Call for Expression of Interest

BEUC/ANEC study: How to keep consumers safe in an era of connected products?

Terms of Reference (ToR)

1. Background

More and more consumer products such as cars, baby monitors, fridges and toys that are coming to the market can connect to the internet. Consumers interact with these devices through voice recognition, cameras and data input. As no clear definition exists, many refer to these new products as the 'Internet of Things', 'e-objects', 'connected devices' or 'smart devices'. This means concretely that physical objects such as a washing machine are integrated into a computer-based environment. Or one could also say that traditional consumer products are becoming a mixture of hardware, software/algorithms, data and service.

While these products potentially offer many new services and convenience to consumers, consumer organisations' research and testing has shown that such products can come with multiple flaws: Consumers health and physical integrity may be at risk and their privacy may be violated.

Besides risks related to data protection and privacy, internet connected products may directly pose safety and security threats to consumers. What if a self-driving car shortly loses internet connection? What if a stranger can talk directly to a child through an unsafe toy? And what if a blood pressure monitor which collects data and proposes dosage of blood pressure pills starts to function inaccurately over time? These questions are currently unanswered even though more and more 'eObjects' are already coming to the market.

Neither EU nor national legislative frameworks are up to date to cover with this new type of products and risks, thereby possibly leaving consumers behind without proper protection as public authorities do not have the tool to act for risk assessment and risk management. It is important to check how far the EU legislative framework which currently is in place to ensure that only safe products are placed on the market is fit for covering these new developments in consumer markets, also in presence of a new range of players intervening in the production and functioning of connected products. In particular those who manufacture the product and

the software and those who store or may make use of collected data and which offer additional services are not the same. This may raise a whole new range of questions such as who is responsible for safety in case something goes wrong. This unclear situation complicates enforcement enormously. As products can also receive updates remotely, not all changes in a product may even be under the control of the manufacturer of the device.

Thanks to the **General Product Safety Directive (GPSD)**, the **Toy Safety Directive** and the **Radio Equipment Directive**, manufacturers are obliged to only make safe products available on the market, and other sectorial "new approach" legislation. The question arises whether the concept of 'safety' included in this legislation is not too narrow for protecting consumers from the security flaws which come along with e-objects. This is because product safety is understood in the traditional sense only with regard to their potential harm to consumers' health and physical integrity such as through exposure to harmful chemicals and injuries. This is outdated knowing that devices which can connect to the internet can be hacked and thereby create new vulnerabilities from distance.

Another severe shortcoming in the legislative framework is the fact that the **Product Liability Directive** which dates from 1985 does not cover software.

Also, a recent proposal from the European Commission for a Regulation suggests to establish a **European Cybersecurity certification scheme**. Such scheme would attest that ICT products and services have been certified in accordance with specific security requirements (e.g. ensure that ICT products are provided with up to date software that does not contain known vulnerabilities and are provided mechanisms for secure software updates). The proposed scheme however is only voluntary.

2. Purpose of the study

Consumer organisations urgently need to develop a concept on how the legislation should be fixed to effectively protect consumers from new risks that are posed by products that can connect to the internet. This requires a different legal concept of a 'safe product' which is much broader and which includes security.

The purpose of the project is the following:

- List the specific challenges in terms of safety and security that are created by connected products;
- provide an overview about the traditional concepts of (product) safety/conformity and security and how these concepts would need to be updated in legislation to properly protect consumers;
- propose policy recommendations on how the legislative framework need to be updated to ensure consumer safety (risk assessment and risk management).

3. Scope

The contractor is asked to:

- Summarize the specific challenges for consumers in terms of safety and security linked to connected products
- provide for an inventory of the different concepts of 'safety' and of 'security' in existing EU legislation on consumer products and services and worker protection.
- Describe how the legislation that protects security and safety for connected products enforced (through national public authorities : which ones, with what mandate and what powers)
- Identify the challenges that the arrival of new technologies such as e-Objects pose to these traditional definitions and how the concepts get blurred/ overlap, as well as their consequences on consumer safety.
- Identify potential opportunities of intervention via security provisions in, eg, data protection and electronic communication legislation.
- Where appropriate, give recommendations on how the law and in particular the concept of 'safety' should be changed to ensure continued consumer safety also in an era of connected products. This needs to include recommendations on the safety of the objects themselves as well as their potential risk to and through their connectivity to a larger network.
- Be specific in the recommendations on which legal approach of the following options would be most feasible way forward for BEUC and ANEC's advocacy work:

  1) a new horizontal solution that need to be developed by the legislator from scratch and which would apply to all consumer products that can connect to the internet (i.e. a separate 'Safe Internet of Things' legislation for consumer products)

  2) a sector specific approach only (for example changing the toy safety directive, the machinery directive etc.) or

  3) a mix of both through adapting existing pieces of horizontal legislation (i.e. the General Product Safety Directive and the Product Liability Directive and updating all sector specific legislation.

- Assess whether a voluntary European Cybersecurity certification scheme can contribute to enhance consumer safety.

When deciding on one of these solutions, the following criteria should be taken into account:

- Which option provides for the best level of safety for consumers?
- Are there differences regarding legal certainty and enforceability?
- Are there differences in the timeline, i.e. are certain options achievable quicker than others?

The contractor should present the recommendations through showing visually how the different pieces of legislation relate to each other in an overview which is easy to understand for selected audiences (such as journalists, policy makers).

4. Methodology

The methodology to be adopted by the contractor needs to fulfil the purpose and scope of this research and shall be illustrated within the proposal.

5. Project planning and timeline

The research project is expected to be concluded within 4-months after the conclusion of the contract.

The contractor shall account for a face to face or skype meeting with the BEUC/ANEC project advisors to discuss the design of the report at the beginning of the study. Feedback shall be provided and when necessary conference calls should be held with the project advisors.

A draft report should be presented after 3 months upon conclusion of the contract. A meeting or phone conference should take place to discuss out comments on the draft report.

The final report must be approved by BEUC and ANEC.

6. Contractor requirements

The successful contractor must have an appropriate track record in this type of research in the specific area of consumer product safety and the Internet of Things. The contractor should provide information on the experience of the personnel who will manage and undertake the project.

7. Costs

A full outline of the costs shall be submitted with the proposal giving details of how the costs are to be attributed. The contractor will be asked to break down the overall costs of a maximum of 12.000 € (VAT excluded) based on work-days needed, including the time required for the different personnel who will be involved in the project and the daily rates of such personnel.

8. Publication and dissemination of the report

The contractor is expected to send the report electronically in pdf and in word version. The copyright of the report is granted to BEUC and ANEC under a non-exclusive license. The authors are free to use the data and information collected in the context of the study for publication in peer reviewed journals provided two conditions:

- Inform BEUC and ANEC before any publication and seek prior approval;

- Indicate clearly that the article is a study carried out for BEUC and ANEC, but does not reflect the position of BEUC or their members.

9. Contact persons

For any follow question, please contact:

- BEUC : Sylvia Maurer, Head of Safety and Sustainability : Sylvia.maurer@beuc.eu
- ANEC : Chiara Giovannini, Deputy Secretary General : chiara.giovannini@anec.eu

Offers should be sent **by 18 February 2018 to**
safety@beuc.eu and cgi@anec.eu