AI algorithms, and the EU could maximize the development of AI within Europe and the value of its digital assets by allowing free access to machine-learning friendly datasets for R&D purposes, provided it is done in a way that sufficiently protects privacy and security.

- We urge the EU to **create opportunities to collect and distribute data responsibly and broker more data-sharing agreements, invest in AI 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 should also continue to **facilitate the removal of other barriers to widespread open data use**. These barriers include lack of awareness, lack of knowledge, poor data quality, and licensing barriers.

- We urge the EU to continue to 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.

ITI Recommendations on Global Cyber and Supply Chain Security

Policy Must Reflect a Shared Responsibility and the Changing Nature of Cyberspace

ITI's members are global companies with complex supply chains around the world, including both producers and users of cybersecurity products and services. We support the EU's continuous work with its international partners to strengthen cybersecurity globally.

Cybersecurity is integral to the EU's modern economy and competitiveness. While cyberspace holds great benefits for society, it also presents opportunities for misuse and exploitation. Cybersecurity concerns hinder innovation and growth, and digital disruptions can threaten national security, businesses, and individuals. Increasingly sophisticated adversaries target European governments, organisations, and citizens, and hit the **global supply chains** of essential products in the EU's digital infrastructure. While 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.

In the world of digital transformation, the full potential of the modern economy cannot be realised without cybersecurity. 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 DSM), but also Europe's democracies, freedoms, and values. The tech industry interests and goal of improving cybersecurity are fundamentally aligned with 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. 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. Government policy is key to encouraging proper use of tools and best practices by stakeholders. These tools and approaches must be manageable and interoperable – too many silos can create a risk of oversight of 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, normally due to misconceptions about improving security or access to data, some governments are also forcing data localisation, 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 and other tools providing a common language to better help organizations comprehend, communicate, and manage cybersecurity risks (such as the U.S. NIST Framework).

The EU Cyber Security Act's certification framework should be implemented in a way that is adaptive, risk-based, and benefits industry for its flexibility and utility. Any approach should recognize that not all organisations are alike – in size, scope, complexity, business, cyber-risk or sophistication. The EU should continue promoting existing international standards for developing certification schemes, and continue supporting countries in the region to develop cybersecurity expertise and capacity. Cyber hygiene and best practices (e.g. patching, network microsegmentation, multifactor authentication) are also key.

Also, we urge the EU to engage closely with international partners – particularly China, Vietnam, Indonesia, and South Korea – to deter them from data localisation and encourage international cooperation that will help identify solutions to balance security and economic growth. Furthermore, we encourage governments to work on law enforcement cooperation multilaterally or bilaterally to establish efficient mechanisms and protocols for threat information sharing and data access requests.

2) Develop a multi-stakeholder, public-private approach to cybersecurity standards and policies. Cybersecurity is a shared responsibility – neither governments nor companies can address it alone. The private sector owns and operates elements of critical infrastructure that are targeted by malicious cyber activities. Those owners and operators should be viewed as partners in ensuring the protection of this critical infrastructure. The ICT community has been foundational in developing the infrastructure of cyberspace. It has also provided leadership, innovation, and stewardship in all aspects of cybersecurity for nearly two decades. Increasingly, companies in all sectors are investing in cybersecurity and want to contribute to public-private partnerships, which have proven to be an effective approach to tackle cybersecurity challenges as they enable targeted resource investment, shared technical expertise, and the identification of appropriate policy solutions.

As many countries launch multi-stakeholder initiatives to address cybersecurity vulnerabilities with different sectors, such as IT, finance and telecoms, we recommend the EU also seek active participation of the private sector in order to direct its resources where cyber risk is most critical and imminent, as well as facilitate a mechanism to deal with the complex nature of global cybersecurity challenges.

3) Address supply-chain security collaboratively. The EU is increasingly concerned about supply chain security and wants assurances on the integrity of the ICT products for their citizens. The manufacturing of ICT products and the development of cloud services rely on numerous enterprises in the supply chain that can span multiple countries, creating a bounty of sabotage opportunities that can compromise security. As the EU is moving towards 5G and supply chain security becomes more important, it should consider:

- Setting baseline security requirements in the supply chain, encompassing risks in both product and service-oriented suppliers.
- Develop incentives to encourage ICT vendors, including in 5G and consumer and industrial IoT, to adopt supply chain and cyber-hygiene best practices, including transparency in how organizations manage supply chain risks.
- Establish public-private partnerships to identify public policies that incentivise companies to adopt identified best practices. Governments must involve industry to ensure workable and effective initiatives to mitigate supply chain risks.

4) Advance policies to recognise the growing complexity of emerging technologies. Cybersecurity risks have intensified as the world's digital infrastructure has become increasingly interconnected from major technological shifts like cloud, IoT, AI, and 5G. To realize the tremendous promise and digital transformation these technologies represent, 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, along with participate in the development of global, voluntary, and consensus-based standards and best practices.

ITI Recommendations on Tax

Ensuring a strong, functioning and dependable international tax system

ITI advocates for policies that promote innovation, open access to new and emerging markets, enhance trust in technology, and foster increased global growth. International tax policy is a key factor in this regard and a focus of jurisdictions around the world. The tech sector is a critical and constructive voice in conversations about cross-border taxation, particularly on efforts to ring-fence digital business for tax purposes.

ITI and its members have long engaged in dialogue in capitals and multilateral bodies such as the Organisation for Economic Development and Cooperation (**OECD**), educating policymakers about business models and discussing how proposed policies impact companies, with the primary purpose of strengthening a functioning international taxation system.

The last decade has seen a fundamental shift in the way companies of all industries operate globally, relying on a vast array of digital technologies to produce, export, market, and sell goods and services. Our members' products and services drive growth and job creation in virtually every sector of the economy, allowing manufacturers, automakers, energy firms, construction firms, and other EU industries to be more competitive, at home and abroad. Tax is a priority issue for our members and our top goal is ensuring a strong, functioning and dependable international tax system.

These efforts have intensified in recent years. Driven by concerns about insufficient or "unfair" taxation, and allocation of tax revenues across countries, jurisdictions are looking to modernize tax rules. In the European Union, a number member states, under the leadership of the large economies, have expressed concern about the profit allocation related to digital activity across the E.U. Spurred by arguments around tax fairness, key economies are pushing for new policies to create greater tax nexus around digital business. These proposals range from short term digital services taxes to long term changes to foundational tax principals like the **permanent establishment** (PE) concept.

Similar efforts are underway in Latin America and the Asia-Pacific. In each of these regions, we have seen governments from Chile to Australia contemplate digital-oriented proposals, including digital services taxes.

This interest is also reflected in ongoing discussions at the OECD. Beginning with the Base Erosion and Profit-Shifting (**BEPS**) project in 2013, major economies have been at work to address comprehensively a number of tax policy issues. Many reforms have resulted from the OECD BEPS process. As referenced above, the effort culminated in an agreed-upon package of fifteen separate work streams, or Actions. More than 115 jurisdictions have contributed to the BEPS "Inclusive Framework" and committed to its implementation. This concerted multilateral initiative represents the first significant reform of global tax standards in nearly a century including limitations to interest deductibility, anti-hybrid rules, CFC rule reform and country-by-country reporting of key tax information. We hope for continued success from the multilateral process.

While most of that work was finalized in 2016, work on Action Item 1—*Addressing the Tax Challenges of the Digital Economy*—continues through 2020 when a final report is due. While the OECD has long recognized the **impossibility of ring-fencing digital activity** for tax purposes, it has also acknowledged legitimate concerns around proper profit allocation. Activity at the OECD will intensify in 2019 as countries look to find a global solution by 2020. In Paris, we anticipate a range of ideas to be under consideration, from continuing interest in digital-oriented ideas to global minimum tax standards.

Absent meaningful results at the OECD, some countries might continue to press for short-term, unilateral measures, specifically digital services taxes. Any approach to include only companies with significant levels of revenue and certain kinds of business models, could create potential violations of tax treaties and risk causing double taxation as economies strive to tax what is essentially the same economic activity.

Significant **reforms to cross-border tax policy** should be best contemplated and agreed to at the OECD, which will be a key venue for discussions around reforms to the international tax system in 2019 and 2020. The OECD is the optimal place for this discussion. We hope the high-level engagement and expertise rationalizes the conversation and leads to constructive policy outcomes that can be rolled out across Europe and beyond.

Our primary objective is to strengthen a functioning international tax system. ITI members rely on clear and established international tax rules to innovate and grow their operations. Unilateral, inconsistent policies that depart meaningfully from long-established rules are a direct threat to efficient global operations. ITI supports the multilateral conversation at the OECD as the best forum to grapple with the complex cross-border policy issues identified and discussed above.

Our Recommendations

- We encourage the EU and its Member States to rely on the OECD as the vehicle for contemplating and agreeing reforms to the international tax system. Any reforms should be comprehensive income tax-based that apply to all sectors of the economy, remain compliant with Tax Treaties, and include appropriate dispute resolutions.

- The European Union and individual Countries should avoid discriminatory, unilateral policies. Many of the proposals under consideration are discriminatory in their current form, raising trade policy concerns while creating a precedent for potential taxes affecting a broad range of data-related activities.

- A patchwork of inconsistent policies is bad for economic growth and innovation. With different countries contemplating taxes with divergent bases and rates, companies face the possibility of similar but distinctly different policies across multiple jurisdictions. Further, given the fairly limited revenue estimates of the digital services tax proposals contemplated thus far, we remain concerned individual countries will purpose broader based taxes and/ or higher rates.

- It is essential to include the broader global business community. Policies under contemplation will create equities for all multinational businesses across economic sectors and geographies.

ITI Recommendations for Trade

Promoting 21st Century Commitments for Europe and the Global Economy

ITI is committed to innovation, creative problem solving, and close consultation with governments. The last decade has seen a fundamental shift in the way global trade is conducted. **Globally competitive companies of all industries now rely on a vast array of digital technologies to produce, export, market, and sell goods and services**. Technology products and services drive growth and job creation in virtually every sector of the economy, allowing manufacturers, automakers, energy firms, construction firms, and other EU industries to be more competitive, at home and abroad. EU manufacturers of automobiles and aircraft depend on technology products and services to lower the cost of production and improve product performance and safety, and 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. For example, it is unclear to what extent current WTO rules protect a company's ability to move data across borders, and companies are often caught between conflicting national laws on a variety of digital issues. **Updated digital trade rules at the WTO and in future Free Trade Agreements (FTAs) would significantly alleviate current uncertainties** in the global trading system. Similarly, continued cooperative efforts to promote the fair and effective development and use of innovative technologies and address unfair practices in the global market are necessary steps in fostering a mutually advantageous trading system.

At the same time, the EU's continued efforts to deepen its trade and investment relationships with key trading partners provide important opportunities to **foster regulatory compatibility in areas of emerging technology**. Nowhere is this more important than in the transatlantic commercial relationship – the largest bilateral trade and investment relationship in the world. Through ongoing engagement, the EU and United States can reduce trade barriers to the benefit of entrepreneurs and consumers in both markets. They can also work to develop strong, compatible regulatory approaches that promote interoperability and adaptability, including through the use of international standards, to ensure that companies in the EU can maintain their innovative edge.

Global data flows have increased current global GDP by at least 10 percent, adding $7.8 trillion to the global economy in 2014 alone. While gains have accrued in large part to the world's most connected economies, **increasing flows of data have opened doors to countries of all sizes, small companies and start-ups, and billions of individuals**.

Protecting and enabling digital trade will allow companies of all sizes to continue to reach global customers, compete more effectively abroad, and create jobs and economic growth at home. In addition, protecting companies from forced source code disclosure abroad will allow EU companies to maintain the integrity of their innovative products and services while exporting to foreign markets with confidence.

The proliferation of data-driven products and services means that data – particularly personal data – must be protected from bad actors and misuse. The tech industry is committed to working with the EU to continually implement and enhance data protection while still facilitating innovation and economic growth. To this end, **strong trade commitments should enable the free flow of data, address forced data localisation requirements and forced disclosure of source code**, and enhance regulatory and enforcement cooperation, including in areas like cybersecurity, leading to stronger privacy protections and establishing a high-standard, practicable model for future trading partners.

Our Recommendations

- Work with industry and like-minded governments to craft a balanced approach to data flows in trade agreements that protects data and allows data to flow freely across borders. Trade agreements should not be used to regulate or circumscribe appropriate privacy or cybersecurity practices, but rather ought to contain narrowly tailored exceptions to digital trade provisions to allow participating countries to adequately protect data while preventing the imposition of measures that are discriminatory or more trade restrictive than necessary.

- Continue to work with industry and like-minded governments to address policies and practices of third countries (e.g., China, Vietnam, South Korea, India, Indonesia) that create unfair competitive conditions and hinder the development and use of innovative technologies, including inappropriate intermediary liability penalties, monitoring and filtering requirements, forced data localization measures, and other requirements to use local servers and software, rather than best available technology; in addition, engage directly with those third countries on trade-related issues through comments and trade diplomacy.

- Utilize the WTO E-Commerce Initiative to secure the strongest possible commitments without diminishing the ability of governments to address legitimate public policy concerns. These commitments include ensuring the free flow of data and prohibiting data localization; prohibiting the forced disclosure of source code, algorithms, and encryption keys; encouraging participants to join the WTO Information Technology Agreement (ITA), protecting intermediaries from liability for content they do not control, and simplifying and expediting customs clearance procedures. The EU should continue to lead in seeking a permanent moratorium on taxes and tariffs on digital products and data flows.

- Pursue strong digital trade chapters in FTA negotiations that recognize the importance of digital technologies in global trade, intensify international regulatory cooperation in digital policies such as cybersecurity and privacy, and secure the same commitments recommended for the WTO E-Commerce Initiative.

- Continue to advance the Better Regulation agenda with a view toward increasing regulatory transparency, improving WTO notification practices and decreasing the emergence of technical barriers to trade.

- Through political prioritization and continued intergovernmental cooperation, 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, helping economies to grow and preventing the risk of trade disputes.

ITI Recommendations on Platform Policies

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

Online platforms and intermediaries have played an incredible role in driving innovation and growth in the economy, creating market opportunities and access for businesses of all sizes. While there is no common, clear-cut understanding of the concept of online platforms or intermediaries, the notion is generally used to indicate different multi-sided marketplaces or services, such as search engines, social networks, and e-commerce marketplaces, among others. The concept can take a very different meaning in B2C or B2B applications.

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 relations, content moderation efforts in the U.S., EU, and Southeast Asia, anti-piracy or anti-sex trafficking in the U.S., competition in the U.S. and EU, and financial regulations in Southeast Europe. Because of the complex and dynamic nature of platforms and intermediaries, it is hard to set a comprehensive regulation. Instead, ITI encourages governments to narrowly focus their regulatory aims to resolving proven market failures.

Internet services have transformed trade and enabled SMEs to reach global audiences in ways never possible in the past. A fundamental reason that services have been able to play this role is their open nature: online platforms and intermediaries can facilitate transactions and communications among millions of businesses and consumers, enabling buyers and sellers to connect directly on a global basis. This model works because intermediaries can host these transactions without being held liable for the vast amounts of content surrounding each transaction or interaction.

Platforms play a beneficial role as engines of the digital marketplace, not least by facilitating information and communication and helping match offer and demand in the Digital Single Market as well as globally. Platforms make it easier for consumers to buy online, compare products and their prices, learn from other consumers' experiences. In e-commerce, platforms are one of the main channels for cross-border transactions, allowing SMEs to compete beyond their national market and grow more, or more rapidly, than they would without an online intermediary. Consumers greatly benefit from the resulting increase in competition, variety, and offer. As the European Commission stressed, they play a prominent role in the creation of digital value that underpins European prosperity, presenting major innovation opportunities for European start-ups, SMEs and large businesses.

Intermediary liability protections are considered by many to be the cornerstone of the internet economy. It is clear that many jurisdictions, including the EU, recognise the benefits that platforms and intermediaries bring to an economy. The EU E-Commerce Directive enables internet services to host, process, and distribute user-generated content without being treated as the creator or originator of such content for purposes of determining liability. The E-Commerce Directive provides appropriate rules on the liability of an intermediary or platform, provided that they take swift action to remove or disable upon notice of illegal activity or information. These safe harbors are key to enabling digital trade and digitisation of industry.

Companies in all industries are innovating, adding more and more sides to these already multi-sided relationships, and creating new value for consumers and other business users. The concept of a platform or intermediary is not new nor unique to the internet, and online platforms allow for faster growth and connections to new markets. At the same time, a number of concerned companies are investing heavily in technologies such as artificial intelligence to combat misinformation, piracy, and illicit content. **There are real opportunities for companies to work together with civil society and governments to improve and expand the effectiveness of these solutions**. Intermediary liability protections make it easier for these companies to self-police and work with governments to identify and remove illicit content without fearing retribution for the content's existence.

While protections for intermediaries and platforms from liability are critical for today's economy, they are not without important nuance and guideposts. For example, efforts in the United States and Europe to combat sex trafficking, false or misinformation, terror content, and piracy require important collaboration between regulators, intermediaries, and other stakeholders in order to ensure that new rules do not create unrealistic or undesirable burdens or have negative impacts on other parties in multi-sided transactions. For instance, such negative impacts or burdens would accompany any requirement to constantly monitor and filter all content or serve as arbiters of fact, analysis, or opinion of citizens, where some parties may not necessarily have the appropriate resources for such a task. Additional requirements to provide default options or to remove a bad actor in a timely manner in a B2B/P2B context would denigrate the consumer experience at the expense of business user fairness or could jeopardize the reputation of the platforms and relations with other business users.

Our Recommendations

- As the notion of a platform refers to very different models, policy makers 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 that markets remain open to innovative challengers, maintaining consumer welfare and economic efficiency as the final objectives and focusing on resolving proven market failures.

- To continue its leadership in digital trade and foster vibrant domestic economies, any future EU action should uphold the fundamental balance provided by the principles of the E-Commerce directive, and focus on a reflection about if and how future policy could address today's information society challenges, primarily through fostering partnerships between online service providers and relevant authorities.

- Tech companies are part of the solution in threading the needle of complicated policies that include multiple facets of the economy and types of business interactions. Policies should achieve increased transparency and competition for this important sector, maintaining the ability of companies to innovate and continue to succeed in Europe.

- Rather than adopting a "one size fits all' or an otherwise overly prescriptive approach towards platforms – unworkable in a dynamic industry with multiple business models, types of users, types of business partners, and existing tools in place to address the issues at stake - any new regulation should focus on how business users interact with and benefit from greater transparency and communication with online intermediation services.

ITI Recommendations on Competition Policy

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 address challenges arising from technological change globally and in the EU. Europe is a leader in several segments of the digital economy, such as app development, which creates revenues in the EU for about a third of the global market. Cybersecurity and software development are other growing areas of expertise in the EU.

Consumers' trust in market rules and players is crucial. Ensuring consumers' control over their personal data according to the EU's General Data Protection Regulation is key. 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, augment human capability and enable advances in education, healthcare, transportation, sustainability, and many economic efficiencies in innumerable fields.

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, for example in transport, communications, or tourism. 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. Recent EU initiatives like the geo-blocking regulation, the New Deal for Consumers and the platform to business rules are increasingly regulating this space.

There is no clear-cut understanding of many digital activities and technologies. For example, 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 well increase competition, but also reduce consumer welfare. While efficiencies of scale and network effects might strengthen a market position, a platform's value to each user may grow with the number of other users, enabling them to use conveniently one or few platforms for shopping, social interaction, transportation, travel, accommodation etc. Strong **network effects** may disincentivise switching platforms and impact choice and competition. Whilst network effects may be offset by multi-homing and increased competition across platforms, this can be reinforced by lack of interoperability or gatekeeper applications. Requirements to bundle operating systems and applications could limit competition, but also benefit consumers, e.g. by offering devices working right out of the box. These factors should be considered, but only together with others like market behaviour and a company's conduct.

Big data and AI are also rapidly changing the way strategic market decisions are made. Certain types of data could possibly be used anticompetitively, but the value is created by the processing of data. So this alone does not justify establishing a special treatment under antitrust rules. Since there do not seem to be default antitrust concerns that would justify sacrificing the potential economic efficiency brought about by data and the use of algorithms, we encourage the EU to evaluate existing policy tools surrounding AI in a way that limits uncertainty. and use caution before taking measures that may decrease competition instead of fostering it.

Our Recommendations

- 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.

- 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.

- Market definitions should better reflect the sectors' competitive dynamics and the fact 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.

- **Data** should be assessed under competition law as any other asset that companies compete with in the market but taking into account 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. Policy makers should particularly consider potential unintended consequences of an unduly strict approach to big data, resisting the urge to create new rules for every new product or business model, which might stifle the adoption of 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.

- 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.

- 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, while avoiding 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 it easier for users to switch across competing applications, i.a. 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.

- As the notion of **platform** refers to very different models, policy makers 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.

* * *