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 6 January 2016 (13 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)

Daphne Keller
Center for Internet and Society, Stanford Law School
559 Nathan Abbott Way, Stanford, CA 94305, USA

daphnek@law.stanford.edu

* 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

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

Defining “online platforms” based on participation in multi-sided markets may help solve legal problems that are primarily economic – problems addressed by competition or consumer protection law. These appear to be the right legal doctrines to address many of the issues raised in the current consultation, and the platforms definition may help there.

But the term isn't helpful for intermediary liability (IL). IL law concerns the exchange of information. The terminology of eCommerce Art 12-15 does not need revision, as discussed in questions below. But for reference, one articulation of relevant protected entities can be found in US law: “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet[.]” 47 U.S.C. 230. Definitions like this one based on function, rather than economic market structure, are the right ones for IL.

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

* Please specify:

100 character(s) maximum

Platforms empower Internet users as active creators and participants, not just consumers.

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

Please list the problems you encountered, or you are aware of, in the order of importance and provide additional explanation where possible.

3000 character(s) maximum

In my ten years working on online notice and takedown issues, most problems have fallen into one of two large categories: intermediaries not removing enough illegal content, and intermediaries removing too much legal content. The first category receives considerable press and political attention. The second is far less conspicuous, and can at times be invisible to nearly everyone involved in the removal process.

The incentives that can lead intermediaries to remove lawful content are obvious. Complying with a removal notice is easy, cheap, and avoids legal risk. Meaningful legal review of removal requests may simply not be a priority, or affordable, for many companies.

But review matters. Intermediaries receive huge numbers of groundless removal requests from individuals or companies seeking to silence critics, rivals, or competitors. Still more requests come from people who are simply misinformed about the law. As an example, both Google and Microsoft report that at least half of their “Right to Be Forgotten” delisting requests, covering hundreds of thousands of webpages, do not state valid claims under European law. Data Protection Agencies reviewing rejected requests have generally agreed with the companies’ conclusions.

Anecdotal evidence of lawful content being removed through legal notice and takedown is abundant. One scientist famously used the US DMCA removal process to suppress reporting about errors in his published research. In another widely reported case, the Church of Scientology claimed copyright over videos critical of the Church, successfully removing thousands of videos from YouTube.

Quantitative data about removal of lawful content exists as well. I have listed all studies I am aware of on the Stanford CIS blog, at http://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws. In one, researchers found that over 50% of removal requests accepted by Google involved competitors targeting each others’ websites; and over 30% raised difficult legal questions.

Harm to ordinary Internet users from these over-reaching requests is very real. The operator of a small business whose homepage is improperly removed from Google search results may suffer a meaningful decrease in sales. The artist who promotes her paintings through a Facebook page may lose both an audience for her expression and an important source of income if that page is taken down. The student looking for furniture on Craiglist, or buying books on Amazon, will be harmed if the most competitive offers have been improperly suppressed.

IL laws can and should help solve this problem through procedural rules that make it harder for abusive removal requests to succeed. I discuss such rules in the “General Observations” section.

How could these problems be best addressed?

- market dynamics
- regulatory measures
- self-regulatory measures
- a combination of the above

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

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

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

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

3000 character(s) maximum

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

Please provide the list of online platforms with which you are in regular business relations and indicate to what extent your business depends on them (on a scale of 0 to 3). Please describe the position of your business or the business you represent and provide recent examples from your business experience.

	Name of online platform	Dependency (0:not dependent, 1: dependent, 2: highly dependent)	Examples from your business experience
1			
2			
3			
4			
5			

How often do you experience the following business practices in your business relations with platforms?

The online platform …

* A parity clause is a provision in the terms of use of an online platform or in an individual contract between the online platform and a supplier under which the price, availability and other conditions of a product or service offered by the supplier on the online platform have to maintain parity with the best offer of the supplier on other sales channels.

	Never	Sometimes	Often	Always
requests me to use exclusively its services	○	○	○	○
applies “parity clauses" *	○	○	○	○
applies non-transparent fees	○	○	○	○
applies fees without corresponding counter-performance	○	○	○	○
applies terms and conditions, which I find unbalanced and do not have the possibility to negotiate	○	○	○	○
unilaterally modifies the contractual terms without giving you proper notification or allowing you to terminate the contract	○	○	○	○
limits access to data or provides it in a non-usable format	○	○	○	○
puts significant constraints to presenting your offer	○	○	○	○
presents suppliers/services in a biased way	○	○	○	○
refuses access to its services unless specific restrictions are accepted	○	○	○	○
promotes its own services to the disadvantage of services provided by suppliers	○	○	○	○

If you do experience them, what is their impact on your business activity (on a scale from 0 to 3).

Impact on my business:
The online platform …

* A parity clause is a provision in the terms of use of an online platform or in an individual contract between the online platform and a supplier under which the price, availability and other conditions of a product or service offered by the supplier on the online platform have to maintain parity with the best offer of the supplier on other sales channels.

	0 – no impact	1 – minor impact	2 – considerable impact	3 – heavy impact
requests me to use exclusively its services	○	○	○	○
applies “parity clauses" *	○	○	○	○
applies non-transparent fees	○	○	○	○
applies fees without corresponding counter-performance	○	○	○	○
applies terms and conditions, which I find unbalanced and do not have the possibility to negotiate	○	○	○	○
unilaterally modifies the contractual terms without giving you proper notification or allowing you to terminate the contract	○	○	○	○
limits access to data or provides it in a non-usable format	○	○	○	○
puts significant constraints to presenting your offer	○	○	○	○
presents suppliers/services in a biased way	○	○	○	○
refuses access to its services unless specific restrictions are accepted	○	○	○	○
promotes its own services to the disadvantage of services provided by suppliers	○	○	○	○

If you are aware of other contractual clauses or experience other potentially problematic practices, please mention them here

1000 character(s) maximum

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

- 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

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

3000 character(s) maximum

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

* Please explain

I am the Director of Intermediary Liability at Stanford Law School’s Center for Internet and Society. My work focuses on the nexus between intermediary liability rules and the rights of Internet users. Before assuming this role, I spent ten years as in-house counsel for Google. Over that time I was intimately involved in notice and takedown processes under European laws and the laws of other countries, and gave evidence about them in public proceedings including the UK Leveson Inquiry.

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

* Please describe the situation.

3000 character(s) maximum

Elsewhere I list shortcomings of current IL law, mostly from implementing law or judicial interpretation:

* “Over-removal” of lawful content under IL rules without protection for online expression

* Market distortions and harms to ordinary Internet users from exaggerated application of the “active hosting” doctrine

* Disincentives to voluntary removal of harmful content

* Unintended consequences from “take down, stay down”

Another issue arises from extremist content, including recruitment and advocacy of violence. There are important open questions about the law governing extremist content, and about who should interpret that law.

Cases involving extremist content can be uniquely difficult, because the expression at issue may relate directly to matters of public concern, and lie on a continuum with legitimate political advocacy. Gray areas abound. Should content be banned if it advocates armed resistance against a dictator? Does it matter if the authors have committed violence, and in what country or against what targets? If one group commits terrorism, should advocacy by politically aligned but non-violent groups be banned? Can videos released by terrorist groups be used in news, or as teaching materials to understand the motivations of extremists?

Leaving these questions to private companies interpreting vague legal standards is unwise, and perhaps dangerous. An intermediary that plays it safe and removes too much can cause significant collateral damage to important, lawful expression – including by silencing and antagonizing more moderate voices resisting the spread of violent extremism in their own communities. Clear legal rules governing this type of speech, including avenues for swift judicial review, should be set by accountable lawmakers in democratic and transparent processes. Leaving tech companies to effectively adjudicate in this area is a mistake.

Transparency would also ease concerns about government, particularly law

enforcement, circumventing the rule of law by asking intermediaries to remove legal content. Government suppression of lawful information through implicit or explicit pressure on intermediaries has been termed “collateral censorship,” and is considered particularly insidious by many human rights advocates. Two recent articles address this. Old School/New School Speech Regulation by Yale Law professor Jack Balkin, discusses the role of intermediaries as proxies for government, monitoring or censoring in ways that would be unlawful if done directly by police. Against Jawboning by Derek Bambauer, covers backroom communications from governments to intermediaries. Finally, in the recent Backpage v. Dart case condemned a local sheriff for pressuring intermediaries to suppress content without a legal authority. While European law might reach different outcomes than the US on aspects of this issue, the larger questions about rule of law, transparency, and fundamental rights are the same.

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

An alarming line of judicial decisions under the “active hosting” doctrine suggests that this concept, and the scope of services protected by IL, is not clear enough. These rulings create tremendous legal uncertainty, deterring investment in the very platforms most valued by users. Neither sensible policy nor the eCommerce Directive requires such rigid, anti-consumer, and anti-competitive outcomes.

Hosts have lost immunities by making content searchable; running ads; linking to related content; mixing user content with material from other sources; and more. None of these automated features, alone, gives a host knowledge or control over user content. Assuming that they do, without assessing a host’s actual involvement in user content, elevates form over function. It also penalizes features that, in 2015, are standard and expected by users.

These rulings tell startups that they can count on IL protections only for the kinds of bare bones hosting platforms that existed fifteen years ago. Building services for the contemporary Internet in Europe is a gamble: the very features that make a product attractive to users also expose it to liability for every piece of content users post. If services with standard features must engage in expensive monitoring efforts, prosperous incumbents will be at a significant advantage. Neither Internet users nor the larger economy are served by this approach.

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

Please provide examples

1500 character(s) maximum

The existing eCommerce Directive service categories can be interpreted broadly to be “future-proof” in cases involving new technologies, as long as courts and lawmakers interpret the law in light of its logic and larger policy goals. In other words, they should avoid the “active hosting” interpretations discussed in the previous answer. Some courts in Europe have done just this, protecting complex technologies including search engines. The opposite approach – rigidly granting immunities only to technologies that have not changed since the law was drafted -- disserves Internet users and the purpose of Articles 12-15.

Legal interpretations that discourage development of contemporary, feature-rich web platforms ultimately hurt ordinary Internet users. A person seeking an audience for her writing, or customers for her business, can find them today on popular, widely used platforms. If those platforms are stripped of IL protections and must act as content gatekeepers, however, then the most useful platforms will be unable to offer the open and democratic access we currently expect. In its worst interpretations, the “active hosting” doctrine would ensure that open online participation persists only on clunky and technically obsolete services; while popular and feature-rich platforms are tightly controlled and offer only limited, pre-vetted content. Lawmakers can avoid this through sensible and flexible interpretation of Articles 12-14.

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
- [ ] 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
- [x] Other:

* Please specify.

500 character(s) maximum

Claims that are very difficult for an intermediary to adequately assess. For example:
- defamation or data protection claims claims based on disputed facts about a public figure
- copyright claims in cases with apparently strong fair dealing defenses, or with disputed facts about licensing or public domain status
- racist, xenophobic, or homophobic content repeated in an educational or journalistic context, where national law lacks clear applicable limitations or exceptions

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

1000 character(s) maximum

Generally speaking, varying notice and takedown processes for different legal claims creates needless complexity. The GDPR's new "erasure" procedure is a case in point.

That said, distinctions may arise based on high risk of harm or the ease of identifying "manifestly" illegal content. Streamlined removal makes sense for child sexual abuse imagery because it is universally considered harmful; easily identifiable on sight; and subject to no legal defenses based on context or other considerations.

At the other end of the spectrum, higher procedural barriers to removal may be warranted for content that is very difficult to identify as unlawful. Courts in Spain applying the eCommerce Directive, as well as courts outside the EU, have held that simple notice may be insufficient to create "knowledge" and trigger removal for claims raising especially hard legal questions, because the validity of the claim cannot be known until a court has adjudicated and issued an order.

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

Opportunities for the accused Internet user to defend against accusations of illegality are critical, given the high rate of false accusation and erroneous removal under notice and takedown systems. (See "over-removal" discussion, above.) Simply knowing that accusations will not remain secret may deter an accuser from making improper removal demands. Opportunities for the accused to object are not, by themselves, sufficient protection against over-removal of legal content, however. In practice, Internet users are often too unsure of their own legal rights to speak up, even when given the chance. Transparent and public removals reporting that allows motivated third parties to review and identify errors may, in practice, be more effective in surfacing and correcting improper removals. So may other procedural tools identified at https://www.manilaprinciples.org/.

The US DMCA's procedure for "counternotice" is an interesting model. Essentially, once a removal is contested, the law takes intermediaries out of the role of adjudicator. An intermediary can reinstate content upon receiving a counternotice defending its legality. It removes the content again only if the accuser is sufficiently sure of her claim to initiate court proceedings and place the matter before a competent judge. Because accepting the court's jurisdiction is required as part of counternotice, the person who provided the initial notice has low procedural barriers to enforcing her claims in court.

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

My response to this question is submitted under separate cover to CNECT-PLATFORMS-CONSULTATION@ec.europa.eu. It incorporates materials on US law requested by the EU Counselor for the Digital Economy at the Delegation of the European Union to the U.S., during the Silicon Valley workshop on the Digital Single Market initiative.

In very compressed summary, it notes:

- Intermediaries cannot confidently develop voluntary monitoring effortls under current EU law because of the “active hosting” doctrine. US lawmakers adopted the opposite policy approach, specifically encouraging monitoring efforts and specifying that .

- Filtering and monitoring requirements under a “take down, stay down” policy would pose serious risks to the rights of ordinary Internet users. In particular, rights to privacy and rights to seek and impart information would be significantly burdened.

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

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

1500 character(s) maximum

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

1500 character(s) maximum

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

The term “intermediary liability” (IL) suggests a dry doctrine of corporate liabilities and immunities. This aspect of the law is of course real, and is relevant for innovation policy. But intermediary immunities also serve a second and perhaps more important goal: protecting Internet users’ rights and practical ability to engage in public participation via the Internet. Well-crafted IL rules are

essential for maintaining an open and vibrant Internet, available to users large and small as a platform for expression, innovation, and commerce. Wise IL policy must consider more than just intermediaries and other businesses. In particular, it should look beyond the interests of the handful of large companies most visible in press, litigation and lobbying. IL law and policy should reflect the needs and interests of the millions of Europeans, and billions of people worldwide, who use intermediaries' services to exercise their own rights and pursue their own goals.

1. Intermediary Liability law protects ordinary Internet users by providing means to remove unlawful content, while protecting lawful content from "over-removal".

Notice and takedown (NTD) systems protect the rights of ordinary Internet users in two primary ways. First, for those whose rights are violated by content online, NTD provides a swift and efficient means to get the content removed. Second, and equally important, well-crafted IL laws allow people to express themselves, seek information, or do business by sharing content online, unhampered by false accusations or overzealous removal of lawful content. As discussed in response to the question above about "problems faced by consumers or suppliers when dealing with online platforms," such "over-removal" is all too common.

The NTD tools to serve both these goals are well known and widely discussed in scholarship, civil society, and within private companies engaged in notice and takedown processes. The law can, for example, require intermediaries to post easy-to-use forms for users to submit removal requests. It can require timely and informative responses from intermediaries. It can penalize people or companies for bad-faith attempts to silence legal content using NTD. It can provide the accused online speaker with notice of the accusation, and an opportunity to defend herself. An extensive menu of these and other procedural tools appears in the civil-society-endorsed Manila Principles, https://www.manilaprinciples.org/. Not every tool in the list is right for every legal system, but most have uncontroversial value for protecting the rights of all Internet users. Almost all could be implemented under the existing eCommerce Directive through codes of conduct, guidelines, judicial interpretation, or updates to national implementing law. Some of these considerations are also discussed in the well-researched and detailed Commission Staff Working document from the 2012 Notice and Action inquiry.

2. Intermediary Liability law protects ordinary Internet users by encouraging platforms to remain open to all participants.

Well-crafted IL rules help Internet users in a second way: by making it possible for large, open platforms to operate in the first place. Without the protections of IL laws, the current generation of platforms

for free expression, commerce, and public participation simply could not exist. The bare minimum IL standard –that intermediaries are not liable for unlawful user activity that they don't know about -- is what makes open intermediary services economically feasible. Without that protection, investment and innovation would shift to monitored and permission-based platforms. Private companies would become ex ante gatekeepers for ordinary Internet users' political arguments, business propositions, book reviews, silly videos, news of scientific breakthroughs, declarations of love, charitable fundraising efforts, and other untold trillions of minor communications that make up the Internet we know today.

Swift, cheap and simple access to the global network is the fundamental source of value and opportunity in today's Internet. Open platforms connect individual users to readers, customers and collaborators, empowering Internet users to pursue their own goals and fuel society-wide cultural, technical and economic development. Preserving the open platforms to make this possible should be a top priority for Internet policy generally, and IL law in particular.

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

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

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

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

5000 character(s) maximum

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

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.

- [ ] 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)
- [ ] Further expanding the scope of the Directive (e.g. to include public service broadcasters, public undertakings);
- [ ] Improving interoperability (e.g., common data formats);
- [ ] Further limiting the possibility to charge for re-use of public sector information
- [ ] 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

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

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

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

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

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)

- ☐ Economic benefits
- ☐ 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?

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

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

DSM Supplemental Response

Daphne Keller
Director, Intermediary Liability
Stanford Law School Center for Internet and Society
daphnek@law.stanford.edu

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

Case Id: df0b08dd-6924-43c2-b877-5fd3ee3f67f8

This response is submitted directly to CNECT-PLATFORMS-CONSULTATION@ec.europa.eu because it exceeds the character limit of the web form. The limit was not stated on the form and did not appear when I pasted template text into the field to test for character limits. The response incorporates materials on US law requested by the EU Counselor for the Digital Economy at the Delegation of the European Union to the U.S., during the Silicon Valley workshop on the Digital Single Market initiative.

The idea of abandoning the EU's existing rule against general monitoring requirements in favor of a "take down, stay down" approach is strange to observers accustomed to other legal systems, in particular that of the United States. Europe's IL law has long been an outlier compared other legal regimes, because EU intermediaries cannot confidently undertake voluntary monitoring efforts without risking loss of IL protection under the "active hosting" doctrine. Correcting this line of (in my opinion incorrect) judicial interpretation would unleash normal technical processes to develop, iterate upon, and improve voluntary efforts. Bypassing this step and going directly to legally mandated monitoring, despite its known risks to Internet users' expression, information, privacy, and business rights, would be highly troubling both as a practical and policy matter.

The EU's case law in this regard is in striking contrast to the express policy of US law. I will spell out the US law in some detail, based on the suggestion of a Commission official. Other policy considerations relating to voluntary content removals by intermediaries, including issues of transparency and potential bias, are outside the scope of this brief review.

The US Congress expressly set out to enable and encourage voluntary monitoring efforts in crafting US intermediary liability rules under Communications Decency Act Section 230. That law was passed in part to overrule a pair of cases much like the current EU "active hosting" rulings. In the first case, an ISP that attempted to find and remove inappropriate content was held liable for defamatory statements that remained on its service; in the second case, an ISP that made no such attempt and presented itself as a passive, neutral platform was held not liable for user content. To prevent this perverse outcome, Congress created a broad intermediary immunity, titled "Protection for "Good Samaritan" blocking and screening of offensive material." 47 USC 230(c). It requires that "No provider or user of an interactive

computer service shall be held liable on account of . . . any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected[.]" Lawmakers stated a number of intended policies, including:

> (3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;
> (4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material[.] (230(b))

A similar approach would be entirely feasible under the eCommerce Directive. Nothing in the Directive itself precludes immunities under Articles 12-15 for intermediaries that attempt to monitor content. While no one expects EU lawmakers to endorse the broad immunities set up in US law, an EU equivalent of the "good Samaritan" monitoring policy is easy to imagine. It requires only legal certainty that an intermediary's good-faith efforts to find and remove offensive or harmful content cannot in itself be grounds, under the "active hosting" doctrine, to strip that immunity of protection under Articles 12-15.

A sober assessment of this and other alternatives short of "take down, stay down" is important, because compelling intermediaries to develop monitoring technologies is a dangerous and potentially irreversible step. As the CJEU identified in its two SABAM rulings, monitoring obligations do not affect only the parties directly involved – typically, well-lawyered and commercially powerful entities including intermediaries and large copyright holders. They also have real consequences for Internet users. The court identified as relevant users' rights "to protection of their personal data and their freedom to receive or impart information." (Par. 48) Also affected is the right of Internet users to conduct their own small businesses, for which the Internet and intermediary platforms may be essential. The Commission's consultation process provides an opportunity to focus on these rights of ordinary Internet users, who may have little opportunity to be heard in typical private litigation or lobbying.

The risks to user privacy and data protection from "take down, stay down" are obvious. The EU just passed a vast new regulation, the GDPR, reinforcing users' legal rights to prevent unwanted monitoring by private companies. Obliging intermediaries to monitor users' online activity would contradict that law's goals. User rights would be similarly burdened if, following the "active hosting" doctrine, monitoring became a precondition of operation specifically for the most feature-rich and popular platforms – the ones people most want to use. The impact on privacy would be still greater if intermediaries were compelled to report suspected illegal activity to third parties, including law enforcement. In any consideration of the proportionality of a "take down, stay down" order, this impact on users' rights should be a key consideration.

Proactive monitoring by Internet intermediaries also poses real threats to free expression and access to information online. The first threat comes from Internet users' changed behavior in the face of surveillance. The link between Internet monitoring and self-censorship is far from speculative. In the wake of the Snowden revelations, a study by the US branch of the PEN International human rights and literary organization found that one in six writers surveyed had avoided speaking or writing online about certain topics because of concerns about surveillance.

Writers specifically reported suspending research on drug laws and mass incarceration, Middle Eastern policy issues, and sexual violence in the military, among other topics. One senior reporter compared journalists' current distrust of online communication to the atmosphere among reporters in Moscow during the cold war. (http://www.pen.org/chilling-effects) Mandating widespread monitoring by private intermediaries based on a panoply of legal claims – defamation, hate speech, intellectual property, defamation – would only add to the topics considered "off limits" by writers, and to the atmosphere of anxiety and self-censorship.

The second threat to Internet users' expression and information rights comes from inevitable failures and inaccuracies of filtering technologies themselves. This is the issue identified by the CJEU in SABAM – a filtering technology "could potentially undermine freedom of information, since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications." (P. 50) Such failures arise because algorithms lack human judgment and cannot adequately assess context. A content filter intended to find copyright violations or illegal racist content, for example, would also suppress those same materials when used lawfully in an educational context.

Accidental filtering of legal information can also arise from purely technical errors. Developing monitoring tools that did not overfilter (remove more information than intended) or underfilter (remove less) would be a significant, perhaps insurmountable technical challenge. Even YouTube's Content ID, the product of years of engineering work and many millions of dollars' investment by Google, is routinely faulted by Internet users for misidentifying and removing lawful content. Laws requiring similar monitoring efforts from Internet intermediaries with smaller engineering budgets would almost certainly lead to even more inaccurate filters, causing more removals of information legally shared by Internet users. It is unrealistic to expect most intermediaries to have the resources to develop more reliable technologies – and, if the statistics on over-removal under current notice and takedown regimes are any indication, many companies lack incentives even to try. Filtering, monitoring, or "take down, stay down" obligations would be a recipe for clumsy implementation and over-removal of Internet users online expression and information.

Finally, lawmakers should be attuned to long-term fallout from monitoring obligations. Filters developed to comply with EU law would also be available as enforcement tools for any other country in which an intermediary does business. Courts and lawmakers in China, Russia, or Indonesia may have very different ideas about what content should be automatically suppressed. The genie of sophisticated Internet censorship technology, once released, would be very hard to put back in the bottle.

This listing of risk from "take down, stay down" models is not intended to minimize the harms caused by unlawful content online. Copyright holders face genuine threats from piracy. Law enforcement and society at large face even graver threats if Internet platforms are used to devise and launch terrorist attacks. But other tools exist to counter these harms. Some of them, including simply giving EU intermediaries clear legal leeway to attempt voluntary monitoring, have barely been tested. More measured efforts are clearly appropriate before resorting to pervasive, mandatory monitoring of citizens' online behavior.