DIGITALEUROPE

ANNEX DOCUMENT

DIGITALEUROPE's response to the public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy.

Brussels, 18 December 2015

Introduction

DIGITALEUROPE welcomes the opportunity to contribute to the public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy, as we believe that these issues deserve in-depth consultation with all parties involved and analysis before rushing into any legislative action.
However, we would like to outline the difficulties we encountered in trying to respond to the questionnaire built by the European Commission. We regret, for instance, that sections for comments were not made available for every question of the consultation as such availability depended on the answer given – yes or no. This constitutes a missed opportunity for respondents to explain their position as well as for the European Commission to understand the context and the reasons why a specific position is taken. We also regret the phrasing of many questions, for which we see a degree of bias that will result in misleading answers from the respondents. Finally, the questionnaire lists a selection of assumed practices of platforms – Section IV of the first of part of the consultation - out of context and in isolation from each other.

In this regard, we would like to provide some additional comments on the first three sections of the public consultation, which we hope the European Commission will find useful.

The Role of Platforms

Definition

DIGITALEUROPE believes that the definition proposed by the European Commission is broad and vague, and would potentially capture a very wide range of companies/activities and not just the well-known brands listed in the consultation document (strictly online businesses, offline doing online business, intra-enterprise, B2B and B2C business models, SMEs and global firms, European and non-European…). In our view, online platforms are not a distinct industry sector. It is not clear what problems the Commission is trying to address. Furthermore we do not see the point of defining platforms at this stage without knowing the objective. We would prefer a wider reflection of the role of actors across the online

value chain, taking into account the benefits as well as potential concerns.. As such, the vague definition proposed by the Commission should not serve as a basis for future regulation or the definition of rules for so-called online platforms. As far as we know there is no definition of offline platforms, so it is unclear to us why there should be one for online platforms.

Interestingly, a recent report, written by an expert committee at the French National Assembly1, recommends not to create a new category of platforms as this would "create further uncertainties and more complexity when it comes to qualify an internet player".

Benefits of using platforms

As mentioned in the Digital Single Market Strategy Communication2, the entire economy is becoming digital. Online platforms have been playing an increasingly central role in our lives and have proven to be beneficial for consumers, businesses and the economy, as they drive innovation, create new markets, and increase consumer choice whilst lowering costs and prices. Their activities contributed to around €430bn to the European Union economy in 20123.

Online platforms facilitate consumers' experience online by making communication and interaction easier and by making information more accessible. They empower consumers that make more informed choices, as they can instantly access and compare an even wider range of products and services, at lower and more transparent prices and at lower costs. Consumers' trust is also increased due to the provision of review and ratings mechanisms. While such mechanisms sets standards for the traders, it also give consumers more information about the products they intend to buy. Additionally, the use of online platforms allows consumers to share and better allocate resources as well as offers the possibility for consumers to become seller themselves.

Online platforms also offer great opportunities for businesses, small and big, that choose to operate through them. Companies can reach a wider audience at a lower cost, therefore helping with aggregating supply and demand. Companies that want to trade across Member States' borders also face legal fragmentation in the European Union. Operating through online platforms can help them abiding by the different local legal regimes when doing cross-border transactions. Online platforms also proved

1 « Numérique et Libertés: Un nouvel Age Démocratique », Recommendation 22, p.83-84 http://www.assemblee-nationale.fr/14/pdf/rapports/r3119.pdf

2 European Commission, 'A Digital Single Market Strategy for Europe', May 2015 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN

3 Copenhagen Economics, 'The impact of online intermediaries on the EU economy', April 2013 http://www.copenhageneconomics.com/dyn/resources/Publication/publicationPDF/6/226/0/The%20impact%20of%20online%20intermediaries%20-%20April%202013.pdf

to be helpful when it comes to creating new markets, often with reduced entry barriers and costs of transactions, therefore allowing new businesses to grow more quickly.

Tacking stock of existing EU provisions

As regards to the questions of transparency, use of information, relations between platforms and traders, suppliers and consumers, as well as the ability to move from one platform to another, DIGITALEUROPE would strongly encourage the European Commission to take stock and make use first of the already existing rules before developing new regulatory measures.

The Consumer Rights Directive lays down information requirements to be provided by traders to consumers (e.g. main characteristics of the product, identity of the trader, total price of the goods including all additional costs, information about delivery, right of withdrawal …).

Moreover, when it comes to transparency, Europe's current and future data protection framework lays down strict requirements for data controllers to provide a variety of information to data subjects when their personal data is collected. This includes the identity and contact details of the data controller, the contact details of the data controller's data protection officer (if applicable), the purpose of the processing, the legitimate interests pursued by the data controller, the recipients or categories of the personal data (if applicable), any intention to transfer the data to a third country or international organisation (including the safeguards taken), the period for which the data will be stored, the existence of the right to request access/rectification/erasure of the data, the right to object to further processing, the right to data portability, the right to withdraw consent (when the data processing is based on consent), the right to lodge a complaint to a supervisory authority, and the existence of automated decision making including profiling.

When it comes to the ability to move from one platform to another, the European Union's current and future data protection framework provides data subjects with the right to data portability, so that all data subjects have the right to receive the personal data they have provided a data controller in a structured and machine-readable format for the transmission to an alternative data controller. This current framework provides data subjects with the flexibility needed to efficiently change providers without the need for further technical requirements. The imposition of sector specific formats for the transfer of data would stifle innovation and become costly for businesses. Moreover, a 'commonly used' format leaves open the potential for a less secure mechanism.

In cases where market distortions are identified and healthy competition is threatened, EU competition rules should apply.

Finally, DIGITALEUROPE would like to stress that many potential problems should be addressed by market dynamics and self-regulatory measures.

Tackling illegal content online and the liability of online intermediaries

DIGITALEUROPE sees no need to reopen the eCommerce Directive and amend Articles 12 to 15. The liability of intermediaries hosting third-party content should be limited as currently provided by the eCommerce Directive. The current regime strikes the right balance between the interests of right holders, consumers and online intermediaries.

The liability limitations for third party content provided by the eCommerce Directive have been essential to the development of online services in Europe and its principles have underpinned the development of the Internet in Europe as the Digital Single Market Communication recognises. The liability limitations for third party content provided by the eCommerce Directive have been essential to ensure and protect freedom of expression in Europe.

Intermediaries should not be required to monitor and remove content proactively as part of an intermediary liability regime. Intermediaries should not be required to remove unlawful content without an order from a judicial authority which has previously determined that the content in question is unlawful. There is no need to modify the rules provided by the eCommerce Directive in Article 15 (no obligation to monitor), and we believe that the methods described in Article 16 (voluntary codes of conduct) are more efficient than any imposed obligation on intermediaries. As a matter of fact, many online intermediaries have already put in place their own monitoring systems.

The eCommerce Directive has proved to be a flexible instrument over time, as its provisions on the regime for intermediary liability are clear, flexible and technology neutral and should remain so. There is no need to revisit the existing categories of intermediary services: the current categories of conduit/caching/hosting have been and can be applied to new activities which have emerged since the adoption of the Directive. Creating new categories of intermediary services each time a new product, activity of service is created is not only unnecessary, it would also render the legislation complex and obsolete. As new services constantly appear and disappear on the market, maintaining the current technology neutral and flexible provisions are therefore much more preferable to creating new layers of rules and categories which could quickly become outdated.

Defining a specific approach for each category of illegal content should be the sole competence of judicial institutions on a case by case basis, and should not be defined via legislation. A negative

consequence of defining specific approaches is that it would create obligations for intermediaries such as proactively monitoring the content they host, which is contrary to the eCommerce Directive provisions. As such, intermediaries should not be responsible for assessing if content is illegal or not, also considering the different approaches in each Member State as to assessing the illegal nature of content.

Data and cloud in digital ecosystems

Free flow of data

Data location restrictions justified by national security reasons or public security reasons should be applied with caution, with a view to removing restrictions wherever possible. In many cases, they are counter-productive and do not help to diminish risks, incidents or unauthorised access. Certainly in relation to the commercial sector, we believe that any localisation requirements should stem only from customer choice as opposed to regulation. Data localisation requirements disrupt the free flow of data and have an impact on both local and global industry, which rely on international data value chains, as well as on the GDP growth of the country adopting it.

Given the importance of the global nature of the Internet based economy, restricting data flows and requiring local storage will strongly impact both international and domestic service providers and their customers. Such restrictions would limit access by domestic companies to leading technology services (including cybersecurity protections) and would impede their ability to operate in global markets, thus reducing their competitiveness and ability to grow. Mandatory location of data storage and / or processing does not improve levels of cybersecurity. On the contrary, data localisation requirements create barriers to market access, particularly impacting small and medium sized enterprises (SMEs), which are eager to attract customers not only domestically, but also in foreign markets. Access to the most advanced security technologies and how those technologies are implemented is more important.

As more countries introduce domestic cybersecurity related policies, it is important to carefully balance the impact of the policies on a country's national security and public safety with its potential impact on global trade, technological innovation and the benefits of information.

Therefore, we encourage the EU to take a leadership role at the European and global level to address protectionism and raise awareness globally on the negative impacts of data localisation requirements for the emerging digital economy.

Data localisation policies will prevent the emergence of a true Digital Single Market. The presumption should always be to allow data transfers within Europe, between Europe and the rest of the global digital economy. Minimal exceptions should only be allowed subject to stringent assessment, in full respect of the basic principles of necessity, proportionality, non-discrimination and subsidiarity – and in line with the exemptions of Art 14 of World Trade Organisation (WTO) General Agreement on Trade in Services.

There are several key areas that must be addressed:

- Prevent, address and remove general sector or market wide data localisation laws and policies;
- Public procurement policies should explicitly allow data transfers in Europe, and wherever possible even outside Europe, with all due safeguards as appropriate and in full respect of the commitments taken by the EU at WTO level;
- Strong monitoring and enforcement mechanisms should be in place to ensure individual procurement exercises adhere to these principles.

As a general remark, DIGITALEUROPE believes that the Free Data Flows Initiative should focus on abolishing unnecessary legal requirements for data localization by Member States, which are the main obstacle for free data flows in the digital single market. We regret that the consultation rather seems to prioritise additional restrictions on the contractual freedom of businesses regarding data access and ownership. Such restrictions are not justified and would risk undermining the development of a dynamic and innovative data economy.

On data access and transfer, the existing contract law framework is not an obstacle to the free flow of data and should not be changed.

Concerning possible regulation of the access to, transfer and the use of data, a range of legal framework apply, including competition, unfair commercial practices, or consumer protection law.

To the extent that the processing (including access, transfer and use) relates to personal data, which is very broadly defined in Europe encompassing any data that has the ability to identify an individual, this is extensively regulated by the current and upcoming data protection rules, in particular by the 95/46/EC Directive as well as the upcoming General Data Protection Regulation. Further rules on use, ownership, transfer and access of non-personal data would be unnecessary and unjustified as these would be not based on the same rationale, namely to protect the fundamental right to the protection of personal data.

Additional rights and obligations, or where the data is not directly regulated, is and should be set by contractual relations between the various parties involved.

European Cloud initiative

We refer to the Commission initiated and industry *led Cloud SiG, Data Privacy Code of Conduct,* which sets out data protection and security objectives and principles that Cloud Service Providers should adhere to in the EU. This code is based on the 95/46 Data Protection Directive with regard to data protection and the ISO 27000 set of standards and provides a comprehensive framework.

DIGITALEUROPE believes that the existing contractual practices in the enterprise cloud market provide a balanced allocation. These contracts are not based on a take it or leave it approach. Contracts are formulated and adapted to suit user requirements while minimising the need for lengthy individual negotiations and legal costs.

Supporting the idea of guaranteeing or ensuring portability or interoperability is not the main issue, as it constrains innovation and does not recognise industry engagement with voluntary standards. The cloud market is evolving rapidly and as a result industry have voluntarily supported and adopted global open standards in fora and consortia combined with formal international standards bodies and collaborative open source projects. This delivers the optimum balance of allowing strong competition to drive innovation and new features whilst promoting interoperability. Users should take care to assess the implications of their use case with regard to interoperability with other systems and portability to switch vendors, balancing innovative functions with interoperability or portability requirements.

We also would like to outline that there is an important distinction between portability of data and open interfaces on the one hand and "application portability". The application itself, for instance a database, will have its own individual design and structure, be it processes, specific formats, behaviours and outputs. This is what differentiates one provider from another and a move to standardise actual applications would have obvious negative implications – destroying competitive advantage and innovation. Such features are typically protected through intellectual property, design rights, copyright, patents and trade secrets. Data Portability and reversibility on the other hand are important requirements – the user should ensure that there are provisions for data to be returned in the event of contract termination, this may or may not be provided for free but should be specified.

While we support the general principle, there should be no new regulatory mandate for data portability.

For more information please contact:
Marion Ebel, DIGITALEUROPE's Policy Manager
+32 2 609 53 35 or marion.ebel@digitaleurope.org

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 fully 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 59 corporate members and 35 national trade associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Alcatel-Lucent, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cassidian, Cisco, Dell, Epson, Ericsson, Fujitsu, Google, Hitachi, Hewlett Packard, Huawei, IBM, Ingram Micro, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Mobility, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, Western Digital, Xerox, ZTE Corporation.

National Trade Associations

Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Cyprus: CITEA
Denmark: DI ITEK, IT-BRANCHEN
Estonia: ITL
Finland: FFTI
France: AFDEL, AFNUM, Force Numérique
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: ICT IRELAND
Italy: ANITEC
Lithuania: INFOBALT
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK