FACTSHEET

How the EU can make smart products consumer-proof

The Internet of Things may be the hottest topic of the late 2010s. It all boils down to this: many new products can connect to the Internet. And not just televisions or thermostats. Even some coffee machines, rubbish bins and plates now have the means. Not to forget about cars.

Regardless of the hypothetical added value of a coffee machine being connected, the question looms how consumers can make the most of this array of new products on the market. What risks are they exposed to? Is people's safety, security and their right to privacy safeguarded?

Tests by consumer groups reveal this is often not the case and point to flaws in our legal system. One of the roots lies in EU law defining 'safety' solely in terms of protection against physical damage. Safety, in legal terms, is too narrow and fails to protect consumers from security flaws that smart products may have. And this has repercussions for our safety, privacy, finances (theft) and property.

What are the new risks that come with connected products? Evidence from the ground

Test Achats / Test Aankoop (Belgium)

The Belgian consumer group asked ethical hackers to test 19 smart home appliances: nearly half contained flaws. In one case the hackers managed to install a malicious app on a children's tablet in less than a minute. This allowed them to monitor the images of the tablet's camera, eavesdrop through its microphone and control its Internet browser function.

Consumentenbond (Netherlands)

A test of 9 smart home devices – including security cameras, a robot vacuum cleaner, printer and toothbrush – revealed their sloppy security. 5 out of 9 apps were not sufficiently encrypted and therefore prone to misuse.

Forbrukerrådet (Norway)

Smartwatches that can be hacked and turned into snooping devices? Or connected toys that can easily be taken control of by a person in the vicinity? The Norwegian consumer group has unveiled this and more.

Which? (United Kingdom)

In the UK, ethical hackers were unleashed on popular smart appliances in homes. 8 out of 15 tested appliances included at least one security flaw. An example is wireless cameras that hackers were able to manoeuvre, allowing them to monitor activity in the house.

These tests unveil shortcomings in our policy-making today...

All products by law must be physically safe for consumers. But such requirement does not include a product's cybersecurity.

Relevant EU law

General Product Safety Directive. Various product-specific laws on toys, electric appliances and machinery.

Problem | Product safety law only covers potential harm caused by physical products to consumers' health and physical integrity. It neither accounts for harm caused by deficient services nor vulnerabilities that occur by strangers accessing and misusing a connected product.

BEUC The European Consumer Organisation

ANEC

This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme

Wireless devices are only required to be safe for our physical safety, not our cybersecurity.

Relevant EU law
Radio Equipment Directive

Problem | In line with the previous problem, wireless devices – which cover the vast majority of connected products – are similarly only required to respect physical safety. The current law does contain a clause that can address data protection/privacy issues and effective software installations (updates), the problem is that it lies dormant: follow-up legislation (a so-called delegated act) is required to activate the clause. In addition, a horizontal cybersecurity requirement must be added to the Directive.

A wrong approach in Europe to tackle the lack of security in connected products.

Relevant EU law
The proposed Cybersecurity Act

Problem | Even where the European Commission makes proposals with effect to such products, they focus on general and non-binding measures. This is demonstrated by the proposed Cybersecurity Act, which would lead to a voluntary scheme that business can use to get a certificate when a product complies with particular requirements. Yet what consumers would need is for their products to have mandatory cybersecurity requirements, such as security updates, strong passwords or encryption.

Product liability law does not clearly cover Internet of Things (IoT) products.

Relevant EU law
Product Liability Directive

Problem | As IoT products can be hacked, they can be turned into dangerous products. Yet it is currently unclear whether consumers who suffer damage from this can seek compensation related to cybersecurity hazards.

Authorities are not ready to perform effective market checks for connected products.

Relevant EU law
The proposed Goods Package (Regulation on Compliance and Enforcement, Regulation on the Mutual Recognition of Goods)

Problem | The lack of a state-of-the-art definition of 'safe' products means spot checks by authorities are not effective in weeding out unsafe products from the market. Consumer groups' testing clearly shows digital products fly under the radar of market supervision.

Policy recommendations?

For people to harness connected products, consumer groups recommend to:

- Ensure consumers' right to security.
- Forge a horizontal EU law that cuts across product groups and demands that connected products are secure by design & default.
- Activate the existing-yet-dormant clause that instructs connected products to meet data protection/privacy and software requirements, for example. The European Commission should do this by adopting a delegated act within its Radio Equipment Directive which would contain a list of connected products.
- Add a horizontal cybersecurity requirement to the Radio Equipment Directive.
- Urge EU and national authorities to talk to their global counterparts about the challenges for product safety posed by connected products.
- Dedicate research grants under the EU's Horizon programme to investigate how issues with connected products can be effectively addressed.