**Synopsis report of the public consultation on the safety of apps and other non-embedded software**

## Introduction

The European Commission launched a public consultation on the safety of applications for mobile devices ("apps") and other non-embedded software on 9 June 2016, which was open for 12 weeks. Although the response to the consultation was rather limited, it presented a variety of concerns, including the need for more legal clarity on the EU legislation applicable. The Commission will explore the matter but no specific Commission initiative seems necessary at this stage further to the consultation.

This consultation gathered input from various stakeholder groups, in particular citizens, industry and public authorities, on their experience related to the safety of apps and other non-embedded software. The purpose was to obtain a better understanding of the possible risks and problems those apps or non-embedded software may pose and how these problems could be dealt with.

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) were covered by this consultation.

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

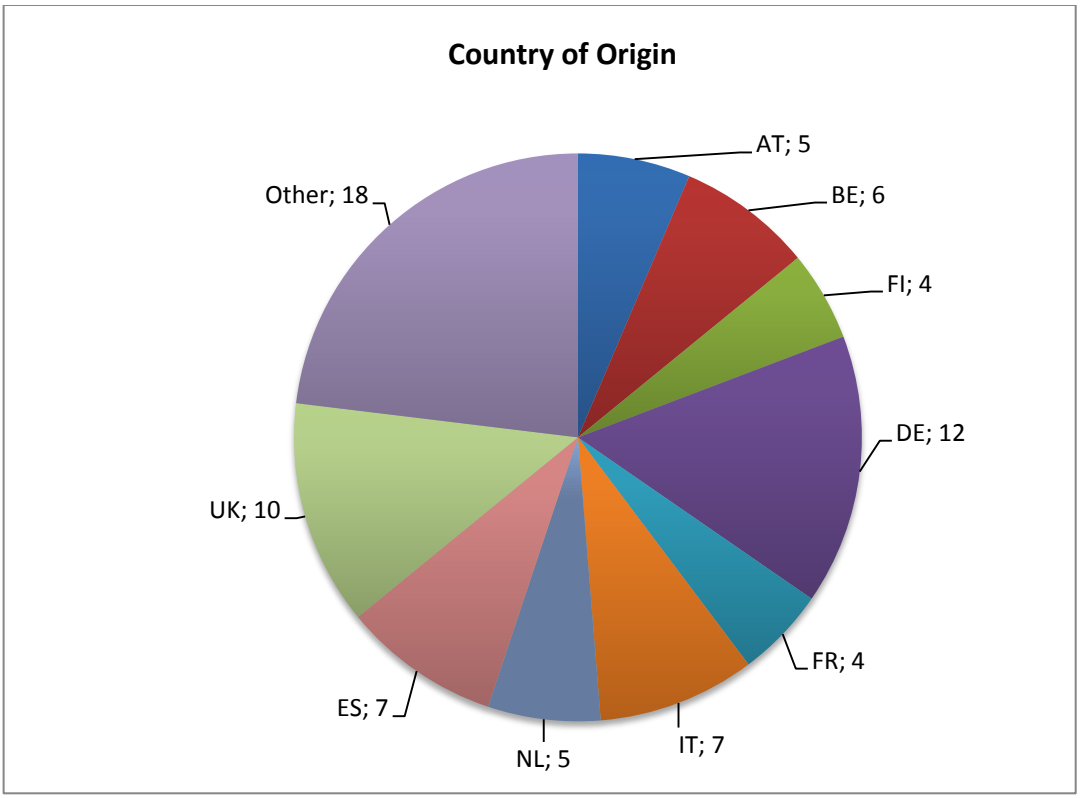
This consultation looked only into the safety of apps and other non-embedded software which are not already addressed and foreseen by sector-specific legislation, such as the Medical Devices Directives or the Radio Equipment Directive, which include provisions on safety ensuring that equipment within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

The replies of contributors who agreed to publication, as well as a preliminary summary of this consultation, are available on DG CONNECT's website. This report analyses the replies to the public consultation.

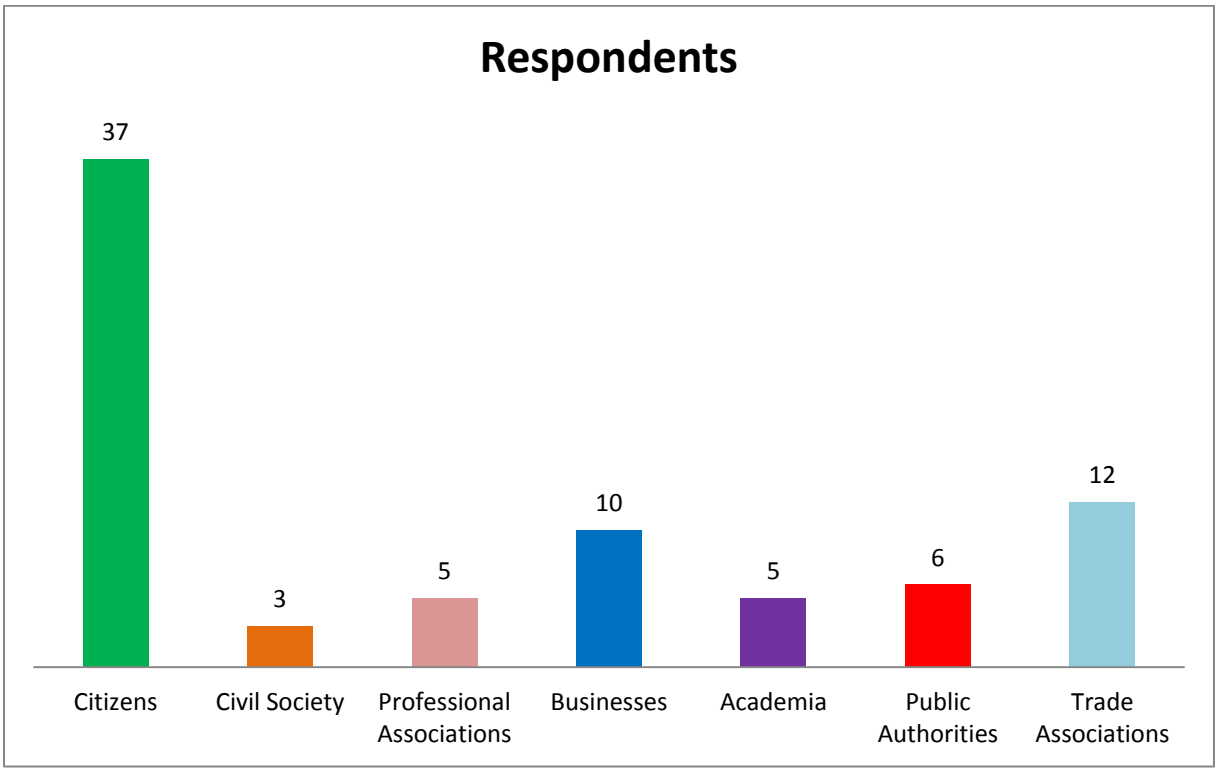
## Who replied to the consultation?

The consultation gathered a total of 78 replies from stakeholders in Member States as well as from outside the European Union.

The largest number of responses came from Germany (12), the UK (10), Spain (7) and Italy (7).




A number of citizens (**37**) have responded to this consultation. **27** replies were received from industry, coming from different categories such as trade associations (12), individual businesses (10) and professional associations (5). **6** contributions came from public authorities, **5** from academia and **3** were received from civil society.



**Questions addressed to all respondents:**

**What type of apps or other non-embedded software pose safety risks?**

As mentioned by 33 respondents across all stakeholder groups, the main category of apps that could pose safety risks are health and wellbeing apps. The following examples are given: apps that give health advice, apps upon which a consumer is taking a health or lifestyle-related decision, apps that track and collect data from the user to assess and monitor health-related metrics (e.g. number of steps, heart rate) or apps that interface with electronic health records.

If the information provided by an mHealth app is erroneous, this can result in people making the wrong conclusions about their health status and making the wrong decisions about their health management. Different types of risk can occur: physical (e.g. wrong medication), psychological (e.g. the stress caused by wrong information regarding one's health), economic (e.g. costly medication that is needlessly taken).

Several industry members say that safety risks exist in the so called "grey zone", where the distinction between apps which fall under the regulatory framework of medical devices and other apps is unclear, given that health and wellbeing apps out of the scope of the medical devices framework are not subject to the same safety controls and those apps in the "grey zone" may pose risks similar to those of medical devices.

Several replies (17) from all stakeholder groups indicate that safety risks can originate from non-embedded software and apps that do not respect data protection principles by accessing or collecting sensitive data without informing the user or requesting consent for processing these personal data.

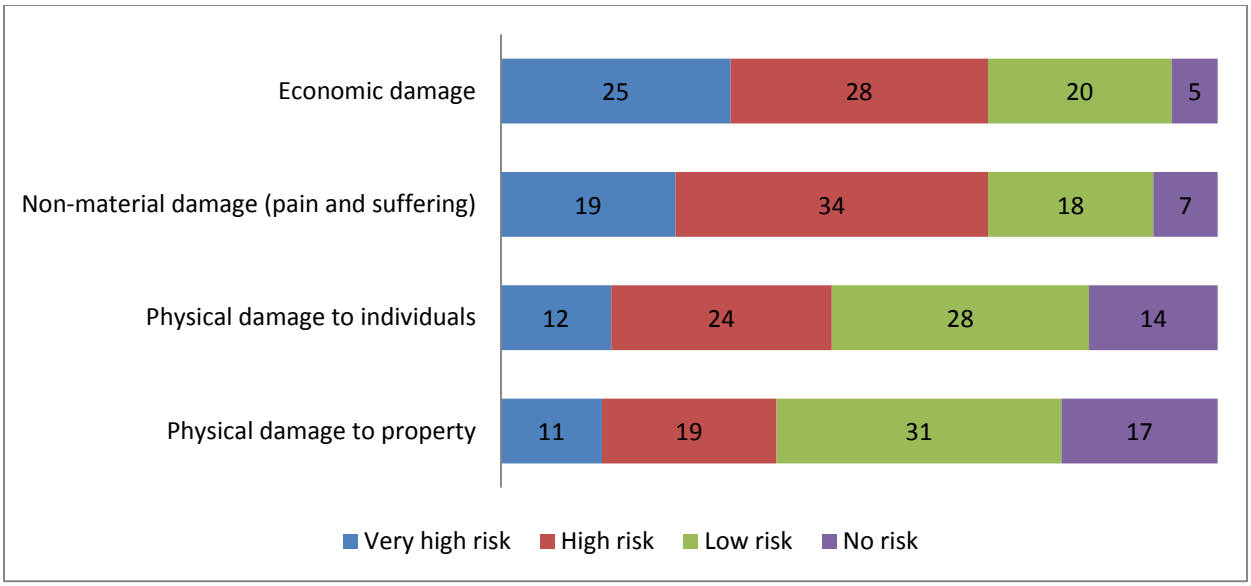
A number (12) of respondents say that some apps may be subject to cyberattacks for various reasons (data collection, financial operations, controlling another device), thus increasing the safety risk of the app.

Other types of apps mentioned posing safety risks are sports apps, financial apps, or apps that geolocalise the user.

**What kind of risks do they pose and which sectors are most affected?**

60 respondents believe apps and other non-embedded software can create economic damages, followed by 55 who mention non-material damage (pain and suffering). 51 respondents mention physical damage to individuals as a risk, 38 physical damage to property and 33 say other (several options could be chosen).

Respondents were asked to classify the different types of damage according to the likelihood of risk they present. They believe that economic and non-material damage pose the highest risks whereas they see the lowest or no risk for physical damage to individuals or property.




As regards data protection related risks, industry stakeholders say that a security breach, especially if there is a leak of commercially sensitive data and/or personal data, may expose the company to legal risks (clients asking for compensation), financial penalties and damaged brand image).

Three citizens and a public authority coincide in saying that data leakage of sensitive financial and health data can lead to identity theft and financial loss. Six citizens say that unexpected disclosure of private information to a third party may have severe consequences (e.g. breach of right to privacy, reputation, economic loss).

Respondents from industry and public authorities point out that one of the risks is the lack of awareness and training of people on the potential danger of apps and other non-embedded software which leads to misuse and potential serious consequences, particularly in the health domain.

For most respondents, the risk is as diverse as difficult to estimate because it can have many sources and depends on the function and the purpose of the apps as well as on the context in which they are used.

The citizens responding to this question list examples of risks that can occur using apps or other non-embedded software, amongst them: (18 and 12 with mHealth apps) physical damage, (15) economic damage, (10) disclosure of personal data to third parties, (8) violation of privacy, (8) damage to property, (6) cybersecurity/hacking, (4) illicit trade of data, (3) destruction of files.

Respondents think the sectors most affected by safety problems are the health sector (52), followed by electronic communications/telecommunications (39), finance (33) and home automation/domotics (28).

Most respondents do not specify their answer further, and those that do specify have varied opinions, ranging from the argument that each sector faces risks which do not necessarily have to do with whether or not an app is used, to the argument that the more dependent the sector is on apps, the more affected it is by risks.

**Questions addressed to citizens:**

**Have citizens encountered any problems with unsafe apps?**

16 citizens out of 37 say that they encountered problems with unsafe apps or other non-embedded software in the past. Eight say that they had problems very often or often, five say a few times and two citizens encountered problems once. Amongst the problems encountered are data breaches, an app turning on the lights in the house or compatibility problems.

For most of them the problem caused no damage, for one it caused a financial loss and for another one, a missed job interview. To the question what they did to tackle these problems, four citizens replied that they did not take any action, three contacted the app or software manufacturer/developer, two contacted a national authority and ten took other actions (e.g. they either updated the software or they stopped using that app).

Out of those citizens who took action, for five of them the problem could be solved while for nine this was not the case.

**Do you feel there is enough possibility to hold somebody accountable in case of damage linked to the use of unsafe apps or other non-embedded software?**

19 respondents think that there is not enough possibility to hold somebody accountable in case of damage linked to the use of unsafe apps or other non-embedded software. Most negative answers indicate a general lack of information concerning whom to contact in case of damage. Several of the respondents think that consumers are unprotected when an app causes some kind of damage. An additional issue that could be found is the difficulty of identifying the origin of the damage.

Eight respondents think there is enough possibility to hold the app or software manufacturer/developer accountable. Most of them indicate a correlation between the app developer and the responsibility originating from the damage produced by the app itself. Another issue that appears in several answers is the lack of knowledge of consumers regarding the chain of responsibility in case of damage linked to the use of an unsafe app.

Six respondents consider that the separation of responsibilities is complex and thus affects all categories of responsible actors.

One respondent says that there is enough possibility to hold the intermediary or distributor accountable while two respondents believe that there is enough possibility to hold accountable the manufacturer of the device the app runs on or controls.

**Questions addressed to public authorities, academia, industry and civil society:**

**Does existing horizontal and sector-specific EU legislation, considered together, sufficiently cover the safety of all types of apps or other non-embedded software available on the market?**

Almost all public authorities, academia and civil society (10 out of 12) do not consider the safety of all apps sufficiently covered by EU legislation. Also the majority of industry (18) does not think that the safety of apps is sufficiently covered by EU legislation while 10 believe that this is the case.

Out of those that responded negatively, the largest number of responses (10) relate to health and wellbeing apps: some mention the classification of health apps as an issue, i.e. whether or not they

are covered by the EU regulatory framework on medical devices; others underline the necessity to have clinically validated and accurate apps. Four respondents highlight the importance of sufficient security measures to protect the data processed by health and wellbeing apps.

One respondent from academia says that more work is needed to understand the impact of apps on users (such as the potential for addiction or the impact on personal support and reliance). One professional association considers that the peculiarities of information (intangible, it can be copied and subtracted without removing it) necessitate specific regulation.

Those that responded positively believe that both sector-specific as well as horizontal legislation provide a sufficient means to monitor apps and non-embedded software from a safety context. In addition to the legislation referred to in the question, the General Data Protection Regulation, the Network and Information Security Directive and the proposed Digital Content Directive are mentioned as imposing additional requirements as well as protection for consumers.

Two trade associations point out that the European Commission has the ability to act against companies that have placed potentially dangerous products on the market.

Other respondents suggest an insurance-based model, guidance or industry best practices or believe that the problem lies with implementation and enforcement rather than with legislation.

**Are there specific rules on safety requirements for apps or other non-embedded software in the EU Member States?**

14 respondents say that there are specific rules on safety requirements for apps or other non-embedded software in the Member State where they operate while 27 say that there are no such rules.

The specific rules mentioned are legislation on medical devices (respondents from France, Germany, UK), data protection (Estonia, France, Germany), consumer protection legislation, liability for defective products (France), certification for medication prescription software (France). Furthermore, sector-specific legislation with security requirements for sectors such as defence, health and banking in France are mentioned.

Others named different guidance documents on safety, security, privacy and quality and the checking process done via app aggregators.

**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?**

The majority of all stakeholder categories do not believe that EU or national safety rules and market surveillance mechanisms are sufficient to monitor and withdraw unsafe apps or non-embedded software from the market (19 out of 29 responses from industry, 4 out of 5 from public authorities, 4 out of 5 from academia and 3 out of 3 civil society).

Out of those who replied negatively, seven did not explain why or mentioned that they are not aware of any rules. Nine respondents say that there are no safety rules or market surveillance mechanisms in place for those health and wellbeing apps that fall outside the scope of the regulatory framework

on medical devices. Two respondents mention the need to improve users' awareness of the safety of apps.

Two think that the main issue comes from the lack of implementation of the existing legal framework and two others support a strong EU wide market surveillance mechanism.

Those respondents who replied positively, note the success of the app economy and the fact that existing safety rules, market surveillance mechanisms and the consumer protection framework are providing sufficient protection. It is also mentioned by two respondents that apps do not present specific safety risks distinct from other software and two others note that EU and Member States authorities have the possibility to remove unsafe apps from the market.

**Identification of unsafe apps or other non-embedded software in a professional context?**

23 respondents to this question affirm that they have already identified unsafe apps or other non-embedded software, or that consumers approached them because they encountered problems with unsafe apps or other non-embedded software. The remaining 18 say that they did not have such experience before.

Out of those who answered that they have experience with unsafe apps or other non-embedded software, nine respondents express concerns related to security vulnerabilities. In particular, respondents mention the lack of security measures taken in the design of apps which can lead to cyber attacks and may consist in fraud such as phishing, or data theft. Some respondents (4) also mention a lack of transparency on how the information collected by the app may be used or that apps ask for inadequate permissions.

Others (4) highlight risks related to health and wellbeing apps, for instance if they provide a wrong diagnosis or due to bad or misinterpreted health advice. A few respondents also point out other specific examples, in particular apps revealing location information or apps making use of augmented reality.

One business operating an online app marketplace mentions their particular incentive programme for detecting vulnerabilities in apps. They also indicate recommendations which they provide to users on how they can protect themselves.

Out of those who replied that they did not have experience with unsafe apps or other non-embedded software, several respondents note that app aggregators have systems in place to assess apps before they are placed on the market. Furthermore, it was mentioned that if there were an issue, this would be covered by EU consumer protection law.

One trade association also points out that, due to the competitive nature of the app economy, app developers strive to produce high quality apps in order to stay in business and to maintain and grow their customer base.

Consequently, respondents who had answered in the affirmative were asked what they did to solve the problems.

The responses received to this question are highly diversified and are mainly given by individual respondents. Among the answers received on how to solve the issues are the following:

- systems put in place by app aggregators (e.g. reporting and the possibility to remove harmful apps from the platform);
- awareness campaigns or education sessions for users;
- measures taken by national competent authorities;
- the creation of registers with certified apps;
- developing criteria or a tool to evaluate safety, purpose, usability and suitability of mobile apps;
- regular audits to identify potential security vulnerabilities;
- software patching;
- putting the harmful app on a blacklist;
- putting stricter security rules in place;
- contacting the developer and adopting a responsive disclosure path;
- performing a factory reset;
- removing the unsafe app or non-embedded software by a controlled process.

**Questions addressed to industry:**

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

10 respondents provided a positive answer to this question indicating that clearly the safety rules applicable to apps and other non-embedded software influence the decision of investing in developing and app. Most of the respondents coincide that clarity in legal obligations is directly correlated to increased investment. Several of the businesses that answered this question point out that the current legal framework has enabled the app economy to thrive in the EU, by providing a suitably flexible environment, open to creativity and innovation. Five respondents provided a negative answer to this question.

**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?**

Nine businesses say that they have considered opening up an Application Programming Interface (API) of a device they manufactured or a service they provide to app and software developers to link their apps to their device or service. Most of them say that they observe safety, security and reliability principles when third parties want to link apps to their devices. One business did not develop their answer due to confidentiality principles. 21 respondents have not found this question applicable and two have provided a negative answer to the question.

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

27 respondents out of the 30 who answered had not been held accountable for damage caused to consumers by an unsafe app or other non-embedded software. Only two intermediaries/distributors and one professional association provided a positive answer to this question. Among the latter we could find professionals asking for a clearer separation of responsibilities and businesses explaining their way of checking security vulnerabilities in apps.