Regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy

Fields marked with * are mandatory.

Objectives and General Information

The views expressed in this public consultation document may not be interpreted as stating an official position of the European Commission. All definitions provided in this document are strictly for the purposes of this public consultation and are without prejudice to differing definitions the Commission may use under current or future EU law, including any revision of the definitions by the Commission concerning the same subject matters.

You are invited to read the privacy statement attached to this consultation for information on how your personal data and contribution will be dealt with.

This public consultation will close on 30 December 2015 (12 weeks from the day when all language versions have been made available).

The Commission invites all interested parties to express their views on the questions targeting relations between platform providers and holders of rights in digital content (Question starting with "[A1]"), taking account of the Commission Communication "Towards a modern, more European copyright framework" of 9 December 2015. Technical features of the questionnaire have been adapted accordingly.

Please complete this section of the public consultation before moving to other sections.

- Respondents living with disabilities can request the questionnaire in .docx format and send their replies in email to the following address: CNECT-PLATFORMS-CONSULTATION@ec.europa.eu.
- If you are an association representing several other organisations and intend to gather the views of your members by circulating the questionnaire to them, please send us a request in email and we will send you the questionnaire in .docx format. However, we ask you to introduce the aggregated answers into EU Survey. In such cases we will not consider answers submitted in other channels than EU Survey.
- If you want to submit position papers or other information in addition to the information you share with the Commission in EU Survey, please send them to CNECT-PLATFORMS-CONSULTATION@ec.europa.eu and make reference to the "Case Id" displayed after you have concluded the online questionnaire. This helps the Commission to properly identify your contribution.
- Given the volume of this consultation, you may wish to download a PDF version before responding to the survey online. The PDF version includes all possible questions. When you fill the survey in online, you will not see all of the questions; only those applicable to your chosen respondent category and to other choices made when you answer previous questions.

* Please indicate your role for the purpose of this consultation

- ( ) An individual citizen
- ( ) An association or trade organization representing consumers
- ( ) An association or trade organization representing businesses
- (•) An association or trade organization representing civil society
- ( ) An online platform
- ( ) A business, including suppliers using an online platform to provide services
- ( ) A public authority
- ( ) A research institution or Think tank
- ( ) Other

* Please indicate your country of residence

Non-EU country

* Please specify the Non-EU country

United States

* Please provide your contact information (name, address and e-mail address)

Center for Democracy & Technology
1634 I Street NW, Suite 1100
Washington, DC 20006
UNITED STATES
Tel: (+1)2026379800
Email: jjeppesen@cdt.org

* Is your organisation registered in the Transparency Register of the European Commission and the European Parliament?

Note: If you are not answering this questionnaire as an individual, please register in the Transparency Register. If your organisation/institution responds without being registered, the Commission will consider its input as that of an individual and will publish it as such.

- (•) Yes
- ( ) No
- ( ) Non-applicable

* Please indicate your organisation's registration number in the Transparency Register

57305017757-64

If you are an economic operator, please enter the NACE code, which best describes the economic activity you conduct. You can find here the NACE classification.

Text of 3 to 5 characters will be accepted

The Statistical classification of economic activities in the European Community, abbreviated as NACE, is the classification of economic activities in the European Union (EU).

* I object the publication of my personal data

- ( ) Yes
- (•) No

Online platforms

SOCIAL AND ECONOMIC ROLE OF ONLINE PLATFORMS

Do you agree with the definition of "**Online platform**" as provided below?

"Online platform" refers to an undertaking operating in two (or multi)-sided markets, which uses the Internet to enable interactions between two or more distinct but interdependent groups of users so as to generate value for at least one of the groups. Certain platforms also qualify as Intermediary service providers.

Typical examples include general internet search engines (e.g. Google, Bing), specialised search tools (e.g. Google Shopping, Kelkoo, Twenga, Google Local, TripAdvisor, Yelp,), location-based business directories or some maps (e.g. Google or Bing Maps), news aggregators (e.g. Google News), online market places (e.g. Amazon, eBay, Allegro, Booking.com), audio-visual and music platforms (e.g. Deezer, Spotify, Netflix, Canal play, Apple TV), video sharing platforms (e.g. YouTube, Dailymotion), payment systems (e.g. PayPal, Apple Pay), social networks (e.g. Facebook, Linkedin, Twitter, Tuenti), app stores (e.g. Apple App Store, Google Play) or collaborative economy platforms (e.g. AirBnB, Uber, Taskrabbit, Bla-bla car). Internet access providers fall outside the scope of this definition.

No

* Please explain how you would change the definition

1000 character(s) maximum

The definition is so broad that it captures just about any website and any online application in operation in Europe and globally. Also, just about any traditionally offline business can be considered to be a two- or multisided market (e.g.restaurants, hotels, car companies, newspapers, airports, stock exchanges, banks). Today, nearly all businesses run websites and are to some extent software-based and would thus fall under the definition. The all-encompassing nature of the definition means that it is not helpful to delineate a set of companies or business models as a category that would determine whether certain regulation does or does not apply. CDT does not want to propose an alternative definition, as it is not clear that one is required. The companies the Commission points to as examples of platforms are already covered by EU rules on data and consumer protection, competition as well as regulation on travel, tourism, music distribution, electronic commerce, etc.

What do you consider to be the key advantages of using online platforms?

Online platforms…

- [x] make information more accessible
- [x] make communication and interaction easier
- [ ] increase choice of products and services
- [ ] create more transparent prices and the possibility to compare offers
- [ ] increase trust between peers by providing trust mechanisms (i.e. ratings, reviews, etc.)
- [ ] lower prices for products and services
- [ ] lower the cost of reaching customers for suppliers
- [ ] help with matching supply and demand
- [ ] create new markets or business opportunities
- [ ] help in complying with obligations in cross-border sales
- [ ] help to share resources and improve resource-allocation
- [x] others:

* Please specify:

100 character(s) maximum

Internet intermediaries, with strong liability protections, are important enablers of free speech.

Have you encountered, or are you aware of problems faced by **consumers** or **suppliers** when dealing with online platforms?

"Consumer" is any natural person using an online platform for purposes outside the person's trade, business, craft or profession.

"Supplier" is any trader or non-professional individual that uses online platforms to provide services to third parties both under their own brand (name) and under the platform's brand.

- ○ Yes
- ○ No
- ◉ I don't know

TRANSPARENCY OF ONLINE PLATFORMS

Do you think that online platforms should ensure, as regards their own activities and those of the **traders** that use them, more transparency in relation to:

a) information required by consumer law (e.g. the contact details of the supplier, the main characteristics of products, the total price including delivery charges, and consumers' rights, such as the right of withdrawal)?

"Trader" is any natural or legal person using an online platform for business or professional purposes. Traders are in particular subject to EU consumer law in their relations with consumers.

- ◉ Yes
- ○ No
- ○ I don't know

b) information in response to a search query by the user, in particular if the displayed results are sponsored or not?

- ◉ Yes
- ○ No
- ○ I don't know

c) information on who the actual supplier is, offering products or services on the platform

- ○ Yes
- ○ No
- ◉ I don't know

d) information to discourage misleading marketing by professional suppliers (traders), including fake reviews?

- ◉ Yes
- ○ No
- ○ I don't know

e) is there any additional information that, in your opinion, online platforms should be obliged to display?

500 character(s) maximum

Businesses in any sector should provide information that allows consumers and customers to make informed decisions about whether and how to use the services they provide. Consumer protection rules include obligations to provide such information. Such obligations apply to all companies, regardless of whether they operate wholly/partly/not online. Successful companies provide better information than required by law. Regulators should intervene if companies fail to meet the requirements of the law.

Have you experienced that information displayed by the platform (e.g. advertising) has been adapted to the interest or recognisable characteristics of the user?

- (•) Yes
- ( ) No
- ( ) I don't know

Do you find the information provided by online platforms on their terms of use sufficient and easy-to-understand?

- ( ) Yes
- (•) No

* What type of additional information and in what format would you find useful? Please briefly explain your response and share any best practice you are aware of.

1500 character(s) maximum

This question is difficult to answer in a meaningful way because it implies that all 'online platforms' are similar in the way they provide information about terms of use. This is arguably not the case, given the broad definition of the concept.

However, as a general matter, there are many examples of companies – both online and offline – whose terms of use are difficult to access. Surveys confirm that many users and consumers do not read terms of use and privacy policies because they are too long and complex to understand. Rather, consumers choose to either trust and use a service or not. This is not a satisfactory position from a consumer perspective.

As concerns best practices, CDT hesitates to endorse any one approach. There are ongoing efforts by research institutions, regulators and business groups to develop and improve transparency for consumers. As concerns transparency of privacy policies, new approaches are likely to emerge with the adoption and subsequent implementation of the General Data Protection Regulation. See below.

Do you find reputation systems (e.g. ratings, reviews, certifications, trustmarks) and other trust mechanisms operated by online platforms are generally reliable?

- Yes
- No
- I don't know

What are the main benefits and drawbacks of reputation systems and other trust mechanisms operated by online platforms? Please describe their main benefits and drawbacks.

1500 character(s) maximum

```
CDT has not done substantive work on reputation systems and other trust
mechanisms.
```

USE OF INFORMATION BY ONLINE PLATFORMS

In your view, do online platforms provide sufficient and accessible information with regard to:

a) the personal and non-personal data they collect?

- Yes
- No
- I don't know

b) what use is made of the personal and non-personal data collected, including trading of the data to other platforms and actors in the Internet economy?

- Yes
- No
- I don't know

c) adapting prices, for instance dynamic pricing and conditions in function of data gathered on the buyer (both consumer and trader)?

- Yes
- No
- I don't know

Please explain your choice and share any best practices that you are aware of.

1500 character(s) maximum

Under the forthcoming General Data Protection Regulation and under the current Data Protection Directive, data controllers – including those with an online presence and as such included in the definition of online platforms – must provide a comprehensive privacy notice to data subjects describing how the entity collects, uses, retains and discloses personal data. Informed consent is also one of the cornerstones of the US Fair Information Practice Principles.

Informed consent is considered to be an effective means of respecting individuals as autonomous decision makers. However, the fact that a privacy disclosure is provided does not in itself protect and support autonomy. Individuals must first understand how their assent affects them. Given that most data subjects neither read nor understand privacy policies and given further the complexities of online platforms' data practices, most of these notices do not provide data subjects with a comprehensive understanding of the opportunities and risks afforded to them and society at large.

Thus, while some disclosures might do a good job in enabling the data subject to make an autonomous decision, most efforts in this regard are formalistic and do not lead to an informed individual. More work needs to be done to make the data practices of data controllers, including platforms, transparent to its users.

Please share your general comments or ideas regarding the use of information by online platforms

3000 character(s) maximum

As discussed above, we believe that all companies, whether operating on- and/or offline, and operating and providing services in the EU, including those captured by the Commission's definition of 'online platform', are and should be subject to the forthcoming General Data Protection Regulation. Initiatives developed under the Digital Single Market Strategy should be in compliance with this legislation. Robust privacy protections do not stand in conflict with a successful digital economy serving all members of society. In fact, we believe that those protections as well as mechanisms to ensure the fair processing of all data, including aggregated and anonymous data, are essential for building citizens' trust and harnessing the full potential of a data-driven society.

Similarly, we would also like to emphasise that we do not see any inherent conflict between promoting the free flow of data in a Digital Single Market and protecting the privacy rights of individuals. Both are essential for achieving the full economic potential while ensuring and working toward a free and equitable society.

RELATIONS BETWEEN PLATFORMS AND SUPPLIERS/TRADERS/APPLICATION DEVELOPERS OR HOLDERS OF RIGHTS IN DIGITAL CONTENT

[A1] Are you a holder of rights in digital content protected by copyright, which is used on an online platform?

- (●) Yes
- ( ) No

As a holder of rights in digital content protected by copyright have you faced any of the following circumstances:

An online platform such as a video sharing website or an online content aggregator uses my protected works online without having asked for my authorisation.

- ( ) Yes
- (●) No

An online platform such as a video sharing website or a content aggregator refuses to enter into or negotiate licensing agreements with me.

- ( ) Yes
- (●) No

An online platform such as a video sharing website or a content aggregator is willing to enter into a licensing agreement on terms that I consider unfair.

- ( ) Yes
- (●) No

An online platform uses my protected works but claims it is a hosting provider under Article 14 of the E-Commerce Directive in order to refuse to negotiate a licence or to do so under their own terms.

- ( ) Yes
- (●) No

Is there a room for improvement in the relation between platforms and suppliers using the services of platforms?

- (●) No, the present situation is satisfactory.
- ( ) Yes, through market dynamics.
- ( ) Yes, through self-regulatory measures (codes of conducts / promotion of best practices).
- ( ) Yes, through regulatory measures.
- ( ) Yes, through the combination of the above.

Are you aware of any dispute resolution mechanisms operated by online platforms, or independent third parties on the business-to-business level mediating between platforms and their suppliers?

- ( ) Yes
- (●) No

CONSTRAINTS ON THE ABILITY OF CONSUMERS AND TRADERS TO MOVE FROM ONE PLATFORM TO ANOTHER

Do you see a need to strengthen the technical capacity of online platforms and address possible other constraints on switching freely and easily from one platform to another and move user data (e.g. emails, messages, search and order history, or customer reviews)?

- ○ Yes
- ◉ No

Should there be a mandatory requirement allowing non-personal data to be easily extracted and moved between comparable online services?

- ○ Yes
- ◉ No

Please share your general comments or ideas regarding the ability of consumers and traders to move from one platform to another

3000 character(s) maximum

Many types of companies, offline and online, seek to create incentives for users/customers to keep using their products/services. Examples of such incentives are loyalty programmes, frequent flyer plans, bonus schemes, bundling of services, volume rebates, etc.

Some companies impose restrictions on switching to alternative providers. A contract may, for example, include a notice period for termination, depending on what applicable consumer and sectoral regulation allows. Other companies may seek to attract customers by not imposing such conditions, and by making it particularly easy to switch provider. There are many ways for companies to differentiate their offerings from those of competitors, and the ease of shifting provider by making it easy to move data such as those in the example, is one of them. As concerns personal data, the forthcoming General Data Protection Regulation will include provisions on portability of personal data. All data controllers, including those covered by the 'online platforms' definition, must comply with these requirements.

In general, companies should provide a high level of transparency about their offerings, including about any restrictions on switching providers, and the ease with which the customer can move data to an alternative provider.

If a company has market dominance, regulators may impose limitations on its conduct. Such limitations may include obligations to make switching easy and/or restrict its use of some types customer retention schemes. Such obligations and restrictions are also applied in certain types of sector-specific regulation. As a general matter, such obligations may be legitimate where there is evidence of market failure, and where they are deemed necessary to ensure competition and consumer benefit.

European competition law and jurisprudence set the framework for how regulators deal with complaints related to market dominance, among other things. The principles of European competition law apply, and are enforced, both in the offline and online environment.

ACCESS TO DATA

As a trader or a consumer using the services of online platforms did you experience any of the following problems related to the access of data?

a) unexpectedly changing conditions of accessing the services of the platforms

- ○ Yes
- ◉ No

b) unexpectedly changing conditions of accessing the Application Programming Interface of the platform

- ○ Yes
- ◉ No

c) unexpectedly changing conditions of accessing the data you shared with or stored on the platform

- ○ Yes
- ◉ No

d) discriminatory treatment in accessing data on the platform

- ○ Yes
- ◉ No

Would a rating scheme, issued by an independent agency on certain aspects of the platforms' activities, improve the situation?

- ○ Yes
- ◉ No

* Please explain your answer

1500 character(s) maximum

As an organisation, CDT has not had experiences such as those outlined in the questions, and we have not done research in this area. As concerns the notion of an independent agency, we would note that the companies included in the proposed definition of 'platforms' are subject to oversight by competition authorities, consumer authorities and 'watchdogs', data protection regulators, and sectoral bodies (for example, in the travel or transport sector). With the broad definition of 'platforms', it is difficult to imagine how any one agency would be able to provide information and transparency across all sectors of business.

Please share your general comments or ideas regarding access to data on online platforms

3000 character(s) maximum

Where personal data is concerned, the Data Protection Directive applies until it is replaced by the General Data Protection Regulation. As mentioned, companies defined as online platforms are covered by this legislation.

Tackling illegal content online and the liability of online intermediaries

Please indicate your role in the context of this set of questions

Terms used for the purposes of this consultation:

"Illegal content"

Corresponds to the term "illegal activity or information" used in Article 14 of the E-commerce Directive. The directive does not further specify this term. It may be understood in a wide sense so as to include any infringement of applicable EU or national laws and regulations. This could for instance include defamation, terrorism related content, IPR infringements, child abuse content, consumer rights infringements, or incitement to hatred or violence on the basis of race, origin, religion, gender, sexual orientation, malware, illegal online gambling, selling illegal medicines, selling unsafe products.

"Hosting"

According to Article 14 of the E-commerce Directive, hosting is the “storage of (content) that has been provided by the user of an online service”. It may for instance be storage of websites on servers. It may also include the services offered by online market places, referencing services and social networks.

"Notice"

Any communication to a hosting service provider that gives the latter knowledge of a particular item of illegal content that it transmits or stores and therefore creates an obligation for it to act expeditiously by removing the illegal content or disabling/blocking access to it.. Such an obligation only arises if the notice provides the internet hosting service provider with actual awareness or knowledge of illegal content.

"Notice provider"

Anyone (a natural or legal person) that informs a hosting service provider about illegal content on the internet. It may for instance be an individual citizen, a hotline or a holder of intellectual property rights. In certain cases it may also include public authorities.

"Provider of content"

In the context of a hosting service the content is initially provided by the user of that service. A provider of content is for instance someone who posts a comment on a social network site or uploads a video on a video sharing site.

- ○ individual user
- ◉ content provider
- ○ notice provider
- ○ intermediary
- ○ none of the above

Have you encountered situations suggesting that the liability regime introduced in Section IV of the E-commerce Directive (art. 12-15) has proven not fit for purpose or has negatively affected market level playing field?

- ○ Yes
- ◉ No

Do you think that the concept of a "mere technical, automatic and passive nature" of information transmission by information society service providers provided under recital 42 of the ECD is sufficiently clear to be interpreted and applied in a homogeneous way, having in mind the growing involvement in content distribution by some online intermediaries, e.g.: video sharing websites?

- ◉ Yes
- ○ No
- ○ I don't know

Please explain your answer.

1500 character(s) maximum

This portion of Recital 42 describes in full that “this activity is of a mere technical, automatic and passive nature, which implies the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.” The threat to freedom of expression created by intermediary liability laws stems from the inherent challenges of holding an intermediary responsible for content of which it is not the author and to which it did not materially contribute - that is, content of which it “has neither knowledge nor control.”

Intermediaries can, of course, be content providers in their own right, and, as for any speaker, it is appropriate to hold them liable for content which they themselves have created. But “content distribution” is not content creation, and holding intermediaries liable for content which is accessed or aggregated through their systems is another form of intermediary liability and will yield the same chilling effects on individual speech and innovation.

Mere conduit/caching/hosting describe the activities that are undertaken by a service provider. However, new business models and services have appeared since the adopting of the E-commerce Directive. For instance, some cloud service providers might also be covered under hosting services e.g. pure data storage. Other cloud-based services, as processing, might fall under a different category or not fit correctly into any of the existing ones. The same can apply to linking services and search engines, where there has been some diverging case-law at national level. Do you think that further categories of intermediary services should be established, besides mere conduit/caching/hosting and/or should the existing categories be clarified?

- ○ Yes
- ◉ No

On the "notice"

Do you consider that different categories of illegal content require different policy approaches as regards notice-and-action procedures, and in particular different requirements as regards the content of the notice?

- (•) Yes
- ( ) No

Do you think that any of the following categories of illegal content requires a specific approach:

- [ ] Illegal offer of goods and services (e.g. illegal arms, fake medicines, dangerous products, unauthorised gambling services etc.)
- [ ] Illegal promotion of goods and services
- [ ] Content facilitating phishing, pharming or hacking
- [x] Infringements of intellectual property rights (e.g. copyright and related rights, trademarks)
- [ ] Infringement of consumer protection rules, such as fraudulent or misleading offers
- [ ] Infringement of safety and security requirements
- [ ] Racist and xenophobic speech
- [ ] Homophobic and other kinds of hate speech
- [x] Child abuse content
- [ ] Terrorism-related content (e.g. content inciting the commitment of terrorist offences and training material)
- [ ] Defamation
- [ ] Other:

Please explain what approach you would see fit for the relevant category.

1000 character(s) maximum

Certain types of illegal content can to some extent be dealt with by technological means. For example, many online service providers use programs that compare hashes of uploaded images to databases of hashes of previously identified child abuse content. In a similar way, some video-sharing sites use technology that matches content against databases of copyrighted material submitted by right holders to enable rapid restriction. It is important to note, however, that technological solutions inevitably carry risks of abuse and can excessively limit individuals' ability to post lawful content. For many types of content, such as alleged defamation or hate speech, human intervention to conduct subjective analysis is typically necessary to determine the legality of content in the context in which it was posted. This type of analysis is most properly conducted by a court.

On the "action"

Should the content providers be given the opportunity to give their views to the hosting service provider on the alleged illegality of the content?

- (•) Yes
- ( ) No

* Please explain your answer

1500 character(s) maximum

If content is challenged as illegal in court, the speaker/creator of the content will have the opportunity to defend herself and the legality of her speech. This is an essential feature of due process. Generally, a court should be involved in the determination of whether content is illegal (as opposed to violating an intermediary's Terms of Service).

If, alternately, a person's speech has been challenged as illegal directly to an intermediary, this should only occur in a framework that gives the speaker the opportunity to file a counter-notice and defend the lawfulness of her speech. It is crucial that the protection for liability for the intermediary not depend on whether it takes the content down - this will make it almost certain that the intermediary removes the speech, regardless of the strength of the speaker's counterclaim.

Rather, if an intermediary receives a notice of alleged unlawfulness of a certain piece of content from a private individual (e.g., a copyright holder) and takes down that content, the intermediary should inform the original poster of the content about its removal and should be protected from liability for restoring the content if it receives a counter-notice from the original poster. In general, users whose content is removed by an intermediary, whether due to a court-order or a notice/content-flag from a third party, should be informed that their speech has been restricted and given the opportunity to appeal that decision.

If you consider that this should only apply for some kinds of illegal content, please indicate which one(s)

1500 character(s) maximum

Should action taken by hosting service providers remain effective over time ("take down and stay down" principle)?

- ( ) Yes
- (•) No

Please explain

We must emphasise that any concept of “take down and stay down” as a required action would necessarily oblige intermediaries to monitor the content on their services, in direct conflict with Article 15 of the ECD. The prohibition on monitoring obligations has been an essential protection for the development of sites and services that host individual speech. A monitoring obligation would create a massive burden for large services that handle vast quantities of content every day; it would also stifle smaller competitors from ever getting off the ground.

On duties of care for online intermediaries:

Recital 48 of the Ecommerce Directive establishes that "[t]his Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities". Moreover, Article 16 of the same Directive calls on Member States and the Commission to encourage the "drawing up of codes of conduct at Community level by trade, professional and consumer associations or organisations designed to contribute to the proper implementation of Articles 5 to 15". At the same time, however, Article 15 sets out a prohibition to impose "a general obligation to monitor".

(For online intermediaries): Have you put in place voluntary or proactive measures to remove certain categories of illegal content from your system?

- ○ Yes
- ○ No

Do you see a need to impose specific duties of care for certain categories of illegal content?

- ○ Yes
- ◉ No
- ○ I don't know

Please specify for which categories of content you would establish such an obligation.

1500 character(s) maximum

See general comments below

Please specify for which categories of intermediary you would establish such an obligation

1500 character(s) maximum

See general comments below

Please specify what types of actions could be covered by such an obligation

1500 character(s) maximum

See general comments below

Do you see a need for more transparency on the intermediaries' content restriction policies and practices (including the number of notices received as well as their main content and the results of the actions taken following the notices)?

- (●) Yes
- ( ) No

Should this obligation be limited to those hosting service providers, which receive a sizeable amount of notices per year (e.g. more than 1000)?

- ( ) Yes
- (●) No

Do you think that online intermediaries should have a specific service to facilitate contact with national authorities for the fastest possible notice and removal of illegal contents that constitute a threat for e.g. public security or fight against terrorism?

- ( ) Yes
- (●) No

Please share your general comments or ideas regarding the liability of online intermediaries and the topics addressed in this section of the questionnaire.

5000 character(s) maximum

Intermediary liability protections, which shield the hosts, conduits, and other services from legal responsibility for content authored by third parties, are a foundational requirement for the protection and promotion of freedom of expression online. This is recognised widely, by intergovernmental organisations such as the OECD and UNESCO, by the current and former Special Rapporteurs on the Freedom of Opinion and Expression, and by the hundreds of human rights advocates (including CDT) and others who have supported the Manila Principles. The ability for individual speakers to express themselves and to access information online depends on their access to a series of intermediaries willing to host and transmit their speech – any of which could decide to become a gatekeeper if faced with the prospect of legal sanction for their users' speech. As a starting point, we urge the Commission to remember this broad policy consensus and to retain strong protections for all Internet intermediaries from liability for content of which they are not the author, as an essential element of the Digital Single Market strategy.

Generally, CDT considers the E-Commerce Directive a solid foundation for handling the liability of online intermediaries in Europe. Rather than

introduce new categories of intermediaries, we encourage the Commission and Member States to read the current categories broadly, given the importance of the liability protections in the ECD to free expression online. Because of the pace of change of technology, any effort to further segment categories of intermediary will risk constraining innovation and will result in a law that becomes quickly irrelevant to the digital market.

Regarding the questions on notice, we caution the Commission regarding the risks to fundamental rights that come from requiring private companies to make fine-grained, subjective evaluations of the legality or illegality of many different types of content. When receipt of a notice creates for an intermediary the obligation to respond or face legal penalty themselves, the incentive for the intermediary will tend to be to block or take down content – even if the challenged material is not clearly unlawful. Notice-and-action regimes should include requirements for the proper form of a notice, including the specific URL of the challenged piece of content, as well as a requirement for the individual or entity providing the notice to describe why the challenged content is unlawful. Beyond a few very narrow categories where content may be considered manifestly unlawful, such as child sexual abuse imagery, notices of illegal content should come from courts.

Regarding the questions on “duty of care”, we note that the idea of imposing through law a “duty of care” for intermediaries related to certain types of content is indistinguishable from creating liability for intermediaries for third-party content. Special liability for a particular sort of content would create the need for intermediaries to evaluate all of the content they handle, as it will not be apparent at the outset what of user-uploaded material falls into the category of content that requires special scrutiny. We strongly urge the Commission not to support the creation of intermediary liability in the form of “duties of care”.

For the questions on transparency reporting, we note the positive work that has been accomplished by a number of leading Internet companies in publishing transparency reports regarding government demands for user data and content restriction. We urge companies to provide more information about their Terms of Service (TOS) enforcement, including, to the extent they are able, the instances of governments using TOS flagging mechanisms, rather than formal legal proceedings overseen by a court, to seek the removal of content from their services. We encourage Internet companies of all sizes to produce, on a voluntary basis, transparency reports for both government-initiated content removal and content removal under their own Terms.

Regarding the question about facilitating “the fastest possible notice and removal of illegal content”, we urge the Commission to clarify that it is essential, even in exigent circumstances, that determinations of illegality of speech are made by independent courts applying clearly articulated laws. Neither companies nor governments should seek to

facilitate expedited extralegal censorship.

Finally, we note that while the questionnaire asks respondents to identify themselves as either an “individual” or a “content provider”, the beauty of online communications is that the majority of individuals who use the Internet are themselves content providers: their photos, videos, blog posts, websites, and messages – their speech – is content provided by third parties to intermediaries for hosting and transmission. Any policy efforts in this arena must consider the consequences for individuals-as-content-providers clearly.

Data and cloud in digital ecosystems

FREE FLOW OF DATA

ON DATA LOCATION RESTRICTIONS

In the context of the free flow of data in the Union, do you in practice take measures to make a clear distinction between personal and non-personal data?

- ○ Yes
- ○ No
- ◉ Not applicable

Have restrictions on the location of data affected your strategy in doing business (e.g. limiting your choice regarding the use of certain digital technologies and services?)

- ○ Yes
- ◉ No

Do you think that there are particular reasons in relation to which data location restrictions are or should be justifiable?

- ◉ Yes
- ○ No

* What kind(s) of ground(s) do you think are justifiable?

- ☐ National security
- ☐ Public security
- ☑ Other reasons:

* Please explain

There are legitimate reasons for restricting the availability of some forms of personally identifiable or national security information in certain contexts. However, data localisation mandates are inconsistent with the borderless nature of the Internet and do not guarantee improved security. Indeed, they may do the opposite. For commercial information, there is little justification for localisation requirements.

ON DATA ACCESS AND TRANSFER

Do you think that the existing contract law framework and current contractual practices are fit for purpose to facilitate a free flow of data including sufficient and fair access to and use of data in the EU, while safeguarding fundamental interests of parties involved?

- Yes
- No

* Please explain your position

3000 character(s) maximum

SAFE HARBOR AND SURVEILLANCE

The Schrems decision exposed the need for a global dialogue regarding data flows for legitimate commercial purposes. Although contractual practices may determine the boundaries of commercial uses of that data, they do not control the interception of the data for national security or counterterrorism purposes. There is need for enhanced transparency and accountability of that interception regardless of the contractual framework in which data is exchanged by commercial entities or their customers.

CROSS BORDER PORTABILITY

The shortcomings of existing contractual practices and frameworks for a certain category of data -- online content -- led to the Commission's current proposal for a regulation on ensuring the cross-border portability of online content and services in the international market. CDT supports the proposed regulation, but notes that its aim is a relatively modest one: allowing users who have subscribed to an online content service in one Member State to access content via that service while temporarily in another Member State. The proposal does not so much remove the national silos that inhibit the creation of a vibrant digital single market as perforate those silos to allow passage of a limited subset of content under limited circumstances. CDT encourages a broader discussion of "geo-blocking" and other limitations on cross-border licensing of content. As the Commission's Digital Single

Market Strategy staff working document acknowledges, the E-Commerce Directive's country of origin principle for information society services is not in itself sufficient to address those limitations. The DSM Strategy should therefore include a thorough review of cross-border access to and use of copyright-protected content as well as a review of how information about territorial restrictions on the access and use of such content is conveyed to consumers.

HARMONISATION OF LIMITATIONS AND EXCEPTIONS

The Commission's staff working document also addressed cross-border aspects of activities related to access to knowledge, research and heritage. In doing so, the document notes that "[m]ost exceptions to copyright foreseen in European law remain optional for Member States to implement, resulting in a fragmented landscape across the EU." That fragmentation of limitations and exceptions, and the ability to override limitations and exceptions via contract, creates potential risk regarding certain cross-border uses of protected works. Harmonisation of a "floor" for limitations and exceptions will significantly facilitate the free flow of data in the Union.

CONTRACT LAW GENERALLY

Apart from the above recommendations, regulatory authorities should rely on existing EU Directives and Regulations regarding contracting practices and maintain a strong presumption against disturbing private contracts.

In order to ensure the free flow of data within the European Union, in your opinion, regulating access to, transfer and the use of non-personal data at European level is:

- ○ Necessary
- ◉ Not necessary

When non-personal data is generated by a device in an automated manner, do you think that it should be subject to specific measures (binding or non-binding) at EU level?

- ◉ Yes
- ○ No

* Which of the following aspects would merit measures?

between 1 and 4 choices

- [x] Obligation to inform the user or operator of the device that generates the data
- [ ] Attribution of the exploitation rights of the generated data to an entity (for example the person / organisation that is owner of that device)
- [ ] In case the device is embedded in a larger system or product, the obligation to share the generated data with providers of other parts of that system or with the owner / user / holder of the entire system
- [x] Other aspects:

* Please specify

There should be a clear obligation to inform the user if a device maintains tracking cookies or other traffic data. Also, if an application or service tracks a user across multiple devices, the user should be aware of that tracking.

Please share your general comments or ideas regarding data access, ownership and use

5000 character(s) maximum

ACCESS:

Data access can refer to any number of subject matters and policy challenges. In CDT's view, the General Data Protection Regulation is the better suited vehicle to address issues regarding access to personal data and data generated by a device. In general, CDT believes that transparency and accountability are core considerations regarding access to that data regardless whether it is generated or stored by an online platform, a device, a simple website, or even offline. Individuals should be able to understand the data generated by their online presence and actions. Use of this data should require consent of the data subject and service providers should be transparent about when consent is implied.

There are particular users for whom access to data poses unique challenges. CDT is encouraged to see that the Commission's recent Communication toward a modern, more European copyright framework proposes implementation of the Marrakesh Treaty to Facilitate Access to Published Works by Visually Impaired Persons and Persons with Print Disabilities. As the Commission explores measures to ensure cross-border access to online content and services, it should ensure that all Europeans can participate in that access, regardless of impairment or disability. CDT also supports proposals to improve access to out-of-commerce works and encourages a discussion of the potential expansion of the Orphan Works Directive to a greater diversity of uses and organisations.

OWNERSHIP:

Issues regarding consumers' ownership interest in their personal information or information generated by the devices they own are better addressed in the GDPR. Transparency and accountability should be touchstones for any regulatory treatment. Further, that treatment should not vary depending on the type of online platform or other content or service provider.

To the extent that "data ownership" refers to online content, CDT cautions strongly against the recognition of new rights or obligations with respect to matters such as hyperlinking or aggregation of content on the Internet. The Commission staff working document discussed the "unclear legal situation" regarding platforms that "make content available to the public without a license" and also invoked concern "about the fairness of remuneration conditions." Many organizations, including CDT, expressed concern that the staff document could presage an effort to impose licensing requirements for displaying snippets of articles in response to search queries or even simply for providing a hyperlink. Although the Commission subsequently disavowed any interest in a "hyperlink license," its recent copyright Communication states that it will explore "whether any action specific to news aggregators is needed, including intervening on rights." Attempts to legislate and license so-called ancillary rights at the member-state level have been unpopular and unsuccessful. Imposing such rights across the EU will not facilitate the advancement of a digital single market. It will merely limit EU citizens' ability to access and share information, as well as their ability to use online platforms and the Internet generally to communicate with one another and create their own original content.

Finally, the staff working document generally calls for improvements in the enforcement of IP rights. The recently announced consultation to assess the functioning of the directive on the enforcement of intellectual property rights (IPRED) is a more appropriate forum in which to discuss IP enforcement matters. In any context, however, it is essential to maintain the E-Commerce Directive's core tenet that intermediaries do not have a general duty to monitor content and activity by third parties. Such obligations would fall hardest on the small firms offering innovative services that are the engine of the digital economy. Moreover, such obligations would chill the free expression of EU citizens who rely on online platforms and other Internet intermediaries to create and communicate their ideas.

USE

The objective announced in the Commission's copyright communication to increase the level of harmonisation of limitations and exceptions will contribute to lawful uses of data that facilitate the growth of the digital single market. Pursuing this objective, the Commission should strive toward greater beneficial uses of works rather than incursions on exceptions (such as the "panorama exception") that are already

well-established in Member States.

The Commission also should consider extending its proposed exception for text and data mining for scientific research purposes beyond the entities falling within the scope of "public research organisations." Regardless of who conducts the research, such transformative uses of works fulfill important public interest objectives while having a minimal impact on the market for the works.

ON DATA MARKETS

What regulatory constraints hold back the development of data markets in Europe and how could the EU encourage the development of such markets?

3000 character(s) maximum

CDT understands "data markets" to refer to commercial cloud computing generally. The most important steps the EU could take to encourage the development of data markets are providing clear liability protections for intermediaries, harmonising copyright limitations and exceptions, and avoiding technology- or service-specific regulatory mandates.

Much of the vibrancy of the cloud-based economy in the United States flows from the clarity of Section 230 of the Communications Act, which states generally that the providers of hosting, caching, or conduit services are not responsible for third-party content that they transmit, cache, or host. That legal clarity allows firms to undertake projects and offer services that would be impossible were they required to scrutinise every scrap of third-party data for liability risk.

The E-Commerce Directive accomplishes much of the same function by preventing Member States from imposing monitoring obligations on intermediaries. However, it allows for the imposition of duties of care on hosting services. It is essential that the Digital Single Market Strategy does not heap new duties of care on "data markets" or other subsets of cloud-based services, effectively imposing a duty to monitor. Regulations that make distinctions between particular categories of cloud service providers will hamper the growth of data markets. For the most part, the ECD's distinctions between caching, hosting, and serving as a mere conduit are clear and administrable. By contrast, tailoring regulations to "online platforms," "essential platforms," or other specific combinations or scales of services will incentivise data market participants to craft their offerings to take advantage of or avoid particular regulatory consequences, rather than basing their offerings on user demand and technological possibility. The Commission should take care to avoid that outcome.

Clear and harmonised copyright limitations and exceptions with respect to user-generated content would facilitate the growth of EU-wide data markets by ensuring that the rules that apply to a particular cloud service provider do not depend on the locations of the user or the server hosting user-generated content. Uniform treatment will facilitate new EU-based participants in data markets, achieving the scale necessary to compete with established cloud service providers.

ON ACCESS TO OPEN DATA

Do you think more could be done to open up public sector data for re-use in addition to the recently revised EU legislation (Directive 2013/37/EU)?

Open by default means: Establish an expectation that all government data be published and made openly re-usable by default, while recognising that there are legitimate reasons why some data cannot be released.

- [x] Introducing the principle of 'open by default'[1]
- [ ] Licensing of 'Open Data': help persons/ organisations wishing to re-use public sector information (e.g., Standard European License)
- [x] Further expanding the scope of the Directive (e.g. to include public service broadcasters, public undertakings);
- [x] Improving interoperability (e.g., common data formats);
- [x] Further limiting the possibility to charge for re-use of public sector information
- [x] Remedies available to potential re-users against unfavourable decisions
- [ ] Other aspects?

Do you think that there is a case for the opening up of data held by private entities to promote its re-use by public and/or private sector, while respecting the existing provisions on data protection?

- (•) Yes
- ( ) No

* Under what conditions?

- [x] in case it is in the public interest
- [ ] for non-commercial purposes (e.g. research)
- [x] other conditions

* Please explain

3000 character(s) maximum

Where the public contributes to the funding or development of data that is subsequently held by private entities, there is a strong case to be made for opening up that data to the public. Further, if privately held data supports the creation of commercial standards that are incorporated into law, such as building codes, there is a strong case to be made for public access to both the standard and the underlying data that led to its incorporation in law. When such data is made available to the public, it should be available in an open, machine-readable format.

ON ACCESS AND REUSE OF (NON-PERSONAL) SCIENTIFIC DATA

Do you think that data generated by research is sufficiently, findable, accessible identifiable, and re-usable enough?

- ( ) Yes
- (•) No

* Why not? What do you think could be done to make data generated by research more effectively re-usable?

3000 character(s) maximum

The current state of copyright law regarding text and data mining inhibits effective reuse of data generated by research. Both the Parliament's report on the harmonisation of certain aspects of copyright and related rights and the Commission's more recent copyright communication recognize text and data mining as an area in need of further clarification. Further, the DSM Strategy staff working document notes the high international mobility of EU researchers. In view of that mobility, an effective EU-wide exception for text and data mining is necessary.

CDT is encouraged that the Commission's copyright communication acknowledges that the "lack of a clear EU provision on TDM for scientific research purposes creates uncertainties in the research community" that harms the EU's competitiveness and scientific leadership. At the same time, we are concerned that the Communication contemplates an exception limited to "public interest research organisations." Much valuable research takes place outside of the institutional setting. Some research initiatives are also "crowdsourced," involving multiple heterogenous organisations and individuals. An identity-based restriction on a texts and data mining exception would exclude that research and the numerous benefits that come with it.

Do you agree with a default policy which would make data generated by publicly funded research available through open access?

- (•) Yes
- ( ) No

ON LIABILITY IN RELATION TO THE FREE FLOW OF DATA AND THE INTERNET OF THINGS

As a provider/user of Internet of Things (IoT) and/or data driven services and connected tangible devices, have you ever encountered or do you anticipate problems stemming from either an unclear liability regime/non –existence of a clear-cut liability regime?

The "Internet of Things" is an ecosystem of physical objects that contain embedded technology to sense their internal statuses and communicate or interact with the external environment. Basically, Internet of things is the rapidly growing network of everyday objects—eyeglasses, cars, thermostats—made smart with sensors and internet addresses that create a network of everyday objects that communicate with one another, with the eventual capability to take actions on behalf of users.

- ( ) Yes
- (•) No
- ( ) I don't know

If you did not find the legal framework satisfactory, does this affect in any way your use of these services and tangible goods or your trust in them?

- ○ Yes
- ◉ No
- ○ I don't know

Do you think that the existing legal framework (laws, or guidelines or contractual practices) is fit for purpose in addressing liability issues of IoT or / and Data driven services and connected tangible goods?

- ◉ Yes
- ○ No
- ○ I don't know

Is the legal framework future proof? Please explain, using examples.

3000 character(s) maximum

The existing legal framework is "future proof" in the sense that it is not determined by particular technologies or device types. Contract and agency law are continually evolving and flexible enough to accommodate new technological developments. Contracts themselves are easily adjusted to balance rights and obligations among multiple entities. As hardware and connectivity become less expensive and more ubiquitous, the number of Internet-connected devices is proliferating at a staggering pace. Attempts at regulating particular classes of devices or technologies are unlikely to keep up with the rate of introduction of new entrants to the Internet of Things, which now includes everything from automobiles to jump ropes.

This is not to say that the Internet of Things is an area that should be wholly free of regulatory scrutiny. When a device manufacturer or seller makes representations regarding the security of a device, it should be held accountable for those representations. Similarly, privacy protections are more, not less, important in the Internet of Things than they are in the Internet generally. However, existing frameworks such as the Regulation on Consumer Protection Cooperation and the General Data Protection Regulations are the appropriate vehicles for addressing regulatory concerns in the Internet of Things. An IoT-specific regulatory framework is likely to be overly prescriptive and outmoded before it is implemented.

Please explain what, in your view, should be the liability regime for these services and connected tangible goods to increase your trust and confidence in them?

3000 character(s) maximum

As stated above, the liability regime for the services and goods that make up the Internet of Things should depend on laws of general application that are not technology-specific and do not impose technological mandates.

As a user of IoT and/or data driven services and connected tangible devices, does the present legal framework for liability of providers impact your confidence and trust in those services and connected tangible goods?

- Yes
- (•) No
- I don't know

In order to ensure the roll-out of IoT and the free flow of data, should liability issues of these services and connected tangible goods be addressed at EU level?

- Yes
- (•) No
- I don't know

ON OPEN SERVICE PLATFORMS

What are in your opinion the socio-economic and innovation advantages of open versus closed service platforms and what regulatory or other policy initiatives do you propose to accelerate the emergence and take-up of open service platforms?

3000 character(s) maximum

We understand "open service platforms" to mean those that rely on open, as opposed to proprietary, standards or platforms that allow for broad participation without payment, pre-screening or specific eligibility requirements. The chief advantages of such standards are interoperability, enhanced value via network effects, and improved security.

Open platforms encompass a broad range of products and services. For example, Wikipedia is an open service platform in the sense that it allows almost anyone to access, create, and edit articles on nearly any topic. The benefits of such platforms are manifest. Wikipedia contains far more information than any compendium of information put together by a closed group of authors or editors. And although it certainly is not free to manage and host that content, the Wikimedia Foundation is able to offer Wikipedia to the entire Internet-connected public without charge. And Wikipedia relies on the hypertext markup language and hypertext transfer protocol, which are themselves open standards.

As Wikipedia demonstrates, network effects are a principal benefit of open service platforms. With every additional article or improvement to an existing article, Wikipedia becomes more valuable. And because the resource is freely available, authors with a genuine interest in explaining a particular subject are motivated to do so through Wikipedia. Network effects also contribute to the value of an open platform or standard. For example, the number and variety of devices that run a particular operating system may encourage individuals and entities to develop applications that run on that operating system. And the more applications available via that operating system, the greater the value of the operating system itself.

Enhanced security is an additional benefit of open standards and, potentially, open service platforms. The more accessible the source code is for any particular program, the easier it is to identify and correct potential security vulnerabilities. "Security by obscurity," which relies on secrecy and nondisclosure to prevent exploitation of security vulnerabilities is not a viable cybersecurity strategy.

To accelerate the emergence and take-up of open service platforms, the EU should explore innovative licensing regimes, such as Creative Commons licensing, to encourage the disclosure, sharing, and modification of standards and source code. The EU also should encourage Member States to make public information and public resources accessible via open standard formats.

PERSONAL DATA MANAGEMENT SYSTEMS

The following questions address the issue whether technical innovations should be promoted and further developed in order to improve transparency and implement efficiently the requirements for lawful processing of personal data, in compliance with the current and future EU data protection legal framework. Such innovations can take the form of 'personal data cloud spaces' or trusted frameworks and are often referred to as 'personal data banks/stores/vaults'.

Do you think that technical innovations, such as personal data spaces, should be promoted to improve transparency in compliance with the current and future EU data protection legal framework? Such innovations can take the form of 'personal data cloud spaces' or trusted frameworks and are often referred to as 'personal data banks/stores/vaults'?

- ○ Yes
- ◉ No
- ○ I don't know

EUROPEAN CLOUD INITIATIVE

What are the key elements for ensuring trust in the use of cloud computing services by European businesses and citizens

"Cloud computing" is a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. Examples of such resources include: servers, operating systems, networks, software, applications, and storage equipment.

- ☑ Reducing regulatory differences between Member States
- ☐ Standards, certification schemes, quality labels or seals
- ☑ Use of the cloud by public institutions
- ☑ Investment by the European private sector in secure, reliable and high-quality cloud infrastructures

As a (potential) user of cloud computing services, do you think cloud service providers are sufficiently transparent on the security and protection of users' data regarding the services they provide?

- ○ Yes
- ◉ No
- ○ Not applicable

* What information relevant to the security and protection of users' data do you think cloud service providers should provide?

As with all providers of online services, accountability and transparency with respect to user privacy and data security practices are essential for cloud service providers. The breadth of this question makes providing an exhaustive list of relevant information regarding those practices a challenging and perhaps unproductive exercise. Online service providers should provide enough information regarding security and privacy practices to allow users to make informed choices among competing providers. Further, CDT encourages providers to use encryption to protect their users and to provide information about their encryption practices.

As a (potential) user of cloud computing services, do you think cloud service providers are sufficiently transparent on the security and protection of users' data regarding the services they provide?

- ( ) Yes
- ( ) No
- (•) Not applicable

As a (potential) user of cloud computing services, do you agree that existing contractual practices ensure a fair and balanced allocation of legal and technical risks between cloud users and cloud service providers?

- (•) Yes
- ( ) No

What would be the benefit of cloud computing services interacting with each other (ensuring interoperability)

- [x] Economic benefits
- [x] Improved trust
- [ ] Others:

What would be the benefit of guaranteeing the portability of data, including at European level, between different providers of cloud services

- [ ] Economic benefits
- [ ] Improved trust
- [ ] Others:

Have you encountered any of the following contractual practices in relation to cloud based services? In your view, to what extent could those practices hamper the uptake of cloud based services? Please explain your reasoning.

	Never (Y[es] or N[no])	Sometimes (Y / N)	Often (Y / N)	Always (Y / N)	Why (1500 characters max.)?
Difficulties with negotiating contractual terms and conditions for cloud services stemming from uneven bargaining power of the parties and/or undefined standards					
Limitations as regards the possibility to switch between different cloud service providers					
Possibility for the supplier to unilaterally modify the cloud service					
Far reaching limitations of the supplier's liability for malfunctioning cloud services (including depriving the user of key remedies)					
Other (please explain)					

What are the main benefits of a specific European Open Science Cloud which would facilitate access and make publicly funded research data re-useable?

- [x] Making Science more reliable by better quality assurance of the data
- [x] Making Science more efficient by better sharing of resources at national and international level
- [x] Making Science more efficient by leading faster to scientific discoveries and insights
- [x] Creating economic benefits through better access to data by economic operators
- [x] Making Science more responsive to quickly tackle societal challenges
- [ ] Others

Would model contracts for cloud service providers be a useful tool for building trust in cloud services?

- ( ) Yes
- (•) No

Would your answer differ for consumer and commercial (i.e. business to business) cloud contracts?

- (•) Yes
- ( ) No

Please share your general comments or ideas regarding data, cloud computing and the topics addressed in this section of the questionnaire

5000 character(s) maximum

DATA ACCESS, OWNERSHIP, AND USE

Policy questions regarding personal data are best addressed through the General Data Protection Regulation. With respect to data generally, and works protected by copyright specifically, CDT strongly supports measures to improve cross-border portability. We consider the existing proposed regulation to be a promising start to that effort but by no means a comprehensive solution. Access to data necessarily includes accessibility of data. CDT therefore strongly supports ratification of the Marrakesh Treaty.

Data ownership and use also implicate critical questions regarding copyright protections as well as limitations and exceptions. Creation of EU-wide ancillary rights would be a step backward for a vibrant digital economy in Europe. The transactional costs entailed in clearing rights necessary to do what is now commonplace activity on the Internet would inhibit the development of new, innovative Internet services. The experiences of Member States that have experimented with ancillary rights show the inherent weakness of the proposal. Its most material outcome has been to make information less accessible via the Internet in the Member State. It is unclear how reproducing that result throughout the EU would advance its place in the digital economy.

Establishing a digital single market in Europe will require harmonisation of limitations and exceptions throughout Member States. A clear, effective exception for text and data mining is a good start to this effort, but there are other innovative, transformative uses of works that are entitled to an EU-wide copyright exception. Some of these, such as a panorama exception, should be relatively straightforward to implement. Others will take more deliberation. Harmonisation should be a path to encourage more transformative uses of works, rather than an effort to cut back on exceptions already available in certain Member States.

CLOUD COMPUTING AND THE INTERNET OF THINGS

CDT cautions the Commission against trying to create a digital single market through a framework of sector-specific industrial policies that target specific types of online services or providers of services. One study concluded that the removal of potential legal risks for cloud services in the 2008 U.S. court decision Cartoon Network, et al. v. Cablevision led to additional incremental investment of up to $1.3 billion by venture capital firms in cloud computing in the two-and-a-half years following the decision. (Josh Lerner, The Impact of Copyright Policy Changes on Venture Capital Investment in Cloud Computing Companies (2011)). The imposition of new duties of care or other liabilities on cloud computing providers is likely to have the opposite effect on Europe-based startups seeking to gain their footing.

Instead, the Commission should seek to rely on existing laws of general application regarding consumer protection, privacy, and competition. Although the application of these protections may differ in any given case, providing a general framework rather than one that targets specific technologies, services, or actors will allow innovation and consumer choice, rather than regulatory frameworks and consequences, to set the pace and direction of the advancement of Europe’s digital single market.

The collaborative economy

The following questions focus on certain issues raised by the collaborative economy and seek to improve the Commission's understanding by collecting the views of stakeholders on the regulatory environment, the effects of collaborative economy platforms on existing suppliers, innovation, and consumer choice. More broadly, they aim also at assessing the impact of the development of the collaborative economy on the rest of the economy and of the opportunities as well as the challenges it raises. They should help devising a European agenda for the collaborative economy to be considered in the context of the forthcoming Internal Market Strategy. The main question is whether EU law is fit to support this new phenomenon and whether existing policy is sufficient to let it develop and grow further, while addressing potential issues that may arise, including public policy objectives that may have already been identified.

Terms used for the purposes of this consultation:

"Collaborative economy"

For the purposes of this consultation the collaborative economy links individuals and/or legal persons through online platforms (collaborative economy platforms) allowing them to provide services and/or exchange assets, resources, time, skills, or capital, sometimes for a temporary period and without transferring ownership rights. Typical examples are transport services including the use of domestic vehicles for passenger transport and ride-sharing, accommodation or professional services.

"Traditional provider"

Individuals or legal persons who provide their services mainly through other channels, without an extensive involvement of online platforms.

"Provider in the collaborative economy"

Individuals or legal persons who provide the service by offering assets, resources, time, skills or capital through an online platform.

"User in the collaborative economy"

Individuals or legal persons who access and use the transacted assets, resources, time, skills and capital.

Please indicate your role in the collaborative economy

- ☐ Provider or association representing providers
- ☐ Traditional provider or association representing traditional providers
- ☐ Platform or association representing platforms
- ☐ Public authority
- ☐ User or consumer association

Which are the main risks and challenges associated with the growth of the collaborative economy and what are the obstacles which could hamper its growth and accessibility? Please rate from 1 to 5 according to their importance (1 – not important; 5 – very important).

- Not sufficiently adapted regulatory framework

- 1
- 2
- 3
- 4
- 5

- Uncertainty for providers on their rights and obligations

- 1
- 2
- 3
- 4
- 5

- Uncertainty for users about their rights and obligations

- 1
- 2
- 3
- 4
- 5

- Weakening of employment and social rights for employees/workers

- 1
- 2
- 3
- 4
- 5

- Non-compliance with health and safety standards and regulations

- 1
- 2
- 3
- 4
- 5

- Rise in undeclared work and the black economy

- 1
- 2
- 3
- 4
- 5

- Opposition from traditional providers

- 1
- 2
- 3
- 4
- 5

- Uncertainty related to the protection of personal data

- 1
- 2
- 3
- 4
- 5

- Insufficient funding for start-ups

- 1
- 2
- 3
- 4
- 5

- Other, please explain

How do you consider the surge of the collaborative economy will impact on the different forms of employment (self-employment, free lancers, shared workers, economically dependent workers, tele-workers etc) and the creation of jobs?

- Positively across sectors
- Varies depending on the sector
- Varies depending on each case
- Varies according to the national employment laws
- Negatively across sectors
- Other

Do you see any obstacle to the development and scaling-up of collaborative economy across borders in Europe and/or to the emergence of European market leaders?

- Yes
- No

Do you see a need for action at European Union level specifically to promote the collaborative economy, and to foster innovation and entrepreneurship in its context?

- Yes
- No

What action is necessary regarding the current regulatory environment at the level of the EU, including the Services Directive, the E-commerce Directive and the EU legislation on consumer protection law?

- No change is required
- New rules for the collaborative economy are required
- More guidance and better information on the application of the existing rules is required
- I don't know what is the current regulatory environment

Submission of questionnaire

End of public consultation

Background Documents

BG_Въведение (/eusurvey/files/17798068-07b6-4cfb-8c80-a8e6a4f75e29)

BG_Декларация за поверителност (/eusurvey/files/0b5a7e6a-5c26-47ca-b263-9ece4aa566ca)

CS_Prohlášení o ochraně osobních údajů (/eusurvey/files/a93fa8dd-757e-421e-81f9-e1c9bca745af)

CS_Úvod (/eusurvey/files/af54c429-c5bf-482f-8525-c156be285051)

DA_Databeskyttelseserklæring (/eusurvey/files/5dd2c272-17fa-47f4-b0c7-2c207a86235f)

DA_Introduktion (/eusurvey/files/05c0d888-2d35-4e19-a314-65e8092597d6)

DE_Datenschutzerklärung (/eusurvey/files/b5e037cf-0350-40c3-b803-04f6357f9603)

DE_Einleitung (/eusurvey/files/300a2e87-e030-422a-b678-33fe2c7520a6)

EL_Δήλωση περί απορρήτου (/eusurvey/files/b408fd27-c292-4fc0-9c2d-fd70c74062c4)

EL_Εισαγωγή (/eusurvey/files/0be38358-a600-4568-bfd0-fd9697b1810f)

EN_Background Information (/eusurvey/files/0873ffeb-56b2-40d7-bf56-5aadbd176c3c)

EN_Privacy Statement (/eusurvey/files/8861750d-baa1-4113-a832-f8a5454501b5)

ES_Declaración de confidencialidad (/eusurvey/files/edd31f1e-fe9d-493a-af5e-7a7c793295a9)

ES_Introducción (/eusurvey/files/600be540-eef2-4bde-bd3a-436360015845)

ET_Privaatsusteave (/eusurvey/files/294d2e58-3a3d-4e32-905f-74e8b376c5e6)

ET_Sissejuhatus (/eusurvey/files/4bc0f8b9-febc-478a-b828-b1032dc0117f)

FI_Johdanto (/eusurvey/files/a971b6fb-94d1-442c-8ad7-41a8e973f2d5)

FI_Tietosuojaseloste (/eusurvey/files/28a1f27e-3a8e-41f3-ae27-201e29134555)

FR_Déclaration relative à la protection de la vie privée (/eusurvey/files/1341b7cb-38e5-4b81-b3bc-bd0d5893d298)

FR_Introduction (/eusurvey/files/308a1cf7-5e78-469c-996a-372b33a1992b)

HR_Izjava o zaštiti osobnih podataka (/eusurvey/files/618120e1-286a-45d4-bbbd-2493d71617fb)

HR_Uvod (/eusurvey/files/6bfc9d48-cd5c-4603-9c68-5c45989ce864)

HU_Adatvédelmi nyilatkozat (/eusurvey/files/76f442e6-3e2d-4af3-acce-5efe8f74932b)

HU_Bevezetés (/eusurvey/files/3ea8491d-429d-4c8f-be30-82db40fa59c5)

IT_Informativa sulla privacy (/eusurvey/files/e2eb5a94-9e5e-4391-a8e3-35f9e151310b)

IT_Introduzione (/eusurvey/files/aa3bf020-9060-43ac-b92b-2ab2b6e41ba8)

LT_Pareiškimas apie privatumo apsaugą (/eusurvey/files/ab30fabd-4c4e-42bc-85c5-5ee75f45805d)

LT_Įvadas (/eusurvey/files/d5a34e68-4710-488a-8aa1-d3b39765f624)

LV_Ievads (/eusurvey/files/3a9bd2b1-7828-4f0e-97f1-d87cf87b7af1)

LV_Konfidencialitātes paziņojums (/eusurvey/files/7156fdc0-b876-4f73-a670-d97c92e6f464)

MT_Dikjarazzjoni ta' Privatezza (/eusurvey/files/03139a3f-7b5f-42c0-9d2f-53837c6df306)

MT_Introduzzjoni (/eusurvey/files/ceb27908-207c-40cf-828a-6cf193731cdf)

NL_Inleiding (/eusurvey/files/ca756d80-8c02-43e1-9704-3148a13c8503)

NL_Privacyverklaring (/eusurvey/files/83d9394e-b179-442f-8a1b-41514ad072df)

PL_Oświadczenie o ochronie prywatności (/eusurvey/files/15612e0b-807d-4c6e-af1c-d65fe4ec9ddb)

PL_Wprowadzenie (/eusurvey/files/df9e1828-bbd0-4e4a-90bb-ec45a8bf46da)

PT_Declaração de privacidade (/eusurvey/files/50a6e820-91bc-4531-9a0f-47b3685753d7)

PT_Introdução (/eusurvey/files/003979c0-5277-41e9-8092-2de66d57ca00)

RO_Declarație de confidențialitate (/eusurvey/files/25c135c6-ce01-4081-a83e-53e86086797e)

RO_Introducere (/eusurvey/files/4334379b-e465-43a5-a944-8602090b0bf5)

SK_Vyhlásenie o ochrane osobných údajov (/eusurvey/files/7fab071c-85f9-47eb-aaa9-949f2239701d)

SK_Úvod (/eusurvey/files/e45df825-5e71-4172-b2ec-e07789cc3966)

SL_Izjava o varstvu osebnih podatkov (/eusurvey/files/498ec1f0-3405-4454-9aa6-40607efe118f)

SL_Uvod (/eusurvey/files/1b0b239a-630d-4d36-a92f-d4b758d41ddc)

SV_Inledning (/eusurvey/files/e9111c5b-4637-4ea1-b235-ece85ef8fe1a)

SV_Regler för skydd av personuppgifter (/eusurvey/files/0d8275b2-8344-4895-8c09-51d075671061)

Contact

✉ CNECT-PLATFORMS-CONSULTATION@ec.europa.eu
