Public consultation on the safety of apps and other non-embedded software not covered by sector-specific legislation*

* such as medical devices or radio equipment

Fields marked with * are mandatory.

1 Introduction

This consultation concerns software and applications (apps) which are neither embedded, nor contained in a tangible medium at the time of their placement in the market, their supply to consumers or when they are otherwise made available to consumers (non-embedded software). Examples include health and well-being apps that can be used on a mobile device, digital models for 3D printing or apps controlling other devices (such as electronic appliances).

The purpose of the consultation is to gather input from various stakeholder groups, in particular consumers, businesses and authorities, on their experience related to the safety of apps and other non-embedded software. The questions aim at obtaining a better understanding of the possible risks and problems that non-embedded software may pose and how these problems could be dealt with. The views gathered will help to define potential next steps and future policies at the EU level including, if appropriate, possible revisions of existing horizontal and/or sector-specific EU legislation.

If apps are giving access to a service, this consultation addresses only the safety aspects in the functioning of the app, and not the underlying service itself (e.g. transport or accommodation). For the purpose of this consultation, only apps and non-embedded software that are downloadable on a device such as a personal computer, tablet or smartphone or accessible on a remote location (cloud) would be covered.

For the purpose of this consultation "safety" and "safe use" should be understood as freedom from unacceptable danger, risk or harm, including security-vulnerabilities ("cyber-security") and cover physical, economic as well as non-material damage.

This consultation will only look into the safety of apps and other non-embedded software which is not already addressed and foreseen by sector-specific legislation such as the Medical Devices Directives, the Machinery Directive or the Radio Equipment Directive which include provisions on safety ensuring that equipment within their scope, if compliant, is safe.

2 General information on respondents

*

Your feedback will be published on the Commission's website unless this would damage your legitimate interests. Do you agree to publication?

- (●) Yes – under the name supplied I consent to publication of all the information in my feedback, and I declare that none of it is subject to copyright restrictions that would prevent publication.
- ( ) Yes – anonymously, I consent to publication of all the information in my feedback except my name/the name of my organisation, and I declare that none of it is subject to copyright restrictions that would prevent publication.
- ( ) No - my feedback cannot be published, though I consent to its being used internally by the Commission.

*

I'm responding as:

- ( ) An individual in my personal capacity.
- (●) The representative of an organisation/business.
- ( ) The representative of a public authority/international organisation/academia.

For representatives of an organisation/business please select the applicable option:

- ( ) Manufacturer of the device the software runs on or controls
- ( ) App or software manufacturer/developer
- ( ) Distributor/intermediary (e.g. app store)
- (●) Industry association
- ( ) Trade union
- ( ) Consumer organisation
- ( ) Other

*

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

Please register your organisation in the Transparency Register of the European Commission and European Parliament before completing this public consultation.

- (●) Yes
- ( ) No

Please register in the Transparency Register before answering this questionnaire. If your organisation responds without being registered, its input will be considered as that of an individual and will be published separately.

*

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

64270747023-20

*

My institution/organisation/business has its main establishment:

- [ ] All EU Member States
- [ ] Austria
- [x] Belgium
- [ ] Bulgaria
- [ ] Czech Republic
- [ ] Croatia
- [ ] Cyprus
- [ ] Denmark
- [ ] Estonia
- [ ] France
- [ ] Finland
- [ ] Germany
- [ ] Greece
- [ ] Hungary
- [ ] Italy
- [ ] Ireland
- [ ] Latvia
- [ ] Lithuania
- [ ] Luxembourg
- [ ] Malta
- [ ] Netherlands
- [ ] Poland
- [ ] Portugal
- [ ] Romania
- [ ] Spain
- [ ] Slovenia
- [ ] Slovakia
- [ ] Sweden
- [ ] United Kingdom
- [ ] Other

*Please specify:

Brussels, Belgium

*

Please indicate the name of your institution/organisation/business:

DIGITALEUROPE

Please indicate your address and contact details:

*First name:

Damir

*Last name:

Filipovic

*E-mail address:

info@digitaleurope.org

Address:

14 rue de la Science, 1040 Brussels, Belgium

More information:

http://www.digitaleurope.org

3 **Consultation:**

3.1 For individuals or representatives of a public authority / organisation / business.

In your view:

*1. What type of apps or other non-embedded software pose safety risks? Please give examples.

10 character(s) minimum

DIGITALEUROPE questions the formation of this initial question as there is likely to be some form of risk to every app and/or non-embedded software. This question presumes that because a product or service is accessed via an app or other piece of non-embedded software it inherently raises greater safety concerns than if that same product or service were accessed by other means. To be able to properly answer this question one would need to understand how the European Commission intends to categorise 'risk' and how the European Commission intends to define 'critical' or 'non-critical' as software can be categorised as 'critical' or 'non-critical'. For 'critical' software there is a clear process in place from a systems perspective and software is just one element of this system. This is already a highly regulated space and there are many safety standards that have to be complied with, such as www.iec.ch/functionalsafety.

As such, we believe the question that the European Commission should be assessing is what is an acceptable level of risk/danger for apps and non-embedded software. This 'high-risk' assessment is the cornerstone of IT security practices and is at the centre of many pieces of European legislation including the upcoming General Data Protection Regulation (GDPR).

Today, 'high-risk' assessments exist at each stage of software development and takes into account every function of a given system. 'Hazope' is an example of such an assessment, which helps to define if a function is 'critical' or 'non-critical' and how risks can be mitigated.

Unfortunately, without fully understanding the European Commission's views on the threshold for 'high safety risk' it is difficult for DIGITALEUROPE to answer this question, particularly as it depends on a case-by-case basis and would go against the concept of neutrality. However, we are of the strong belief that there is no need to regulate apps differently than other services in the same sector. We also caution against an expansion of 'safety risk' of apps or non-embedded software beyond direct physical harm.

*2. What risks can apps or other non-embedded software pose?

- [ ] Economic damage
- [ ] Physical damage to individuals
- [ ] Physical damage to property
- [ ] Non-material damage (pain and suffering)
- [x] Other

*Please explain:

10 character(s) minimum

As mentioned in the previous question there is a risk to everything. We believe it is impossible to fully avoid risk in all situations and therefore it is difficult for DIGITALEUROPE to properly answer this question as the question should focus on 'high-risk' rather than simply 'risk'.

We wish to note that if the objective of the European Commission is to attempt to create further safeguards to reduce level of risks of health and well-being apps through further information gathering, opt-outs, etc. then this could be a useful exercise. However, we caution the European Commission if the objective is to avoid risk entirely in a horizontal matter. While there is no 'horizontal EU legislation' on the issue of risk, it is often covered by Member State law. We believe that national civil codes sufficiently cover damages related to risk. It is also important to note that damages related to risk are sufficiently covered by contractual schemes. If a consumer or business is provided a service and that service causes damages, the entity who provided the service is responsible for the damages. This contractual model applies as well to apps and non-embedded software as existing liability schemes sufficiently cover any damages.

Furthermore, we wish to highlight that many apps provide information to users regarding potential risks. The provision of this information (coupled with mitigation factors) works to reduce the potential damages/risk (high or low) to users.

Please give your opinion on the following options:

	No risk	Low risk	High risk	Very high risk
*Economic damage	◉	○	○	○
*Physical damage to individuals	◉	○	○	○
*Physical damage to property	◉	○	○	○
*Non-material damage (pain and suffering)	◉	○	○	○
*Other	◉	○	○	○

Please explain:

10 character(s) minimum

DIGITALEUROPE objects to the assumption that because a product or a service is accessed via an app or non-embedded software it therefore 'raises' risks to consumers. We wish to express our concern with the framing of this table, particularly with the lack of an 'not applicable/no opinion' or 'other' option. We believe that this exercise should focus on 'low-risk' and 'high-risk' only. However, even with such an option each situation is different therefore making such a table difficult to fill in.

*3. In which sectors are apps or non-embedded software most affected by safety problems?

- [ ] Agriculture
- [ ] Electronic Communications / Telecommunications
- [ ] Health
- [ ] Home automation/ Domotics
- [ ] Energy
- [ ] Financial
- [ ] Transport
- [x] Other

Please specify:

10 character(s) minimum

Each sector faces different (inherent) risks, which may or may not depend on whether they use apps or any other type of software. In this sense, it is impossible to prioritise one sector over another as one can find potential problems in all. However, as previously noted, 'zero risk' does not exist. This question should instead focus on areas where there is a likelihood for high risk only.

3.2 For representatives of a public authority / organisation / business. In your view:

*4. In your professional experience have you already identified unsafe apps or other non-embedded software or have consumers approached you because they encountered problems with unsafe apps or other non-embedded software?

- ( ) Yes
- (•) No

Please specify:

10 character(s) minimum

If an app is submitted to an app aggregator and it is deemed as ‘unsafe’ then it would never end up on the app aggregators public marketplace for consumers. If there is a safety problem then it would be rejected prior to reaching the public marketplace. App aggregators dedicate significant resources to properly assessing apps before they are placed on the market. However, if there were to be an issue, then we wish to express that it is properly covered by EU consumer protection law.

4.1 If yes: What did you do to solve these problems?

10 character(s) minimum

*5. Are existing EU or national safety rules and market surveillance mechanisms sufficient to monitor and withdraw, where necessary, unsafe apps or non-embedded software from the market?

- (●) Yes
- ( ) No

*Please explain:

10 character(s) minimum

We believe that existing rules are sufficient to monitor and withdraw potential unsafe apps. The European Commission has the ability to act against a company that has placed a product on the market that can be deemed as dangerous. This is supplemented by national civil codes, which also ensure that dangerous products are removed from the public marketplace.

We would also like to emphasise the potential for the Consumer Protection Cooperation (CPC) Network to fill any perceived gaps. The CPC Network is an umbrella committee covering all consumer safety agencies and is chaired by DG JUST. The CPC works to ensure that if there is an enforcement action in 1 Member State, and the issue is also identified in other Member States, proper coordination occurs. The CPC is currently going through a revision and looking at enhancing its powers. This revision is a potential vehicle to harmonise civil law provisions when related to apps and non-embedded software.

*6. Have you been held accountable for damage caused to consumers because of unsafe apps or other non-embedded software?

- ○ Yes, as manufacturer of the device the software runs on or controls
- ○ Yes, as an app or software manufacturer/developer
- ○ Yes, as an intermediary/distributor (e.g. app store)
- ○ Yes, other
- ◉ No

6.1 If yes: What did you do?

10 character(s) minimum

*7. Do you think that existing horizontal and sector-specific EU legislation (e.g. General Product Safety Directive, Market Surveillance Regulation, Medical Device Directive, Radio Equipment Directive) taken together sufficiently cover the safety of all types of apps or other non-embedded software available on the market?

- (●) Yes
- ( ) No

Please explain:

10 character(s) minimum

As previously noted we believe that existing rules are sufficient to monitor and withdraw potentially unsafe apps. The European Commission has the ability to act against a company that has placed a product on the market that can be deemed as dangerous. This is supplemented by national civil codes, which also ensure that dangerous products are removed from the public marketplace.

*8. Have you considered opening up an Application Programming Interface (API) of a device you manufactured or a service you provide to app and software developers to link their app to your device/service and use its functionalities? If so, have you taken into consideration safety aspects?

- ( ) Yes
- ( ) No
- (●) Not applicable

*Please provide details:

10 character(s) minimum

While it is difficult to answer this question on behalf of all DIGITALEUROPE members, we wish to express that DIGITALEUROPE members always take into consideration safety aspects when developing apps and non-embedded software. Furthermore, when opening up an API to allow control of another device/service safety considerations remain a key priority in overall risk assessment.

*9. Has the legal framework on safety influenced your decision on whether to invest in developing apps or software?

- ( ) Yes
- ( ) No
- (●) Not applicable

Please explain:

10 character(s) minimum

*10. In the EU Member State where you operate, are there specific rules on safety requirements for apps or other non-embedded software?

- (●) Yes
- ( ) No

*Please select the country where you operate:

- [x] All EU Member States
- [ ] Austria
- [ ] Belgium
- [ ] Bulgaria
- [ ] Croatia
- [ ] Cyprus
- [ ] Czech Republic
- [ ] Denmark
- [ ] Estonia
- [ ] Finland
- [ ] France
- [ ] Germany
- [ ] Greece
- [ ] Hungary
- [ ] Italy
- [ ] Ireland
- [ ] Latvia
- [ ] Lithuania
- [ ] Luxembourg
- [ ] Malta
- [ ] Netherlands
- [ ] Poland
- [ ] Portugal
- [ ] Romania
- [ ] Slovakia
- [ ] Slovenia
- [ ] Spain
- [ ] Sweden
- [ ] United Kingdom
- [ ] Other

Please explain:

10 character(s) minimum

The law in Member States aims to protect individuals from safety risks. In civil codes of all Member States you can find protections regarding safety. Furthermore, under the concept of reasonable and foreseeable use and requirements to assess risk, if a manufacturer allows a device to be controlled by an app, it should take this into account and ensure the device still meets the requirements of regulations under these conditions.

13. Do you have any further comments?

As eluded to throughout our response, it is unclear to DIGITALEUROPE if the goal of this consultation is to try and define all apps and non-embedded software as ‘critical?’

An analogy for such an exercise could be for a satellite navigation system. If a lorry is directed towards a low height bridge and the lorry driver drives the lorry under the bridge and the lorry is damaged there is clearly a safety issue. However, the navigation system is an information system. There must be warnings and disclaimers for the human operator to take notice of. It is there as a guide and not to make all of the decisions for you.

If we refer to a connected vehicle and that same lorry is driven towards the low height bridge, the system in the vehicle should have applied the brakes. If it does not then the safety risk is high and the system should have a mitigation functionality built in. This is a ‘critical system’ which is machine controlled whereas a navigation system is an information system and is human controlled. The European Commission appear to be referring to information systems throughout this consultation (i.e. non-critical software), which are human controlled.

Are these apps and non-embedded software supposed to be considered as ‘critical’? Is the objective of this exercise to make sure that all software and systems architects must mitigate every possible activity that could happen, even when the person not applying common sense uses the app ? It is unclear to us how this would be governed? We highlight that most apps come with a clear legal text disclaimer stating that it is the end user’s responsibility to read and understand and apply common sense.

Lastly, we wish to add that there is a healthy and competitive market for apps. If manufacturers and developers are not taking adequate precautions to prevent unsafe solutions then the market would respond accordingly and their products will not be successful. Adding regulation in a situation when the problem is not entirely clear will increase market entry requirements and reduce customer choice and competition.

14. Please upload any files with evidence or references that you consider relevant:

Contact

CNECT-PUBLIC-CONSULTATION-APPS-SAFETY@ec.europa.eu