

Brussels, 31 October 2012

DIGITALEUROPE POSITION ON THE EU-US REGULATORY COOPERATION

DIGITALEUROPE welcomes this opportunity to express industry views on how to make regulatory regimes more compatible across the Atlantic. This paper presents key issues for the European ICT industry which could be considered in the framework of the preparations for the EU-US agreement. We believe that those initiatives would substantially improve the environment for conducting business on both sides of the Atlantic.

DIGITALEUROPE is promoting free trade; we stand for openness and we call for a level playing field across the globe. As a consequence of the global nature of the ICT industry, globalisation of supply chains, and expansion of the digital economy, we support trade liberalisation and cooperation on multinational trade arena, as well as conclusion of comprehensive free trade agreements. Those actions will further release trade potential, create new economic opportunities and hopefully reinvigorate much needed growth.

We recognise the momentum in the transatlantic relations; we observed prominent European and American leaders expressing their strong interest in market opening arrangements. The European Union and the United States are important markets for the ICT sector. We believe that their economic partnership would benefit from further enablers, such as a comprehensive trade agreement. We are particularly glad that the European Commission and the US Government share the goal of reducing excessive regulatory costs, unjustified regulatory differences and unnecessary red tape. A more harmonised or compatible transatlantic market would have a positive effect on market growth by increasing the competitiveness of our industries and reducing their costs.

With regard to regulations, a strong set of common principles has been jointly affirmed in the High-Level Regulatory Cooperation Forum's statement on "Common Understanding on Regulatory Principles and Best Practices." However, differences in the EU and US regulatory systems and approaches to risk management make it difficult to apply these principles to achieve harmonisation. Moreover, in practice product requirements imposed by EU and US technical regulations at times diverge, even when underlying regulatory objectives are equivalent. Those regional differences in product requirements may force the industry to develop different versions or functionalities of the same product; this leads to delays in time to market and significant additional costs. Removing unnecessary divergences in regulatory requirements that products and services need to comply with in order to achieve general market access or be eligible for (or enjoy a preferential status in) public procurement would

DIGITALEUROPE

Rue de la Science, 14 >> B-1040 Brussels [Belgium]

T. +32 2 609 53 10 >> F. +32 2 609 53 39

www.digitaleurope.org

Transparency register member for the Commission: 64270747023-20

lead to significant efficiencies and cost reduction. Solving existing discrepancies and avoiding future regulatory divergences should be a priority.

The European ICT industry asks for an improved and more coherent regulatory environment. In this paper we recommend an approximation or mutual recognition of regulations in the areas of standardisation, e-accessibility, e-health, conformity assessment, e-labelling, intellectual property (IP) and environment. We also think this is a great opportunity for both the EU and the US to remain leaders in developing digital services and hence to stress the need for a framework guaranteeing global data flows. Those topics are discussed in detail in this contribution.

In addition, DIGITALEUROPE wishes to call on the European Commission and the Government of the United States to avoid divergent policy approaches. For instance, coordination between the EU and the US with regards to the nascent Internet of Things would be commendable. Secondly, the work of the EU–US cyber security working group should continue with a view to guarantee compatible solutions. Security of infrastructure and devices is crucial in enabling further trust in the Global Digital Infrastructure. DIGITALEUROPE welcomes the creation of the EU – US cyber security working group and calls for the EU and the US to continue coordination on various cyber security policies that third countries are creating to ensure that these do not disrupt the Global Digital Infrastructure (GDI). The transatlantic cooperation should also increasingly focus on ensuring that third country approaches to security are not restricting market access.

Further, we ask for coherent policy in regard to European and American R&D programmes. Given the global nature of the ICT industry and its product markets, large enterprises transfer IP across borders throughout their organisations as a normal course of action. Such enterprises have design and product development teams located in multiple countries that share “know-how” and ideas among their employees, and the products that these teams develop are in most cases sold in global markets regardless of where IP is created, legally owned or registered. Therefore, there should not be any restrictions on the transfer of foreground IP to other affiliated entities in the framework of publicly financed R&D. Furthermore, affiliated entities worldwide should have the same access rights as participants.

Looking beyond the regulation of the European and American markets, DIGITALEUROPE wishes to encourage the EU and the US to jointly promote trade liberalisation and to address problems created elsewhere, such as requests to provide far too much unnecessary confidential business information to show compliance with technical regulations and thus gain market access. The EU and the US need to address the increasing tendency of some emerging markets to develop regulations that mandate the use of specific technologies rather than being performance based. We hope that the two partners will work together towards elimination of forced localisation requirements. Governments are increasingly requiring businesses to locate R&D, IP, manufacturing, etc. as a condition of market access. An EU-US agreement should prohibit such trade distorting requirements and commit both governments to push back on those measures wherever they occur.

In this regard, the agreement should be creative – for example, where binding language cannot be employed to address specific third party issues, the document could still include helpful preamble language that provides policy direction and/or incorporate best practices or policy principles on evolving topics like cyber security and forced localisation requirements.

Finally, we encourage the two partners to reaffirm their joint commitment to maintain the status quo on Internet governance (ICANN/IGF, etc.) and ensure that the Internet ecosystem remains open to innovation and commerce globally. The EU and the US should continue to promote this arrangement globally.

We are pleased that industry was invited to participate in the task to map initiatives to be undertaken by the two partners. We are prepared to work with you to achieve the ultimate goal of regulatory coherence.

1- COMMENTS AND SUGGESTIONS ON EU-US COOPERATION ON STANDARDS IN THEIR POTENTIAL TO FORM NON-TARIFF TRADE BARRIERS

Generally, EU as well as US policies with regard to standards in their potential to limit or burden trade between nations are strongly founded in a firm commitment to the WTO TBT Agreement, including an emphasis on the use of voluntary global standards.

This forms a strong common basis that the EU and the US should seek to further exploit in trade relations – in the bilateral EU-US trade relation, as well as in cooperating towards reducing barriers faced by both in third countries.

In the bilateral EU-US relation, and in spite of sound basis of common policy principles, the actual standards systems in the EU and the US display notable differences and are built on different regulatory traditions. Generally, the ICT industry has not encountered dramatic trade issues as a consequence of these differences, but there is potential for further reducing unnecessary cost factors introduced by divergences in the actual standards requirements that products and services need to comply with in order to satisfy conformance requirements, in order to be eligible for (or enjoy a preferential status in) public purchasing, or to satisfy public policy goals.

The ICT industry in general operates on a global scale. Differences in standards requirements between the US and the EU will typically require the implementation of more than one standard for the same functionality, and hence lead to duplicated implementation efforts and costs. In some cases, such duplications are unavoidable consequences of, and economically reasonable responses to different market-driven requirements expressed by different voluntary standards. However, non-market driven divergences in standards requirements lead to unnecessary and economically unreasonable duplication of cost and effort. More harmonised or compatible requirements on products for the same market

segment would have a positive effect on market growth and create more opportunities for industries in the US as well as the EU.

A full harmonisation of standards systems between the EU and the US is neither likely, nor necessary to avoid negative trade impacts. However, cooperation and tools to address and prevent such impacts can be improved. Some valuable principles towards this aim have been jointly laid down at the EU-US Transatlantic Economic Council in November 2011 (“Building Bridges between the U.S. and EU Standards Systems”). Implementation of those principles and intentions should be one matter of priority for the EU and the US. At a more detailed level, the new EU framework on standards provides for enhanced convergence opportunities. The recognition of the role of global fora & consortium standards in the ICT industry in that new legal framework enhances the scope of specific standards and technical specifications that can potentially be commonly be referenced in EU and US public purchasing and policy. This opportunity should be exploited; the EU should explicitly consider and address transatlantic trade aspects in processes towards the identification of ICT technical specifications eligible for direct referencing in public purchasing and sectoral policies (and the US and the EU already cooperate in a number of sectoral policy areas, such as eHealth, smart grid and eVehicles). The EU should ensure that processes around identification of ICT standards in the multi-stakeholder platform foster transatlantic compatibility. In particular, it is important to avoid handicapping cooperation towards compatible sets of standards by using this process to unduly discriminate or exclude relevant specifications that represent US Voluntary Consensus Standards that comply with the European framework’s criterion that such standards meet the WTO TBT criteria for international standards.

In relation to third countries, the EU and the US should exploit their substantial commonalities in policy principles around standards in trade. EU and US industry is often facing the same standards-related trade issues in countries with different policy principles – issues that have to do with lack of compliance with, or a different interpretation of WTO TBT principles. The US and the EU should strengthen their cooperation on a trade political level to jointly promote common policy principles and interpretations, to jointly address concrete issues as they arise, and to jointly lead global evolution towards unimpeded trade with demonstrated best known implementation methods.

2- AN EU-US COOPERATION IN THE AREA OF E-ACCESSIBILITY

In keeping with the intent on the new EU Regulation on **standardisation**, the area of accessibility requires recognition by any relevant regulations and policy makers of the importance of international standards and global fora & consortia technical specifications as they relate to accessibility. In particular the W3C WCAG 2.0 guidelines and the emerging W3C WAI-ARIA specifications are critical and their importance is recognised within both Section 508 in the US and the Mandate 376 work underway in the European Standardisation Organisations (ESOs). Additional standardisation efforts or references in trade arenas

should contribute to the international work in this area, be consistent and compatible to international and global standardisation approaches, and subject to mutual recognition procedures. Any limitation to ESO or national standards should be minimised and subject to the criteria of consistency and compatibility.

Examples that highlight the need for consistency with international approaches and mutual recognition would include use of ANSI/IEEE C63.19 2011 which covers the compatibility between hearing aids and mobile phones.

Supplier Declaration of Conformity (SDoC) has been successfully used for accessibility compliance in the U.S and is a stable and proven approach. If accessibility compliance in the EU is subject to regulation (as has been proposed), the SDoC approach should be replicated and form the basis of a mutual recognition agreement. Any requirements should be based on standards which specify functional requirements, are cross-platform, objectively testable, technology neutral and support further innovation and competition.

A consistent approach to accessibility and any requirement to conform to accessibility standards is critical to maximise the availability and effectiveness of accessible solutions. Market fragmentation via differing technical standards can only harm levels of accessibility. DIGITALEUROPE therefore proposes **mutual recognition** as the appropriate method to drive cooperation and coordination to achieve the highest level of consistency without creating a barrier to innovation.

Accessibility approaches should recognise the constant innovation in accessibility approaches and technology capability as well as a pragmatic approach to promoting accessibility in new product areas.

3- ACCEPTANCE OF E-LABELLING

It is currently an obligation that all apparatus complying with the essential R&TTE requirements in both the EU and US affix the regulatory marking (e.g. CE mark in the EU, FCC mark in the US) on the product or its data plate. The role of regulatory marking like CE is to indicate to the consumer that the product is in compliance with all the regulatory requirements and safe to use, as well as assisting Market Surveillance authorities in ensuring this.

However, the fast pace of technology development has led to a reduction in the size of devices like hand held mobile devices whilst at the same time increasing their complexity. This has meant more labelling requirements and ever decreasing areas in which to place them. In addition, the future use of software defined radio (SDR) would allow devices to be configured post sale, which could potentially render any label affixed at point of sale redundant.

To answer those challenges, DIGITALEUROPE proposes the acceptance of an optional Electronic Marking on Radio and Telecommunication Terminal Equipment with integral display in the framework of the EU-US Free Trade Agreement.

The mobile industry has already been proactive in this area in both Europa and the US and has specified the use of MMI Command *#07# within 3GPP TS 22.030 for the purposes of displaying this regulatory information. Electronic marking would ensure that where the device is reconfigured, any changes to the regulatory markings e.g. Alert symbol could be updated and remain relevant. In addition the use of electronic marking would give the consumer better access and understanding of the regulatory information as well as paving the way for improved accessibility to the disabled user.

Electronic marking or labelling (e-labelling) is an option (for products with screens) to display via a product's integral screen, some of the required and voluntary regulatory marking information instead of physically affixing a permanent label to the product. For the purpose of this proposal, *regulatory marking requirements* shall be the marking required to be placed on the product (In the EU by R&TTE Directive).

1. CE Mark.
2. Notified Body identification number – when applicable
3. Equipment Class Identifier – when applicable
4. Type, batch and/or serial numbers and the name of the manufacturer or the person responsible for placing the apparatus on the market.)

With the proposed electronic marking, the regulatory marking requirements for the packaging and accompanying documentation would remain unchanged.

Furthermore, and following needs from Authorities when performing Market Surveillance activities, the requirement to place the *Identification of the product* (point 4 above) on the device would also remain as a method of linking the product to its Declaration of Conformity.

Finally, a temporary label (e.g. film label) would be added to the product allowing the consumer and any Market Surveillance Authority to see all product regulatory markings (points 1 to 4 above) at the time of purchase without having to switch the device on. After purchase, the remaining regulatory marking (points 1 to 4 above) would be accessed e.g. via the device keypad using an industry recognised method.

In short, the benefits of e-labelling are:

- Better access and information on regulatory and compliance information for the consumer;
- Better design flexibility for the manufacturers;
- Faster time to market; and
- Reduction of costs.

4- ENHANCE MARKET ACCESS: SUPPLIER'S DECLARATION OF CONFORMITY

The ICT industry, as truly global, considers the ongoing proliferation of national/regional product safety regulations a major restraint on achieving free trade. The European Union has established a concept of 'New Approach' which allows free trade between Member States, based on Directives which contain high level 'essential requirements' combined with conformity assessment modules to show compliance of the involved products, such as electrical and medical products, machinery, toys, etc. The success of this system was supported by the possibility to allow the manufacturer to issue a **Supplier's Declaration of Conformity** (SDoC) based on harmonised European standards. These standards are typically derived from international (IEC) safety standards, as also used in the IECEE (CB scheme) and their status of harmonisation is determined by the Commission.

Another element of this concept is **Market Surveillance** performed by the national authorities. Market Surveillance ensures that products are safe after they have accessed the market, and that Economic operators have a diligent approach. Instances where IT products that have been the object of inspection in the EU have obtained 3rd Party safety approval for other countries yet requiring correction, are not infrequent.

In this context, DIGITALEUROPE believes that the acceptance of a Supplier's Declaration of Conformity (SDoC) on both markets as sole prerequisite to put products on the US Market would enhance trades without prejudice to safety.

SDoC is mostly used for products and sectors which involve a low or medium risk to health, safety and the environment. However, an analysis of risks is not the only factor that Members take into account in their decisions to allow for the use of SDoC for a specific product or in a specific sector. The following elements may be considered in combination with the nature of the risks involved:

- the particular characteristics and the infrastructure of a given sector;
- the number of existing voluntary marking schemes for a product;
- the types of production methods used for the manufacture of the product;
- the level of commercial confidence; and
- other economic and social factors.

SDoC has been used for the following categories of products: disposable lighters; electrical products; electromagnetic compatibility (EMC) and radio and telecommunication terminal attachment equipment (RTTE); electronic safety equipment; electronics; equipment for use in potentially explosive atmospheres; machinery; medical devices; motor vehicles and motor vehicle equipment; personal computers (PC's) and PC peripherals; personal protective equipment; recreational crafts; steel profiles for power transmission towers; telecommunications; toys; vehicle catalysts; and, vehicular natural gas.

The following summary describes the scheme recommended by DIGITALEUROPE:

- **Market Access Conformity Assessment**

SDoC should be the preferred option, used already today by nearly all participants from the ICT/CE industry. The preferred choice of the manufacturer should be a SDoC based on qualified manufacturers Laboratories (accredited to ISO/IEC 17025 or integrated into the manufacturer's ISO quality system) or 3rd Party Conformity Assessment Bodies accredited (by IECEE CB Scheme, or ILAC/IAF schemes to 17025) with appropriate Product Certification Labs (accredited for ILAC Schemes). In any case SDoC is based on profound technical documentation residing at the manufacturer and available for the authorities. Duplication of identical efforts, including time consuming administrative processes, already performed at the Supplier's qualified testing laboratories, by additional 3rd Party Testing (independent from Manufacturer Labs) does not provide additional 'assurance of safety'.
- **Product Liability**

The product liability is described and resides with the company that brings the product into the respective national markets. This is either the 'Manufacturer' or an 'Importer' as the 'authorised representative' of the 'Manufacturer' or as a 'Distributor'. In any cases the responsibility for product liability resides with this company, regardless of the usage of SDoC or 3rd party testing
- **After Market Surveillance**

In the EU, it is the responsibility of national authorities established by Member States to ensure market surveillance and worker safety and levy penalties for false or misleading declarations. Member States' organisation of market surveillance varies: some have a centralised system while others deal with it through local governments. Despite the differences in approaches and procedures, the EU is continuously improving its effective market surveillance along with its Member States through initiatives such as "joint visit programs", EMARS. These initiatives could, in the future, lead to the application of common criteria for market surveillance for all Member States. In the use of SDoC, the EU has identified, through market surveillance, two categories of products for which there is a high degree of non-conformance, namely electronic goods and toys. In the case of obvious safety hazards, the "safeguard clause" of the EU Directives is used to prevent unsafe products entering the EU market. This means that if a safety problem is detected in one Member State, all Member States are immediately informed, steps are taken to withdraw the product from all markets and a system to investigate is set up.

Market surveillance is necessary for all types of Conformity Assurance systems. Systems that require mandatory 3rd Party Product Certification & Manufacturing Inspections do NOT have lesser recall rates nor do they need less emphasis on market surveillance than systems based on the 'Supplier's Declaration of Conformity'. Statistical data from Europe and the US clearly show, that also detected and recalled unsafe products have been certified.

The EU experience clearly proves that this balanced approach of Market Access, Product liability and After Market Surveillance is the fastest, most flexible and the most cost efficient way for suppliers and at the same time ensures a steady improvement in consumer and workers safety.

Nowadays manufacturing sites are distributed globally and products are used globally – it does not matter by whom the product and its subcomponents are manufactured; what matters, however, is that the product placed on any specific national market should be safe as defined by that Nation's regulation. The essential product requirements and respective test standards should be internationally harmonised based on commonly defined regulatory requirements. Those are a key factor to the success of global market players.

We strongly advocate the use of harmonised international standards to define the technical requirements that have to be met. The EU experience successfully shows that it is possible to harmonise the requirements of many national legal requirements. We also support the suggestion that all ICT Equipment should be allowed to be brought into the US market based on meeting the requirements of the current international product safety standards, particularly including the international Safety Standard IEC 60950.

5- AN EU – US TRADE AGREEMENT SHOULD ADDRESS DIGITAL ECONOMY ISSUES AND ENSURE CROSS-BORDER DATA FLOWS

Global cross-border trade in services has grown strongly in recent years. From 2003 to 2008, world exports of services more than doubled, jumping from \$1.8 trillion to \$3.8 trillion, before falling back to \$3.3 trillion in 2009. Trade in these services, which include transportation and travel, insurance and other financial services, telecommunications and IT services, business professional and technical services, royalties, license fees and many other services, has yielded clear global economic benefits. The European Union and the United States, as large services exporters, have much to gain by promoting services liberalisation in the EU-US trade agreement.

Much of the growth in global services trade has largely been enabled by the development of fast, efficient and cost-effective electronic communications networks, including the Internet, which has become "the global trade route of the 21st Century". In fact, almost half of cross-border trade in services worldwide is enabled by information and communications technology (ICT) services, and the share of electronically delivered services is increasing.

The group of services enabled by ICT extends far beyond computer and related services and telecommunication services. As the European Centre for International Political Economy (ECIPE) has pointed out, a sampling of ICT-dependent services would include financial analysis, engineering, research and development, insurance claims processing, design, education, publishing, medical services and journalistic work.

Enabled by robust ICT networks, it is knowledge and expertise that is crossing borders in these cases. As such, cross-border trade in these services is, fundamentally, the exchange of data across borders. Innovative firms in many service industries are increasingly able to use data to more effectively serve customers around the world, reduce transaction costs and improve efficiency. This has in turn driven economic growth, productivity and innovation.

However, the tremendous increase in cross-border data flows that has accompanied burgeoning services trade has raised concerns on the part of many governments. Some are enacting, or considering, restrictions on such flows on the basis of privacy, consumer protection, security or other reasons. Given that cross-border services trade is, at its essence, the exchange of data, unnecessary restrictions on data flows have the effect of creating barriers to trade in services. These restrictions, like localisation of resources, could actually harm European service providers and their workers. There are a number of possible mechanisms to ensure that data flows, and the services trade that depends on them, can continue.

Restrictions on cross-border data flows could become a major barrier to trade in services. International trade in many services depends on cross-border data flows between service providers and their clients. Electronic delivery of services across borders is simply not possible without the ability to send and receive information over networks. While a government might make cross-border services market access commitments in trade agreements, if it blocks or severely restricts data flows unnecessarily, those commitments would be undermined and would provide no benefit to multinational service providers.

The EU-US trade agreement needs to ensure cross-border data flows. Data flow commitments or non-binding agreements should be negotiated to complement cross-border services commitments and promote responsible and accountable treatment of data. This might be achieved through provisions in the EU-US trade agreement, balancing the need to protect data with the right to move data. The EU and the US need to work together to develop approaches to privacy, data security and protection that will instil confidence in, and reduce resistance to, cross-border data flows. It could reduce the government's perceived need to restrict data flows and provide greater opportunities for cross-border trade in services.

There are a number of possible mechanisms to ensure that data flows, and the services trade that depends on them, can continue such as ensuring greater legal harmony between EU Member States on data protection and IPR arrangements. In addition, ensuring more interoperability between the EU and third countries in for example data protection will also provide more legal certainty to users and organisations.

The discussion in the EU on a new data protection regime is an opportunity to discuss the issue in a cooperative spirit and with the goal of avoiding obstacles to transatlantic and global flows.

The prospect of a bilateral EU-US agreement presents an important opportunity for the world's two leading services economies to establish a model agreement and rules to enable the global digital economy, ensuring the ability of their service providers and multinational businesses to move data around the world so that they can manage their businesses and server their customers most efficiently. The EU and the US should follow through on their pledge to implement the [EU-US Trade Principles for ICT Services](#) and should also seek to incorporate the [OECD Internet Policy Principles](#) in any agreements that they negotiate with each other or with other parties.

Together, the EU and the US can set a positive example for how to enable strong growth and job creation in the digital economy. The EU and US should hold regular bilateral dialogues on assessing impact of various government actions that are restricting such flows and creating barriers to trade, which should be addressed both bilaterally but also in the EU and US governments' dealings with third countries. The current Information Society Dialogues (ISD) could serve as such a platform if it includes participants from all relevant agencies/departments on both sides.

6- IMPROVED IP FRAMEWORK – PATENTS, TRADE SECRETS, CONTENT PROTECTION AND TRADEMARK¹

DIGITALEUROPE is delighted that the EU and the US share the goal of reducing excessive regulatory costs, unjustified regulatory differences, and unnecessary red tape. We fully agree that promoting this goal will help businesses to grow, create jobs, and compete globally.

In the field of intellectual property, this common objective is fully in line with earlier agreements made in the WTO Agreement on trade-related aspects of intellectual property rights (IPRs), in which Articles 41 and 62 state that procedures concerning enforcement and acquisition of IPRs shall not be unnecessarily complicated or costly.

In this framework we applaud the US' intention to join the international industrial design registration system that is administered by the World Intellectual Property Organisation ("WIPO"), as this will greatly simplify the acquisition of industrial design rights ("design patents") for innovators at both sides of the Atlantic. The EU is already a party to this system.

As regards **patents**, in 2000 the WIPO Patent Law Treaty ("PLT") was concluded, aiming to reduce red tape in the acquisition of patents for inventions. While the European patent system has been largely adjusted to the PLT standards by means of a revision of the

¹ Please note that this position paper has been adopted under a broad majority (DIGITALEUROPE By-laws require a two-thirds majority). Opposing DIGITALEUROPE member does not agree with some parts of section 6 of the paper. Opposing member considers the requirement for an inventor's signature on a patent declaration in the United States to be indispensable because it is a manifestation of an inventor's rights granted by the US Constitution, protects the rights of the inventor and the company/entity that the inventor chooses to assign the patent, and prevents others from taking what is not theirs or claiming more than what is specified in the patent.

European Patent Convention (“EPC2000”), the European Patent Organisation has not yet ratified the PLT. This omission should be repaired. We applaud the US’ intention to ratify the PLT, and we hope that in this connection the US will also bring its patent system more fully in line with the PLT standards.

We applaud the US’ recent introduction of the possibility for corporate applicants to file patent applications, which was already possible elsewhere in the world. However, the US requirement that the inventors need to sign declarations is at odds with the requirement of Article 6(6) PLT that evidence may only be asked for if the office may reasonably doubt the applicant’s statements. In Europe, the applicant only needs to state the names of the inventors and how he got the right to be granted a patent (for which purpose it suffices to state: employment agreement). We believe that the US should similarly do away with the need to chase the inventors for signatures.

Just as Europe has done when the EPC2000 entered into force, the US should withdraw all its notices of incompatibility that prevent applicants from benefiting from modernisations in WIPO’s Patent Cooperation Treaty (“PCT”), which facilitates patent acquisition for 146 states.

We believe it to be important that the EU and the US join efforts in convincing other states to fully meet the WTO-TRIPs agreement to ensure that IPR procedures are not unnecessarily complicated or costly. However, to be able to do so, the EU and the US should lead by example, and the ratification and full and unreserved implementation of the PLT by both sides is essential in this respect.

Protection of **trade secrets** is also increasingly important as their theft and forced regulatory disclosure is on the rise. The patchwork of different approaches across Europe has likely led to costly or inefficient protection of trade secrets within the EU’s internal market. The lack of adequate protection of trade secrets impairs their dissemination from employer to employee and customer/supplier, which is a further hindrance to domestic innovation. Moreover, inconsistencies within European legal systems undermine EU demands that its trading partners treat European trade secrets as a form of intellectual property and increase their protection.

Effective trade secret protection as a form of intellectual property is crucial for industry investment decisions. U.S. authorities generally treat trade secrets the same as other forms of IPRs such as patents or copyrights. In recent years, trade secret law in the US has become largely statutory through the model Uniform Trade Secrets Act, which has now been adopted in the great majority of states. Once it has been established that a trade secret has been misappropriated, a number of remedies are available including injunctions and damages for the actual loss caused by the misappropriation, largely consistent with infringement of other forms of IPRs. In contrast, there are significant discrepancies among the trade secrets laws of the EU’s member states, and not all member states or the EU even clearly recognise trade secrets as a form of intellectual property right. This leaves the EU in a weak position in seeking better protection of European trade secrets by foreign nations like China and India, particularly compared to countries with more robust trade secret regimes like Japan/US. The EU is at a disadvantage in safeguarding its trade secrets and

should not miss an opportunity to fix its IPR system – especially since this form of IP has become more important over time as critical “know-how” in services and manufacturing is increasingly difficult and expensive to protect as patents. Therefore, the parties to the incoming agreement should abide by their duty to implement Section 7, Art. 39 of the TRIPS agreement on protecting undisclosed information as a form of intellectual property, and the European Union should start considering how to more fully implement its TRIPS obligation concerning trade secrets. In order to provide adequate border measures, Union-wide trade secrets, as other intellectual property rights, should also come within the ambit of the Customs Regulation.

In terms of **content protection**, an appropriate action of the European Union might be to encourage continued industry discussions regarding private agreements that would provide for the pan-European licensing of content and market-driven private agreements related to development and implementation of technological solutions, such as those that exist today to protect premium content from unauthorised use, copying and distribution. DIGITALEUROPE believes that a “markets, not mandates” approach to copyright should govern all content protection issues. In our view “content protection” is achievable, but “consumer policing” is not effective.

DIGITALEUROPE also wants to present remarks regarding **trademark**. Since there are no uniform trademark protection laws across the world, some countries almost appear to encourage the theft or misuse of this type of intellectual property; those involved in trademark infringements and selling fake non-or-barely-working hardware, true counterfeit products, or remarked products pass themselves off as legitimate sellers of the manufacturer’s products and the end user or buyer becomes a serious victim. The traffickers in copied trademarks and products who are transporting (importing and exporting) or selling the products find ways to avoid paying appropriate taxes which hurts the government and the honest tax payers; the trademark violations can also be contractual issues against a company’s vertical distribution agreements and contractual agreements for production limits, sales in certain countries or sales outlets, etc. The EU and the US should work together. Two actions would improve the fight against trademark infractions and counterfeits: better product classification systems by government and purchasers so that critical components are only purchased through appropriate authorised distribution and increased coordination and information exchange between brand owners and law enforcement and customs organisations to better utilise the manufacturer in identifying authentic versus suspect counterfeit products at the borders to each country. Neither side can do this on its own – it must be a working partnership. To this end, we propose better training for those trying to stop electronic and semiconductor counterfeits at the borders. Improvements must be made to the system of allowing stakeholders to identify counterfeit products at the borders or with local and regional law enforcement to ensure efficient enforcement of intellectual property laws domestically. We recommend that actions are taken to ensure that Customs provide brand owners with sufficient information about seized goods to enable the brand owners to distinguish between their genuine products and counterfeit goods, and to better assist Customs with their duties, improved cross-border information sharing so that both the exporters and importers can be investigated and prosecuted, better (and preferably cross-Atlantic) cross-functional teams

between brand owners, law enforcement and customs organisations. Interoperability between EU and US data exchange systems should be provided to avoid that IP owners have to fill databases in different ways with the same info.

7- ENVIRONMENTAL REGULATION

As there has been certain instances where environmental regulation constitutes barriers to free trade this regulation need to be addressed also in this context.

Substance restrictions: There is increased interest by individual US states (e.g., CA, MN, WI) in prohibiting the usage or reducing the exposure of certain priority chemicals that may be deemed to pose risks to the environment or human health if not managed properly. Some of these efforts overlap or are similar to the objectives of EU REACH Regulation and RoHS Directive, but are not entirely the same for legal and jurisdictional reasons. The challenges are compounded when efforts to identify priority chemicals by US states is not entirely the same, nor are the methodologies to measure exposure or risk. One result could be varying regulations across the US states, banning different chemicals with different implementation dates. The result could be that for the US market there are either different product lines for sale within US (and the US and Canada), or there are no products sold at all because compliance costs are too high. The EU RoHS has become a de facto international standard that most large companies follow globally. We propose that the US and the EU should strengthen their cooperation on a political level to jointly promote common policy principles regarding substance restrictions in order to ensure that products fulfil the highest standards on both markets and to eliminate any unnecessary delays in bringing new products to market because of different bureaucracy or differing product requirements.

Energy efficiency: There are various efforts underway to improve the efficiency of external power supplies or battery charging systems in many markets, we recommend that efforts to enable global commerce and the widest gains on efficiency can be made by using common definitions, standards, common methods for measurement and developing realistic timelines for implementation.

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies.

DIGITALEUROPE ensures industry participation in the development and implementation of EU policies. DIGITALEUROPE's members include 60 global corporations and 33 national trade associations from across Europe. In total, 10,000 companies employing two million citizens and generating €1 trillion in revenues. Our website provides further information on our recent news and activities: <http://www.digitaleurope.org>

THE MEMBERSHIP OF DIGITALEUROPE

COMPANY MEMBERS:

Acer, Alcatel-Lucent, AMD, APC by Schneider Electric, Apple, Bang & Olufsen, BenQ Europa BV, Bose, Brother, Canon, Cassidian, Cisco, Dell, Epson, Ericsson, Fujitsu, Hitachi, HP, Huawei, IBM, Ingram Micro, Intel, JVC Kenwood Group, Kodak, Konica Minolta, Kyocera Document Solutions, Lexmark, LG, Loewe, Microsoft, Mitsubishi Electric, Motorola Mobility, Motorola Solutions, NEC, Nokia, Nokia Siemens Networks, Océ, Oki, Optoma, Oracle, Panasonic, Philips, Pioneer, Qualcomm, Research In Motion, Ricoh International, Samsung, SAP, Sharp, Siemens, SMART Technologies, Sony, Sony Ericsson, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, Xerox, ZTE Corporation.

NATIONAL TRADE ASSOCIATIONS:

Belgium: AGORIA; **Bulgaria:** BAIT; **Cyprus:** CITEA; **Denmark:** DI ITEK, IT-BRANCHEN; **Estonia:** ITL; **Finland:** FFTI; **France:** SIMAVELEC; **Germany:** BITKOM, ZVEI; **Greece:** SEPE; **Hungary:** IVSZ; **Ireland:** ICT IRELAND; **Italy:** ANITEC; **Lithuania:** INFOBALT; **Netherlands:** ICT OFFICE, FIAR; **Poland:** KIGEIT, PIIT; **Portugal:** AGEFE, APDC; **Romania:** APDETIC; **Slovakia:** ITAS; **Slovenia:** GZS; **Spain:** AMETIC, **Sweden:** IT&Telekomföretagen; **United Kingdom:** INTELLECT
Belarus: INFOPARK; **Norway:** IKT NORGE; **Switzerland:** SWICO; **Turkey:** ECID, TESID, TÜBISAD; **Ukraine:** IT UKRAINE.