The Consumer Voice in Europe

PROTECTING EUROPEAN CONSUMERS IN THE WORLD OF CONNECTED DEVICES

Position Paper

Contact: Frederico Oliveira da Silva – digital@beuc.eu

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2021-091 15/10/2021

Contents

Why it matters to consumers

In recent years, connected devices have become omnipresent in the lives of many consumers. From connected coffee-makers and security cameras to cars and medical devices, the rise of connected devices is changing the way we conduct our lives. While digitalisation of devices provides many benefits for consumers, the risks and challenges it brings are equally important, if not even greater. For example, what happens when the service provider of your smart home system decides to shut down their servers? And who is responsible if your smart TV is compromised or rendered useless because of a lack of software updates? It is therefore important to develop clear and forward-looking EU policies and a legal framework that ensure that consumer rights are maintained in this connected environment.

Summary

The European Commission's last horizontal policy assessment about the Internet of Things - staff working document "Advancing the Internet of Things in Europe"[1] – was published in 2016.[2] We call on the European Commission to renew its strategy and put forward concrete policy measures aimed at improving the levels of consumer protection in the Internet of Things.

Key BEUC recommendations:

1. Cybersecurity: the European Commission should propose a new horizontal cybersecurity law which establishes mandatory, minimum, security requirements for all connected devices.
2. Safety: the definition of 'safety' in the proposed General Product Safety Regulation (GPSR) and sector specific legislation should be broadened to include (cyber)security aspects that have an impact on safety.
3. Data Protection:

- Manufacturers and service providers should make sure that connected devices are fully compliant with the GDPR and the ePrivacy Directive.
- Swift adoption of a strong ePrivacy Regulation that updates and reinforces the protection of the confidentiality of communications and consumer's connected devices is essential.

4. Artificial Intelligence: the Commission's AI Act proposal should be amended to ensure that it properly regulates medium and low risk AI applications, not only those to be considered as 'high risk'. Connected devices with AI intended for consumers should fully fall under the scope of the Regulation.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016SC0110

[2] Sveriges Konsumenter and AK Europa, BEUC's Swedish and Austrian members respectively, have recently published a position paper on the Internet of Things:

http://sverigeskonsumenter.se/nyheter-press/pressmeddelanden/konsumentrorelsens-krav-pa-sakernas-internet/

https://www.akeuropa.eu/sites/default/files/2021-02/Consumers%20expectations%20of%20the%20Internet%20of%20Things_0.pdf

5. Software updates:

- Security and functionality updates should be provided separately.
- Security updates should be provided by the manufacturers and service providers during a minimum period of time which must correspond to the expected lifespan of the product and its associated service.
- Manufacturers must ensure that consumers, including those who are not tech-savvy, can easily install updates.

6. Contractual rights:

- In line with Articles 5 and 6 of the Consumer Rights Directive, essential information regarding the functionality and limitations of the connected device, including data protection and security policies, must be clearly presented to consumers before purchase and in case of off-line shops, at the point of sale.
- The list of possible unfair contractual terms in the Annex of the Unfair Contract Terms Directive should be updated to include contractual terms that are considered unfair in the Internet of Things (e.g. allowing manufacturer to modify the terms without a valid reason and/or without informing consumers).

7. Product Durability:

- The upcoming revision of the EU Ecodesign directive should put a much stronger focus on durability, repairability, reusability and other circularity aspects of IoT products, including but not limited to availability of software updates and spare parts, repair information, requirements on interoperability, modularity and ease to disassemble.
- The European Commission should take into account the impact of connected devices in the environment (in terms of energy consumption and risk of increased electronic waste) and the role respective policies have to play to achieve a green transition.

8. Product Liability: the Product Liability Directive (PLD) must be amended and adapted to the multiple challenges brought by new technologies, which includes the development of connected devices. For example, the notion of 'product' should be revised, to consider its full digitalised dimension in which tangible items, digital services and digital content interact and cannot be differentiated

9. Interoperability and competition: following-up on its recent sector inquiry, the European Commission should, where appropriate, open investigations regarding practices undermining competition and consumers' interests in Internet of Things markets.

10. Connectivity and net neutrality:

- In line with the European Electronic Communications Code and the Open Internet Regulation, public authorities should ensure that consumers have access to a stable, adequate broadband internet connections in a non-discriminatory way. Connected products can be used as expected and needed by consumers.

11. Enforcement:

- Consumers should have a right to redress, including collective redress, if connected devices cause them damage. The EU legislator must ensure that any relevant legislation will be included into the material scope of the Representative Action Directive (e.g., the newly proposed AI Act).
- Complaints handling and redress mechanisms should be accessible, affordable, independent, fair, accountable, timely and efficient.

1. Introduction

In the span of the last few years, connected devices have become ubiquitous in the lives of many consumers. Whereas before we would normally be in front of a computer to access the internet, we now carry internet-connected smartphones everywhere we go. Simultaneously, an increasing amount of the everyday devices around us are being fitted with sensors and connected to the internet. From connected coffee makers and security cameras to cars and medical devices, the rise of connected devices is commonly known as the "internet of things", or IoT.

Connecting large amounts of devices to the internet raises both opportunities and risks for consumers. The interconnected world promises increased comfort, seamless experiences, and potentially significant improvements to quality of life. Aggregated information from these devices could also lead to new insights in areas such as medical science, artificial intelligence, and city planning.

For example, a smart home filled with connected devices and sensors may learn the habits and preferences of its owner, and tailor its functionality accordingly. Simultaneously, the different individual devices can communicate with each other, so that for example a low cardiac rhythm detected by a smart watch generates an urgent message to the closest hospital. Furthermore, the capability of remote monitoring of devices through the internet can help individuals who are in need of assistance retain their independence, for example by unlocking doors remotely without the need of walking to the door. In sectors such as industry and health, the internet of things is set to have potentially transformative effects on efficiency and information accumulation.

In order to further develop and customise connected devices and their services, connected devices will typically collect vast amounts of data about its users and its environment. This widespread data collection raises a number of pressing concerns related to data protection and privacy. As more aspects of our lives are increasingly embedded in a wider network of sensors and devices, the potential risks and scope of data breaches and cyberattacks also grow. Every new device we connect to the internet adds another potential attack surface, and the chain of devices is often only as strong as its weakest link. The emergence and implementation of artificial intelligence in IoT technologies also poses challenges related to fairness, accountability, and more.

Other challenges that are introduced or exacerbated through the internet of things include artificial limitation of product lifecycles, lock-in effects and product liability. For example, what happens when the service provider of your smart home solution decides to shut down their servers? And who is responsible if your smart TV is compromised or rendered useless because of a lack of software updates?

Also, networked devices have an increased energy consumption due to their required networking components. A large part of this energy consumption arises from the continuous responsiveness of the devices via the network (idle mode). Friedli et al. (2016) projected that global standby losses will increase from 7.5 TWh in 2015 to 47 TWh in 2025, based on the standby consumption of networked devices that are permanently connected to the power grid.[3]

[3] https://nachhaltigwirtschaften.at/resources/iea_pdf/reports/iea_4e_edna_energy_efficiency_of_the_internet_of_things_technical_report.pdf

The European Commission's last horizontal policy assessment about the Internet of Things - staff working document "Advancing the Internet of Things in Europe"[4] – was published in 2016. At the time, the complex ecosystems and supply chains of the internet of things, together with the rapid growth and adoption of the technology, underscored the need for a new coherent strategy that develop clear and forward-looking EU policies and a legal framework that ensure that consumer rights are maintained in the connected environment. Unfortunately, five years later and at a moment where the number of connected devices in the EU market is skyrocketing, the European Commission has not followed-up on their 2016 publication with a strategy and concrete policy measures aimed at improving the levels of consumer protection in the Internet of Things.

2. Cybersecurity and safety

2.1. Cybersecurity

Connected devices differ from other products due to the inclusion of embedded software and their connectivity. The inclusion of embedded software is essential for digital devices and allows for a range of features. However, software is dynamic, and can be affected and/or changed through software updates ("patching"). When vulnerabilities appear, devices with embedded software may be subject to remote attacks or exploitation, for example through remote access by hackers. This presents new challenges to the safety of consumers, who normally have no way to assess cybersecurity risks in connected devices.

As demonstrated by several of our member organisations, many connected devices suffer from poor cybersecurity. Many IoT-manufacturers and developers either lack the necessary experience and competence to secure their devices, or simply neglect these responsibilities in the rush to push their products onto a swiftly changing market.[5]

Already back in 2016 a campaign by our Norwegian member Forbrukerrådet– #ToyFail[6] – looked at the technical features of popular connected toys sold on the EU market. Forbrukerrådet discovered that with a few simple steps anyone could connect to a children's doll named Cayla, one of the connected toys tested, and speak to the kids using the toy, thus putting the child's physical *safety* and privacy at risk.

A second campaign launched by Forbrukerrådet in October 2017 (#WatchOut[7]) tested the security features of smart watches whose main function is to enable parents to keep in touch with their children and track their real-time location. Again, Forbrukerrådet discovered serious security flaws in these devices, including the possibility for an attacker to easily change the geo-location of the watch ('location spoofing') and to track and contact the child directly.

In August 2021, our Belgian member, Test Achats/Test Aankoop, installed several popular smart devices (including a baby phone, an alarm system, a smart TV, a Kitchen Robot, a door lock, a speaker and a vacuum cleaner robot) in a house and challenged cybersecurity researchers to find security vulnerabilities. 10 of the 16 devices were found to have a "critical" or "severe" vulnerability.[8]

---

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016SC0110

[5] Exacerbating the problem, a large number of IoT-devices are designed using cheap, small, and/or low-energy components, which for various technical reasons cannot accommodate sufficient security measures.

[6] https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/

[7] https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf

[8] https://www.test-achats.be/hightech/smart-home/presse/la-securite-des-appareils-domestiques-intelligents-est-une-veritable-passoire

In recent campaigns, our members Which?[9], Stiftung Warentest[10], OCU[11] and Consumentenbond[12], consumer organisations from the United Kingdom, Germany, Spain and The Netherlands respectively, found similar security flaws in other connected consumer devices.

Cyberattacks and computer viruses are not a novel phenomenon but may take many new shapes and create new levels of risk when manifesting through the internet of things. For example, a typical "ransomware" attack may lock you out of computer until you pay a monetary ransom.[13] In the internet of things, potential attack scenarios include hackers taking control of your security cameras,[14] shutting down your car[15], or even stopping your connected pacemaker.[16] Another example is the proliferation of so-called "stalkerware", software that is used or abused by malicious actors to spy on or otherwise abuse individuals.[17]

These examples of targeted attacks illustrate how lax or non-existent security measures in connected devices could have potentially devastating real-world consequences for consumers.

Unfortunately, despite the serious risks outlined above, the EU still lacks solid legal requirements to ensure the cyber security of all connected consumer products available in the EU market.

The EU's Cybersecurity Act (in force since June 2019) does not remedy the situation because the framework for certification schemes it introduces is only voluntary for businesses, rather than mandatory (Article 56 (2)). Moreover, the European Commission will only roll out these voluntary schemes incrementally over time, so any potential positive impact will still take time to materialise.

The General Data Protection Regulation (GDPR) can play a role in ensuring secure connected devices. If strong authentication mechanisms such as unique passwords are implemented to ensure the security of personal data, harmful attacks become more difficult. However, the GDPR has several limits. For example, the GDPR applies to the data controller and processor, which are not always the manufacturer of connected devices. Also, the GDPR does not include public enforcement intervention measures from data protection authorities such as the withdrawal of a noncompliant connected product from the market.

The Radio Equipment Directive (RED) could potentially address some of the cybersecurity-related issues with connected devices. BEUC strongly supports the European Commission's recent progress on the activation of the RED cybersecurity provisions (Articles 3 (3) d), e)

---

[9] https://www.bbc.com/news/technology-54339973

[10] https://www.test.de/Smart-Toys-Wie-vernetzte-Spielkameraden-Kinder-aushorchen-5221688-0/

[11] https://www.ocu.org/organizacion/prensa/notas-de-prensa/2017/juguetes-conectados-201217

[12] https://www.consumentenbond.nl/nieuws/2019/deel-beveiligingscameras-te-hacken

[13] Ransomware is a type of malicious software from crypto virology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. (Definition from Wikipedia) https://en.wikipedia.org/wiki/Ransomware

[14] https://www.bleepingcomputer.com/news/security/new-hacking-tool-lets-users-access-a-bunch-of-dvrs-and-their-video-feeds/

[15] https://video.wired.com/watch/hackers-wireless-jeep-attack-stranded-me-on-a-highway

[16] https://www.wired.com/2016/03/go-ahead-hackers-break-heart/

[17] https://www.wired.com/story/eva-galperin-stalkerware-kaspersky-antivirus/

and f)).[18] In this regard, BEUC has been advocating for a delegated act with a broad scope (i.e., applicable to all devices falling under the scope of the RED) and with a short date of applicability (i.e., delegated act in force no longer than 12 months after its publication). However, even if the full potential of the RED will be used, the Directive cannot ensure security by design and by default of all connected consumer products (e.g. scope does not cover all consumer connected devices).

The current situation is dangerous, and it is key that the EU framework is adapted to ensure that all connected devices intended for consumers are secure by design and by default. This is only possible with the adoption of a new horizontal regulatory instrument that implements a set of baseline cybersecurity requirements.

We welcome that President Von der Leyen announced a new 'European Cyber Resilience Act' in her 2021 State of the Union speech.[19] As confirmed by Commissioner T. Breton, this Act will establish common European cyber security standards for products (especially connected objects) and services that are placed on our market.[20]

New horizontal rules should require manufacturers of connected devices to, at the minimum, implement the following security requirements:

Security updates: When put on the market, connected devices should be protected against any known vulnerabilities. Security updates must be made available for the duration of the expected lifespan of the product and in line with consumers' expectations.[21]

Strong authentication: secure authentication methods should be implemented in every device. For example, unique and complex passwords should be the default setting of connected products and consumers should be required to choose strong passwords in case they want to change the default one. Also, two factor authentication should be mandatory.

Encryption: Companies must encrypt the data which are transmitted and stored by products and services they produce.

BEUC recommendations:

- In line with the announcement in President Von der Leyen's 2021 State of the Union speech, the European Commission should propose a new horizontal cybersecurity law which establishes mandatory, minimum, security requirements for all connected devices.
- Products should be secure during a minimum period of time which shall correspond to the expected lifespan of the product and its associated service (e.g. apps).
- The European Commission must swiftly adopt the delegated act that will activate the cybersecurity provisions of the Radio Equipment Directive. This delegated act must have a broad scope (i.e., applicable to all devices falling under the scope of the RED) and be applicable quickly (no longer than 12 months after the publication of the delegated act).

[18] The RED's relevant provisions are not fully applicable and effective, because a complementary EU secondary act (so-called delegated act) needs to be adopted by the European Commission. The European Commission recently opened a public consultation to comment on the draft delegated act.

[19] https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701

[20] https://www.linkedin.com/pulse/how-european-cyber-resilience-act-help-protect-europe-thierry-breton/?published=t

[21] For more information on updates, please see Section 5.

2.2. Safety

Thanks to the General Product Safety Directive and sector-specific legislation, such as the Radio Equipment Directive or the Toys Safety Directive, manufacturers are obliged to only place safe products on the EU market. However, the concept of 'safety' is interpreted too narrowly. It is not clear whether new risks, in particular safety risks related to a security vulnerability, also known as 'cybersafety' risks (e.g. cybersecurity vulnerability in a connected smoke alarm might endanger the safety of its users), fall under the scope of the current product safety rules.

The regulator needs to make sure that cybersecurity flaws that can have an impact on the safety of consumers are covered by the definition of 'safety'. An expanded definition of 'safety' so as to include cybersecurity, will allow the legislator to make a safer product design mandatory and enable market surveillance authorities to act quickly in alerting consumers, and remove products where a lack of cybersecurity can have an impact on the safety of the consumer.

In the Internet of Things era, we can't talk of users being safe if their cybersecurity is compromised. The connected toys that were tested by our members could be considered safe according to today's product safety legislation, but they still have serious cybersecurity risks that might endanger the physical safety of their users.

Furthermore, the current provisions of product safety legislation require a product to be safe when it is sold. There is no further specification on how far a producer must monitor over time the behaviour of a product in the market, including with the provision of regular software updates. With an increasing number of connected products in use, this concept needs to be replaced with a concept of 'continued conformity' and a requirement on producers to carry out continuous conformity assessment against appropriate standards.

This would require companies in the supply chain to make sure that products are both safe and secure when being placed on the market and during the whole duration of their expected lifespan. This concept should ensure that safety risks related to (lack of) software updates or connectivity, for instance, are addressed even after a product has been placed on the market.

BEUC recommendations:

- Ensuring that the final version of the proposed General Product Safety Regulation (GPSR) and sector specific legislation include (cyber)security aspects that have an impact on safety.
- Ensuring that the concept of 'continued conformity' is introduced in EU product safety legislation such as the proposed GSPR. This would require companies in the supply chain to make sure that products are both safe and cybersafe when being placed on the market and during the whole duration of their expected lifespan.
- Ensuring that authorities have the necessary human, financial and technical means to enforce legislation.
- Designating EU laboratories in the context of the new market surveillance Regulation to develop technical expertise and guidance related to connected products and their safety.
- Making sure connected devices are blocked at external EU borders before import into the EU if no responsible person in the EU internal market has been designated.

3. Data protection and privacy

Many connected devices are designed to continuously monitor their surroundings through a multitude of sensors, for example detecting movement, air quality, sound, voice recognition, and so on. These sensors collect vast amounts of data about both their environment and their users, which is used for real-time adaptation based on context, and to customise and personalise user experiences according to the users' perceived needs. Additionally, companies selling internet-connected devices and services may treat this user data as an additional revenue stream, by using it for research and product development, or by selling data to third parties.

Connected devices that we use in our daily basis provide an exceptionally detailed picture of us as individuals, and this information can be used to create profiles about individual consumers. Such profiles are often used to target advertisements or other messages but can also be used to make decisions about us, for example to decide whether we are eligible for a loan or insurance premium.[22]

Many connected devices collect data that doesn't only relate to the user. For example, a smart speaker will collect data on anyone in the vicinity of the device.

3.1. General Data Protection Regulation

Information such as our daily habits and preferences is considered personal data under the General Data Protection Regulation (GDPR). Companies that collect personal data about consumers have to be sure that they process this data according to the rules set forth in the GDPR. These rules include, but are not limited to, the principles of data minimisation, purpose limitation and data protection by design, and the obligation to obtain user consent depending on the purposes of data processing.

Data minimisation (Art. 5 (1) c) GDPR): companies should only process the minimum amount of personal data that is necessary in order to provide their service to the user. For example, a connected TV may collect technical data that is necessary in order to connect to the internet (e.g. IP-address), but should not be collecting the particular viewing habits of individual consumers, unless the user has expressly consented to such data collection.

Data retention (Art. 5 (1) e) GDPR): companies should only keep connected devices' data for as long as technically necessary.

Purpose limitation (Art. 5 (1) b) GDPR): companies should not use personal data for other purposes than what it was originally collected for. For example, location data collected through a connected vehicle should not be used for insurance purposes, unless the user has given consent to such data usage. The principle of purpose limitation would often be in conflict with the concept of using internet of things data as an additional revenue stream. In most cases, reselling or otherwise sharing data collected from a personal internet of things environment, will not be necessary in order to deliver the service requested by the user.

Consent (Art. 7 GDPR): the small size and lack of a physical interface on many connected devices can make it difficult for users to know how their data may be used. To comply with the GDPR and depending on the purposes for which data is processed, users will often have to be asked for consent to their personal data being collected and used, and if the service-provider wishes to use this data for other purposes, users should be asked for a separate

[22] The use of personal data collected from connected devices in profiling and advertising is described in our member organization the Norwegian Consumer Council's report "Out of Control": https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf

consent in a clear and explicit manner. Consent should always be informed and freely given. In particular, service providers should not make the use of their devices contingent on the user consenting to the reuse of personal data for other purposes. Unlike purely digital services, connected devices have usually been purchased and unboxed before users have a chance to read the privacy policy or give their consent. This makes it particularly important that users have a choice about how their personal data is used, as it might not be possible to back out of the purchase if one does not wish to consent to the processing of personal data.

Data protection by default and by design (Article 25 GDPR): privacy-preserving and enhancing technologies should be part of the design of a product or service from the beginning of development. The principle of data protection by default includes that settings should be set to the most privacy-friendly option by default, while less privacy-preserving settings should require the user to opt-in. As an example, a fitness wearable could include the option to share fitness data through a social network. Such a setting should not be enabled by default.

Security of processing (Article 32 GDPR): companies must implement a risk-based approach and put in place technical and organisational measures to ensure a level of security appropriate to the risk. These measures include the pseudonymisation of data and other well-known security principles better known as the 'CIA triad' (ensuring the confidentiality, integrity, availability and resilience of processing systems).

Data portability (Art. 20 GDPR): Consumers must be able to easily move their personal data between service providers.

The rules and principles of the GPDR are paramount. However, it is important to underline that not all manufacturers of connected devices will be forced to comply with its rules as these only apply to situations in which the manufacturer is the processor or the controller of personal data.

3.2. ePrivacy Regulation

Connected devices would normally be considered terminal equipment and send data over publicly available communications networks. In this sense, it is essential to preserve the confidentiality of such communications and ensure that connected devices are protected against any unauthorised access. These issues normally fall under the scope of the ePrivacy Directive.

In 2017, the European Commission put forward a proposal for an ePrivacy Regulation (ePR), which would replace the existing Directive. The ePR, which is meant to update the current rules and ensure legal coherence with the GDPR, has not been adopted yet. The Parliament already adopted its position back in October 2017 while Council only reached a position in February 2021. It is crucial that the new regulation provides a high level of protection for consumers and duly covers aspects related to IoT.

BEUC recommendations:

- Manufacturers and service providers should make sure that connected devices are fully compliant with the GDPR and the ePrivacy Directive.
- Swift adoption of a strong ePrivacy Regulation that updates and reinforces the protection of the confidentiality of communications and consumer's connected devices is essential.

4. Artificial Intelligence

Connected devices generate a huge amount of data which needs to be collected and processed for the sake of providing a service or for the functioning of the products themselves. Artificial Intelligence (AI) and Automated Decision Making (ADM) power connected devices and accelerate these processing activities via the use of powerful algorithms. These algorithms convert the data into actionable results that can be implemented by the connected devices. While this capacity to manage big datasets in shorter time comes with big promises to make consumers' lives easier and societies better, the widespread use of AI and ADM technologies in consumer products also raises many concerns.

In September 2020, BEUC published a survey about consumer perceptions regarding AI. The results of this survey show that consumers have high expectations about AI, but also that they fear AI is used to manipulate them and subject to discriminatory treatment and arbitrary decisions. Consumers also consider that the current regulatory framework is not adequate to protect them and address the challenges posed by AI.

In April 2021, the European Commission presented its proposal for an Artificial Intelligence Regulation.[23] While we strongly support the European Commission's intention to introduce a legislative framework for AI in the EU, we have doubts about the effectiveness of the Regulation proposed by the European Commission, in part because of its limited scope.[24]

When it comes to connected devices with AI, a large majority of them (e.g. personal assistants, smart thermostats) will not be classified as 'high-risk AI' under the proposed Regulation. While manufacturers of these devices might need to apply standards that cover the requirements applicable to high-risk AI in certain situations[25], the obligation to comply with the main requirements established in the Regulation such as the need for human oversight of the AI or transparency, will not apply to them.

BEUC recommendations:

- The Commission's AI Act proposal should be amended to ensure that it properly regulates medium and low risk AI applications, not only those to be considered as 'high risk'. Connected devices with AI intended for consumers should fully fall under the scope of the Regulation.
- Legal obligations for producers and users of AI systems should gradually increase in line with the identified level of risk, starting from the principle that some basic principles and obligations (e.g. regarding fairness and transparency) should be applicable to all AI applications. Thereon, the greater the potential of algorithmic systems to have adverse impacts, the more stringent the legal requirements should be.

5. Software updates

Some connected devices are relatively low-cost items used for short-term purposes, such as certain connected toys. Others, such as connected home appliances, have significantly

[23] Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts.

[24] See BEUC's position paper on the AI Act for more information.

[25] Article 43 (3) of the AI Act proposal.

longer lifespans. Unlike traditional "analogue" devices, which can be used until they physically break, connected devices rely on both physical and digital maintenance.

It is important that such devices receive digital support during their lifetime, for example in the form of software updates, to ensure that they will continue to function securely and safely as intended. If the digital support ceases, the device may become unusable[26] and/or put consumers' privacy and safety at risk.

In a recent opinion, the 'Sub-Group on Artificial Intelligence (Ai), Connected Products and other new challenges in Product Safety' to the Consumer Safety Network (CSN) also highlighted the necessity to move from the static concept of safety at the time of first commercialisation of a product to the concept of *continuous conformity*. In other words, at the time of the design, the producer of a connected device needs to take into account the probability of subsequent modifications to this product, including software modifications. In this context, if a software update leads to a safety or security issue, it means that the concept of continuous conformity was not respected.[27]

Software updates for connected devices come in large numbers and concern various issues (security, functionality, resolving a bug, etc.).

5.1. Security updates

When consumers use a connected product such as a mobile phone, a smart TV or a connected toy, they have the right to a product that is as secure as possible considering the state of technology at the time. Many cybersecurity attacks are only possible precisely because the security protections of connected products are inadequate or outdated.

This is why it is so important that manufacturers and service providers provide the necessary security updates in a swift and efficient manner during a minimum period of time which must correspond to the expected lifespan of the product. Naturally, it is equally important that such security updates do not create additional risks to those they are trying to solve.

Consumers should be informed before purchase about the expected lifespan of a specific product.[28] This period should reflect the timeframe for which manufacturers will provide security updates.

Consumers should be informed before purchase about the end-of-life policy for that specific product. This policy must include information for consumers regarding the date until which manufacturers will provide security updates.[29]

One major challenge that consumers face when purchasing a connected device is to know what they can/should do with a device that is no longer receiving software updates and is thus no longer supported by its manufacturer. The lack of support in the form of security updates renders devices vulnerable to malicious attackers. As a consequence, consumers face serious risks such as break-ins if their smart door lock is hacked.

[26] This is what happened with Revolv, a smart hub-system that was acquired by Google. When Google decided to shut down the servers, the owners were left with useless devices: http://uk.businessinsider.com/revolv-smart-home-hubs-lifetime-subscription-bricked-nest-google-alphabet-internet-of-things-2016-4

[27] In this context, manufacturers cannot be held responsible when the safety or security vulnerability is due to a substantial modification introduced by a third party.

[28] For more information on BEUC recommendations in this area, see BEUC position paper "Durable and repairable products: Changes needed for a successful path towards the green transition", BEUC-X-2021-061

[29] See Section 6.1 for more information on information to consumers.

In any case, the main features of a device that does not per se require connectivity should continue to work when the product or service is not connected to the internet (e.g. connected water kettle should still heat water if disconnected).

5.2. Functionality updates

In addition to the challenges related to security updates, functionality updates, including those linked to the operating system (OS), can also be a problem for consumers. Too many functionality updates, or the lack of them, may reduce the functionality or performance of the device considerably.

It is important to enhance and improve the transparency of software updates for consumers. At present, it is not always clear to them whether the proposed updates are necessary to improve security, to resolve a software bug, or to install new functionalities, or whether they serve other purposes.

Functionality and security updates must be provided separately. In this regard, manufacturers must clearly explain the reason of the update (functionality or security), its impact on the product, and importantly, must not misuse the update for example to unilaterally change the conditions of the service.[30] This is the only way consumers can correctly assess the purpose (security issue or functionality issue) and importance of the provided update.

In November 2020, the Italian Antitrust Authority found that HP, since (at least) the end of 2016, misled consumers by encouraging them to update their new firmware while omitting to inform them of the impact it would have on the use of non-original ink/toner cartridges (i.e. supplied by third parties). This was done in order to falsely persuade consumers not to use third party cartridges or to have them replaced because they were defective or lacking quality. Recently, Test-Achats, OCU, DECO Proteste and Altroconsumo, our Belgian, Spanish, Portuguese and Italian members respectively, asked HP to pay damages to consumers.[31]

5.3. EU legal framework

According to the directives on digital content and sales of goods, connected devices must be supplied with updates, including security updates, for the period of time that consumers can reasonably expect. (Articles 8 (2) Digital Content Directive and Article 7 (3) of the Sale of Goods Directive). According to their respective Recitals 47 (DCD) and 31 (SGD), the length of this obligation is linked to the legal guarantee period but can also go beyond it. While these rules generally favour the consumer, there must be security updates and digital support during the lifespan of the product, not just during the legal guarantee period.

Another shortcoming of the Digital Content and Sales of Goods Directives is the fact that the entity responsible for providing updates is the seller and not the manufacturer of the device.

The Cybersecurity Act (CSA) also addresses the issue of updates. Article 56 (1) b) of the CSA determines that manufacturers of certified products must provide information regarding the period during which security support is offered to end users, in particular as regards the availability of security updates. While we strongly support the reasoning behind this rule, the certification schemes put in place by the CSA are voluntary in their nature.

[30] See Section 6.2 for further development on Terms and Conditions.

[31] https://www.euroconsumers.org/Activities/printergate-euroconsumers-asks-hp-to-compensate-printer-owners-up-to-eur150

In other words, manufacturers will only have to comply with this transparency obligation regarding updates if they opt to certify their devices with a specific certification scheme.

BEUC recommendations:

EU legislation, including digital sales laws, a new horizontal cybersecurity law, the proposed General Product Safety Regulation and Ecodesign Directive, must ensure that:

- Security and functionality updates should be provided separately. Manufacturers must explain the reason of the update (functionality, security, etc.), its impact on the product, and importantly, must never misuse the update, for example, to unilaterally change the conditions of the service.
- In exceptional circumstances where there is an increased risk to the safety of consumers (e.g. when using a self-driving car), security updates can be installed automatically. However, in this case, the update should only be processed automatically on the condition that

  (i) consumers are notified about it immediately,

  (ii) the update does not negatively affect the performance of the connected device and

  (iii) manufacturers are not circumventing the rules on consent established by the data protection legislation, including the ePrivacy Regulation, under the disguise of critical security updates.
- Security updates should be provided by the manufacturers and service providers during a minimum period of time which must correspond to the expected lifespan of the product and its associated service.
- The manufacturers and service providers' end-of-life policy must be clear to the consumers before purchase. Such policy shall explicitly mention the period until which updates, including security updates, will be provided.
- Consumers should be informed about the different possibilities once the manufacturer is no longer supporting the product (e.g. disconnect from the internet; dispose it in a responsible way; repairability options; making source code available; possibility to use offline; possibly to use with less functionalities).
- Manufacturers must ensure that consumers, including those who are not tech-savvy, can easily install updates.

6. Contractual rights

6.1. Contractual information

The Consumer Rights Directive has, at its core, the idea that consumers must be given essential information so that they can make an informed purchasing decision (Articles 5 and 6 CRD). According to this Directive, consumers have the right to receive essential information about the product (e.g. its characteristics or its price) before buying it.

It is important that essential information about functionality and possible limitations are clearly presented to the consumer at the point of purchase and not hidden, for instance, in the terms & conditions. For example, if the device requires an app, a stable internet connection or a subscription[32] to function as intended, this should be made clear to the consumer prior to purchase.

[32] https://twitter.com/airavn/status/1375200803393318913

Consumers should also be informed about the business model of the device, in particular if the product is sold as a one-time payment, as a subscription service or a mixture (upfront payment and subscription).

Furthermore, as mentioned in Section 7, consumers should be given information regarding the period of time during which manufacturers will provide digital support to the connected device.

Finally, when it comes to information related to the GDPR, such as information regarding the use of personal data, while this information is not explicitly listed as pre-contractual information when selling products and services under the Consumer Rights Directive[33], it must be considered essential information and thus is obligatory pre-contractual information requirement provided before purchase under EU consumer law. In that regard, sellers should be required in the CRD to provide - without prejudice to the obligations of data processors and controllers under the GDPR - information related to the use of personal data of a given IoT product in a standardised and comparable manner at the point of sale.

6.2. Unfair contract terms

The complexity and multi-layered nature of connected products makes it difficult for consumers to understand how exactly those products and their associated services work, and whether their rights are being respected, hampering trust in such an environment. For certain devices, consumers would have to read many legal documents (e.g. terms of service, end-user licensing agreement, privacy statement, security policy, etc.) which are often extremely difficult to understand, leaving consumers unaware of their rights and obligations under the contract.[34]

Another important point is that the acceptance of software agreements imposed on consumers by licensors, service providers or third parties occurs at the moment in which they connect the device to the internet for the first time. This happens by way of 'clickwrap'. At this stage, the incentive for consumers to read the licensing agreements and to oppose them is very low: first, the price has already been paid; second, the connected device will not function without the provision of these associated services.[35]

Certain terms that are regularly used by manufacturers should be deemed unfair and thus blacklisted. For example, manufacturers often reserve the right to unilaterally modify the general terms and conditions of an ongoing contract related to a connected device. This raises several questions, in particular whether consumers have consciously consented to the new terms and whether such clauses are fair.[36]

The Court of Justice of the European Union already ruled on such clauses, in particular price amendment clauses in the context of consumer contracts. In *Invitel*, *RWE* and *Kásler*, the Court has consistently ruled that price amendment clauses are valid only if there is a valid reason for the change, the trader informs the consumer with reasonable notice before

[33] Directive 2011/83/EU on consumer rights

[34] Guido Noto La Diega and Ian Walden, *Contracting for the 'Internet of Things': looking into the Nest*, European Journal of Law and Technology, Vol. 7, Nº 2, 2016;

[35] Christiane Wendehorst, *Sale of goods and supply of digital content – two worlds apart?*, In Depth Analysis. European Parliament - Policy Department for Citizen's Rights and Constitutional Affairs, 2016, p. 9;

[36] Stacy-Ann Elvy, *Contracting in the age of the Internet of Things: Article 2 of the UCC and beyond*, HOFSTRA Law Review, Vol. 44.839, p. 882

the change is applied and the consumer is given reasonable time to terminate the contract.[37]

The same reasoning should be applied to similar clauses in the context of connected devices but also to other unilateral changes of contract, in particular clauses that modify substantially the rights and obligations of the other parties to the detriment of consumers. In this regard, when consumers have not been properly informed of the changes regarding the terms and of services[38], they should not be considered to have agreed with new contract terms solely because they continued to use the connected device.[39]

Under the Digital Content Directive, any unilateral changes to the digital content or digital service need to be compatible with the conformity criteria established in Article 8 of the Digital Content Directive, unless the trader has informed the consumer in advance.

BEUC recommendations:

- In line with Articles 5 and 6 of the Consumer Rights Directive, essential information regarding the functionality and limitations of the connected device, including data protection and security policies, must be clearly presented to consumers before purchase and in case of off-line shops, at the point of sale.
- The list of possible unfair contractual terms in the Annex of the Unfair Contract Terms Directive[40] should be updated to include contractual terms that are considered unfair in the Internet of Things (e.g. allowing manufacturer to modify the terms without a valid reason and/or without informing consumers).
- A summary of the most important elements of the terms and conditions (including the summary of the software's user agreement) should be provided to consumers before they enter into a contract (e.g. sharing / collection of personal data; who to contact in case of harm; any risks associated to the product).

7. Durability, premature obsolescence and right to repair

Whatever the cause, planned or not, the widespread early failure of connected devices, also called 'premature obsolescence', is an important challenge for consumers and a major obstacle to a sustainable economy.

In some cases, companies deliberately lead consumers to discard products in exchange for newer ones. In December 2020, Test-Achats and OCU, BEUC's Belgian and Spanish members respectively, launched class-action lawsuits against Apple over the planned obsolescence of the Apple iPhone 6.[41]

[37] Marco Loos, Joasia Luzak, *Update the Unfair Contract Terms directive for digital services*, European Parliament, Study requested by the JURI Committee, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, PE 676.006, February 2021.

[38] Recital 53 of the Digital Content Directive enables traders to derogate from the conformity criteria mentioned in Article 8 if "*the trader informs the consumer before the conclusion of the contract that a particular characteristic of the digital content or digital service deviates from the objective requirements for conformity and the consumer has expressly and separately accepted that deviation*".

[39] Ibid, p. 23.

[40] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

[41] https://www.test-achats.be/actions-collectives/apple-iphone

In a recent report, Which? discovered that despite costing hundreds of pounds more than their standard counterparts, connected devices could be rendered obsolete after as little as two years, as manufacturers stop providing vital software updates.[42]

The lack of product repairability is one of the key aspects contributing to premature obsolescence. Consumers face many barriers to repairing their connected products, including, for instance, the lack of repair information, availability or affordability of services. Also, product design complicates disassembling a device for diagnostics and repair. In a survey published in February 2019, the German Verbraucherzentrale Bundesverband found that 89% of consumers thought that the EU should oblige producers of large household appliances to make products more easily repairable.

Another important point is that due to the expected rapid growth in the number of connected devices, the use of raw materials and resources per device quickly adds up to quantities that are relevant for global consumption. Measures should thus be put in place to ensure that these devices are disposed in an environmentally responsible manner at the end of their life. For example, many consumers do not dispose of their old smartphones but leave them in a drawer, thus taking them out of the cycle and preventing their raw materials from being re-used. This should not occur with every connected device.

In this regard, a comprehensive sustainable product policy should also address the potential of more sustainable business practices. Renting, second-hand markets, collaborative or sharing economies, for example, have high potentials, as they can boost the uptake of more sustainable consumption practices among increasingly environmental conscious consumers. Thanks to reuse and repurposing of products, for example, fewer products are needed on the market to accommodate more people, which benefits the environment.

Premature obsolescence and consumers' 'right to repair' are high on the EU agenda. In her 2021 State of the Union Letter of Intent[43], President Von der Leyen announced a legislative proposal on the right to repair for 2022. Other upcoming policy initiatives such as the review of the Ecodesign Directive, as well as sector-specific legislation - such as the Circular Electronics Initiative – can also set requirements for longer lasting, repairable products by design. It is critical that the additional challenges posed by connected devices are considered. There is a risk that the lack of repairability of connected devices may lead to a large increase of prematurely discarded devices, posing a major risk to stated goals of sustainable and green consumption.[44]

Finally, devices with embedded software may also challenge traditional notions of ownership. Although the consumer may think that they are the owner of their smart fridge, consumers are actually only granted a limited license to the embedded software within the device. This could mean that they are not allowed to resell the device and could prevent consumers from repairing a malfunctioning device because they do not have the rights to tinker with the embedded software.[45]

[42] https://press.which.co.uk/whichpressreleases/a-fridge-too-far-the-smart-appliances-that-cost-a-grand-more-but-may-only-last-two-years/

[43] See footnote 19.

[44] Ref.: https://www.bbc.com/news/business-51385344

[45] This issue made the headlines when American farmers found themselves unable to repair their connected John Deere tractors, because any modifications of the tractors would constitute a breach of the copyright license.

https://www.theguardian.com/environment/2017/mar/06/nebraska-farmers-right-to-repair-john-deere-apple

BEUC recommendations:

- The upcoming revision of the EU Ecodesign directive should put a much stronger focus on durability, repairability, reusability and other circularity aspects of IoT products, including but not limited to availability of software updates and spare parts, repair information, requirements on interoperability, modularity and ease to disassemble. At the end of life stage of the product, there need to be proper collection and disposal measures of connected products.
- The European Commission should assess how different IP rights would apply vis-à-vis the right to repair products and, where appropriate, to provide the necessary exceptions and limitations to such rights enabling the reparability of products in a legally compliant way.
- The features of a device that in its core functionality do not require connectivity should continue to work when the product or service is not connected to the internet (e.g. connected water kettle should still heat water if disconnected).
- Measures should be put in place to ensure that connected devices are disposed in an environmentally responsible manner at the end of their life.

7.1. Lifespan label

According to the Commission's behavioural study from 2018[46], consumers lack information on product durability and repairability whilst such information is potentially very influential on their purchasing decisions. The study also showed consumer would be ready to pay more for more durable and repairable products[47].

In order to help consumers make more sustainable choices, but also to create the conditions for companies to compete on better quality and durability criteria, new information requirements covering durability/expected lifespan of products, repairability, availability of spare parts and (security) updates should be added into EU law.

To make this information more accessible and easily understandable for consumers, BEUC recommends the EU to develop a *mandatory 'guaranteed lifespan label'* which would be displayed on products themselves and available to consumers at the point of sale[48] before they make their purchase. Such label shall indicate the period for which a product is covered by a legal guarantee[49].

Finally, BEUC recommends the EU also considers developing an EU repair index[50] to better inform consumers about how repairable products are. This index should complement the guaranteed lifespan label and could eventually become a broader sustainability/durability index.

Clear, reliable and readily accessible information about connected devices and their characteristics is a core safeguard of consumer rights and interests. Labels, pictograms and use instructions are for example essential to ensure the safe, secure and correct use of connected devices, such as smart hubs, smart meters or smart.

---

[46] https://ec.europa.eu/info/sites/info/files/ec_circular_economy_final_report_0.pdf

[47] See for more information page 12 of the above-mentioned study.

[48] Both off-line and online.

[49] For more information on BEUC recommendations in this area, see BEUC position paper "Durable and repairable products: Changes needed for a successful path towards the green transition", BEUC-X-2021-061

[50] A repair index was already introduced in France and will progressively appear in France as of 2021 on five selected product groups (smartphones, computers, TVs, washing machines and lawn mowers). A durability index is scheduled to be introduced as from 2024.

BEUC recommendations:

- BEUC recommends that new information requirements on durability/expected lifespan, repairability, availability of spare parts and updates are introduced.
- A new *mandatory* guaranteed lifespan label should be introduced, which would express the length of the legal guarantee period.
- The EU should consider developing an EU repair index.

8. Liability

The relevant Product Liability Directive ('PLD') was drafted back in 1985, long before one could consider the use of connected devices, let alone foresee the challenges ahead. It is no longer adapted to tackle the challenges by the internet of things and to ensure compensation to consumers when things go wrong. In April 2020, BEUC made several recommendations to ensure that EU product liability rules remain fit for consumers in the digital age and to IoT.[51]

Several key principles should guide EU policymakers when adapting the liability framework to the challenges brought by the internet of things.

- *The scope of the Product Liability Directive is currently too narrow and its key notions should be clarified*. In particular, the notion of 'product' should be revised, to consider its full digitalised dimension in which tangible items, digital services and digital content interact and cannot be differentiated. All of them should be covered under the definition of "product" in the PLD.
- *The liability framework should be clear and consistent*. On top of a possible revision of the PLD, the European Parliament has called on the European Commission to envisage a specific initiative laying down civil liability rules for Artificial Intelligence.[52] The proposal would propose a double-track liability depending on the risk-profile of products. BEUC considers that tailoring liability rules on the risk-profile of products is a bad idea for consumers. Instead, consumers must have access to swift compensation regardless of the risk profile of their products. In any event, there should be a clear interplay and consistency between the different EU initiatives on liability, and the revised PLD should serve as a clear safety net for consumers when things go wrong.
- *The liability framework must be easy to navigate for harmed consumers*. Consumers should easily know where to go to when things go wrong. Therefore, all professionals involved in the supply chain should be jointly and severally liable and consumers should be entitled to address their claim to one of them. It should be up to the professionals to organise their liability as they wish through contractual arrangements. Consumers should not have to play "ping pong" with professionals to identify who the relevant, liable party is.
- *Liability rules must follow the dynamic nature of connected devices*. The liability of professionals should not stop once the product has been put on the market. Today, products stay much longer into the sphere of control of businesses (e.g., in the form of software updates). For the same reason, the risk development defence should no longer be permissible.

[51] BEUC, *Product liability 2.0 - How to make EU rules fit for consumers in the digital age*, April 2020, www.beuc.eu/publications/product-liability-20-how-make-eu-rules-fit-consumers-digital-age/html

[52] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)), www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html

- *The notion of "defect" in the PLD should be broadened and no longer limited to users' safety expectations.* The PLD should build on an extended notion of 'defect' no longer limited to users' safety expectations. A product should be considered 'defective' when it deviates from the reasonable expectations that users may have for their products, which include: the product should be safe, it should be free from cybersecurity failures and other personal security risks and should be GDPR-compliant**.**
- *Rules on the burden of proof must be adapted.* Given the salient asymmetries of information existing between consumers and professionals (the latter being the most likely to have the relevant information about the functioning of their products), the burden should be reversed. This is a matter of fairness.
- *All types of damage should be compensated:* liability rules should not introduce liability thresholds and compensation should be possible for damage to data and other pure economic loss. This is because the range of damage caused by connected products is nowadays much wider than those caused by traditional offline products.

BEUC recommendations:

- The Product Liability Directive (PLD) must be amended and adapted to the multiple challenges brought by new technologies, which includes the development of connected devices.

9. Interoperability and competition

One of the main selling points of the internet of things is its interconnectivity. Devices that "speak to" each other form the backbone of a seamless connected environment. Technical features such as network standards helps to facilitate these internet of things ecosystems but can also be used to exclude certain services or actors. For example, if your digital assistant only works with other connected devices from the same manufacturer, this pushes consumers toward purchasing more devices from this manufacturer, further entrenching the individual consumer into a closed ecosystem. This creates a lock-in effect and can be bad for competition, consumer choice and innovation.

In its Preliminary Report on the Sector Inquiry into Consumer Internet of Things[53], the Commission shared these concerns.[54]

Interoperability in the energy sector is also crucial to help Europe achieve its climate objectives. For the delivery of smart energy services to consumers, energy suppliers and aggregators need information on real time electricity consumption data from smart

[53] https://ec.europa.eu/competition-policy/system/files/2021-06/internet_of_things_preliminary_report.pdf

[54] *"389. However, (…), the leading consumer IoT technology platforms are generally vertically integrated companies (Google, Amazon, Apple) that also offer first-party smart devices and consumer IoT services in competition with third parties present on their technology platforms. These leading consumer IoT players may have therefore incentives to restrict the operability of third-party products and services by limiting their access to the full functionalities of their technology platforms, thus influencing the functionalities and user experience they are able to provide.*

390. From a technical perspective, respondents [to the public consultation of the sector inquiry] explain that consumer IoT technology platform providers allow fewer capabilities and features to third-party smart devices and consumer IoT services (compared with their first-party products and services) by exposing less functionalities through the APIs available for third parties."

393. Overall, respondents indicate that it is generally not possible to provide richer functionality and user experiences through third-party technology platforms than what is provided by the first-party products offered by technology platform providers themselves. This makes it difficult to compete directly with many of the consumer IoT services and smart devices provided by leading consumer IoT technology platform providers."

appliances or electric vehicles. Currently, there is a variety of energy data formats used by different appliances, electric vehicles, suppliers and aggregators, which limits their ability to communicate data that is key for the delivery of smart energy services. The inability of all appliances/electric vehicles to communicate to all suppliers/aggregators limits consumers' choice and competition among products and energy services. A standardised format for electricity data is hence needed to increase competition among providers of smart energy services.

Standards harmonising the format of electricity data allowing smart products to communicate with a range of electricity suppliers and aggregators should be set to increase competition, which will push companies to make more remunerative offers available to consumers.[55]

It is essential that IoT markets are competitive for consumers and not distorted by data access restrictions, self-preferencing, misuse of standards or other company practices that structurally distort competition. The Commission's Sector Inquiry into the IoT for consumer-related products and services in the EU[56] should identify and follow up on any other barriers to free and fair competition in IoT markets, in addition to interoperability issues, to make sure that consumers benefit from the best and most innovative products at the best prices.

BEUC recommendations:

- Policy makers must prevent lock-in effects and establish open internet of things ecosystems.
- Following-up on the sector inquiry, the European Commission should, where appropriate, open investigations regarding practices undermining competition and consumers' interests in Internet of Things markets.
- The findings of the sector inquiry should be reflected in the proposal for a Digital Markets Act.[57]

10. Connectivity and net neutrality

10.1. Connectivity

In order to work as intended, the internet of things requires an affordable, reliable and adequate internet connection. Many connected devices require constant connectivity to perform their functions. Some connected products, such as connected cars, need to maintain this connectivity while moving around at high speeds, sometimes in low-connectivity areas. Other devices may be permanently situated in low-connectivity places, such as in basements or in the remote countryside. It is important consumers benefit from access to the internet regardless of the terminal equipment used and wherever they go[58].

While an increasing number of connected objects could theoretically lead to increased stress on the existing internet infrastructure, the deployment of 5G network capacity is also expected to increase substantially.

[55] For further information, see BEUC, Do's and don'ts for smart, flexible electricity offers, 2017, ref: BEUC-X-2017-018.

[56] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1326

[57] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

[58] https://www.beuc.eu/publications/beuc-x-2020-084_the_review_and_prolongation_of_the_eu_roaming_regulation_response.pdf

10.2. Net neutrality

Consumers should have a clear expectation that access to Internet services are provided in a neutral, non-discriminatory way. The EU rules[59] and the Guidelines on its implementation[60] by the Body of European Regulators for Electronic Communications (BEREC) ensure that consumers can access and distribute information and content, use the apps, services and terminal equipment of their choice.

Moreover, internet service providers must treat all internet traffic equally without discrimination, restriction or interference. This view has recently been upheld by the Court of Justice of the EU, which ruled in Cases C-854/19, C-5/20 and C-34/20 that offers applying a 'zero-tariff' to specific apps - and therefore limitations that derive from the activation of these options (on bandwidth, tethering or on use when roaming) – are in violation of Article 3(3) of the Open Internet Regulation and, therefore, are illegal under EU law. Service providers should therefore review their commercial practices in line with this interpretation to ensure that they fully respect EU rules on net neutrality.

EU rules opened the door for some very targeted exceptions. For example, optimised services may be provided to meet requirements for a specific level of quality under certain circumstances[61]. Another example: connected medical devices used in tele-surgery could see their traffic optimised. Connected cars will likely be treated similarly, particularly in cases where internet connectivity is vital for main functionalities.

The enforcement of EU rules on net neutrality by telecoms regulators, however, still lacks a truly harmonised approach. Reports on the first two years of enforcement note that national regulatory authorities still have different approaches across the EU, from contradictory rulings to incoherent sums of fines to telecom companies for net neutrality violations.[62] As an increasing number of devices become connected, it is fundamental that net neutrality rules are respected and upheld.

As BEREC has pointed out, with the deployment of 5G network capacity, the "overall quality [of Internet Access Services] will evolve positively over time leading to a situation where a [specialised service] might no longer be necessary"[63], thus leaving no reason to deviate from the principle of net neutrality. It is therefore vital that telecoms regulators monitor the market closely to ensure that net neutrality principles are not eroded in the context of the ecosystem of the Internet of Things.

BEUC recommendations:

- Public authorities should ensure that consumers have access to a stable, adequate broadband internet connections in a non-discriminatory way.

[59] Regulation (EU) 2015/2120 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union.

[60] https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/9277-berec-guidelines-on-the-implementation-of-the-open-internet-regulation

[61] Companies can only justify such optimisation if the network capacity is sufficient to provide them in addition to internet access services provided and such a specialised service could not be used as a replacement for the internet access service or be to the detriment of the availability or general quality of internet access services.

[62] https://epicenter.works/document/1522

[63] https://www.beuc.eu/publications/beuc-x-2019-075_berecs_public_consultation_on_its_draft_updated_net_neutrality_guidelines.pdf

- Consumers should be able to use their connected devices seemingly across the EU/EEA. This includes ensuring that, when roaming, consumers benefit from high data allowances and the same quality of service as they experience at home.
- Authorities should adopt a harmonised approach to net neutrality enforcement across the EU.

11. Enforcement and market surveillance

Besides the need to improve existent laws or adopt new ones, their enforcement and possibility of redress when they are breached are key to ensure that consumers are protected.

Furthermore, national enforcement authorities need adequate powers to investigate the compliance of connected devices with different pieces of legislation and stop infringements.

Depending on the law breached, enforcement of connected devices may fall under the sphere of competence of different public authorities: a data protection authority, a telecommunications authority or a consumer protection authority. It is important that each authority's sphere of competence is clearly identified, and that consumers' complaints are dealt with in a timely manner. In addition, Member States should put in place a platform to foster cooperation and information sharing between cross-sector national public authorities.

BEUC recommendations:

- Consumers should have a right to redress, including collective redress, if connected devices cause them damage. The EU legislator must ensure that any relevant legislation will be included into the material scope of the Representative Action Directive (e.g., the newly proposed AI Act).
- Complaints handling and redress mechanisms should be accessible, affordable, independent, fair, accountable, timely and efficient.
- Where connected devices and their associated services cut across jurisdictions or sectors, regulators should work across jurisdictions and sectoral boundaries to support cross-border and cross-sector enforcement actions.

This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).