Opinion
Consumers and IoT security

ENISA ADVISORY GROUP

Prepared by the ENISA Advisory Group's Working Group on a cybersecurity consumer perspective:
Liam Lynch, Ursula Pachl (rapporteur), Kai Rannenberg, Elena Santiago, Ben Wagner, Kurt Einzinger

Disclaimer: Not every member of the ENISA Advisory Group agrees with every single statement in this opinion. The ENISA Advisory Group however overall supports the opinion and its objectives.

September 2019

Contents

1. Consumers and IoT cybersecurity – why it matters and what consumers need

The Internet of Things[1] and the proliferation of connected devices can bring many benefits to consumers. Connected devices are convenient and simplify numerous aspects of consumers' daily routines. For example, consumers can interact with a virtual assistant, use their energy more efficiently with the help of a smart thermostat or control the doors of their house remotely through a smart lock. According to a recent study, 67% of Europeans believe that digital technologies have a positive impact on their quality of life.[2]

However, from a consumer perspective, the widespread penetration of connected products in consumers' lives is also a cause for concern. As the IoT ecosystem grows, the exposure of connected products to an eventual cybersecurity breach also increases. As pointed out by the European Commission, in 2016 there were already more than 4.000 ransomware[3] attacks per day. This represents an increase of 300% if compared with 2015. In some Member States, half of all the crimes are already cybercrimes.[4]

More connected products translate in a risk of higher number of vulnerabilities for hackers to exploit but also into more risks for peoples' privacy. Not surprisingly, consumers are concerned about the security of their products, their privacy and their safety. According to the latest Eurobarometer from the European Commission, 86% of consumers believe that the risk of becoming a victim of a cybercrime is increasing. Also, 87% of consumers avoid disclosing personal information online because of cybersecurity-related issues.[5]

As consumer organisations have shown[6] and as it is widely recognised by cybersecurity experts[7], connected devices for consumers often do not include the most basic security features, and are therefore vulnerable to the most basic cyberattacks and misuse. For example, in September 2016, the website of cyber security reporter Brian Krebs was targeted by a botnet.[8] This botnet (called 'Mirai') was made up of tens of thousands of compromised consumer connected products such as routers, surveillance cameras and smart home appliances. This botnet was used again in October 2016 to attack the service provider Dyn, which impacted the services of Amazon, Twitter, Netflix and Spotify on East

---

[1] This paper applies to IoT products which are intended to be used by consumers (e.g. connected toys, smart watches, baby monitors, smart home appliances such as smart door locks or smart thermostats) and the associated services for such products.

'Associated services' are considered as the digital services that are necessary for the functioning of the IoT devices, for example, mobile applications, cloud computing/storage and third-party Application Programming Interfaces (APIs);

The scope of the present paper is similar to the scope of the UK's Code of Practice for Consumer IoT Security.

[2] European Commission, Special Eurobarometer 460, Attitudes towards the impact of digitalisation and automation on daily life, May 2017

[3] 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)

[4] European Commission Staff Working Document, Impact Assessment accompanying the proposal for a Regulation on a Cybersecurity Act, Part 1, p. 12

[5] European Commission, Special Eurobarometer 464a, Europeans' attitudes towards cyber security, September 2017

[6] See point 4) to the present opinion;

[7] Ken Munro, *WHY is consumer IoT insecure?*, 7 March 2018, <https://www.pentestpartners.com/security-blog/why-is-consumer-iot-insecure/>

[8] Brian Krebs, *KrebsOnSecurity Hit With Record DDoS*, 21 September 2016, https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

coast of the US.[9] Mirai exploited default passwords and also built a backdoor on some of the devices. Recently media reported that one of the most advanced banking malware, Emotet, is now using poorly secured IoT devices to evade detection, by turning them into proxies for its command and control servers[10].

Despite the clear evidence about the problematic vulnerabilities found in the majority of the tested products[11], there has been barely any intervention from market surveillance authorities and the products are still being circulated within the EU and sold to consumers thus being placed in consumers' homes. Furthermore, upon being notified about their products' vulnerabilities, manufacturers often do not take action (e.g. provide a security update) to fix the security flaw.

For example, in December 2016, Forbrukerrådet (Norwegian Consumer Council) looked at the technical features of popular connected toys sold across the EU. They discovered that with a few simple steps anyone could access the microphone of the connected doll "My Friend Cayla" and speak with the children through it (without the knowledge of their parents) or listen in on the conversations in the kid's room. Almost two and half years after the launch of this campaign about the dangerous features of this toy, to which more than 20 consumer organisations across the EU participated, "My Friend Cayla" is still being sold in most EU countries and has only been withdrawn from shops in Germany.[12]

The French data protection authority CNIL, who investigated the case, closed it in July 2018 on the grounds that the producer had declared to stop using the voice recognition function of the doll. However, because of continued existence of a security flaw through an unprotected Bluetooth connection, CNIL transferred the case to the DGCCRF (French authority for competition and consumer protection) in charge of product safety[13]. To date it seems that no decision has been taken by the authority.

The general lack of security of connected products is due to a great extent to the fact that manufacturers have no legal obligation to respect minimum security, and to the fact that consumer awareness is still low. Since there is no regulatory nor economic incentive, the market fails to provide appropriate measures.

The EU legislative framework is not fit to address the problem of lack of cybersecurity of consumer IoT products. It is unclear whether under the new EU Cybersecurity Act[14] a certification scheme for consumer IoT will be developed. Even if ENISA should develop a certification scheme for consumer IoT such a certification scheme and its components, for example the certificate's end-user information about the lifespan of the security updates, will be first of all of a voluntary nature.

---

[9] Ref.: https://youtu.be/AsEzDXjyhG8

[10] https://blog.trendmicro.com/trendlabs-security-intelligence/emotet-adds-new-evasion-technique-and-uses-connected-devices-as-proxy-cc-servers/

[11] It is important to note that the existing security flaws of connected products are often combined with a lack of policy from the manufacturers regarding new vulnerabilities and how to manage these (vulnerability management). The latter point is also addressed in this opinion in subpoint 2.k)

[12] BBC, *German parents told to destroy Cayla dolls over hacking fears*, 17 February 2017, http://www.bbc.com/news/world-europe-39002142

[13] Décision n°du 17 juillet 2018 Clôture de la décision n°MED-2017-073 du 20 novembre 2017 mettant en demeure la société GENESIS INDUSTRIES LIMITED at https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000037219760

[14] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act);

A general legal obligation for the cybersecurity of IoT products doesn't exist in the EU, which is not compatible with the obligation of the EU to provide for a high level of consumer protection.[15] The concept of 'safety' on which product safety legislation is based, seemingly only covers "physical safety" risks that have a direct impact on the health and safety of their users through the exposure to for example harmful chemicals or mechanical flaws. It remains unclear whether the lack of security of a connected product that could have an impact on its users' health or safety (e.g. hackable smart oven) would fall under the scope of EU product safety legislation.

Contrary to EU product safety rules, which stipulate that all products that are placed on the European market must be safe, consumers cannot trust that the connected products they buy are cybersecure.

Regrettably, instead of resolving this legal vacuum, the recently adopted Cybersecurity Act provides a framework of *voluntary* certification schemes certifying connected products/services associated to different cybersecurity assurance levels. It is key that consumers can rely on rules that can be directly enforced, and voluntary certification schemes are less likely to provide such a level of reliability.

The next European Commission should therefore make it a priority to propose a horizontal mandatory legal "Security by default and by design" rule to ensure the EU's framework is fit to enable trust and appropriate consumer protection for devices in the Internet of Things. A consumer right to the cybersecurity of connected products and its associated services should be established, complementing the consumer right to safety.

While waiting for the EU to take the next step, other measures are necessary to increase the cybersecurity of products for European consumers, and ENISA's mandate and activities are key in achieving this objective. Below we suggest how ENISA should use its role and powers in this endeavour (see chapter 3.)

2. Key elements of cybersecurity for connected consumer products

a) Cybersecurity by design and by default

The principle of cybersecurity by design and by default is stipulated in the new Cybersecurity Act.[16]

Cybersecurity by design means that all connected products and associated services should incorporate cybersecurity functionalities appropriate for consumer IoT products from an early stage of and throughout their design process and before putting the products on the market. The design strategy of a product should bear in mind the known and possible vulnerabilities of the product, and respond with a security strategy accordingly, in particular for the most recurrent, widespread vulnerabilities Such strategy must include policies which handles the product life cycle security, specifically vulnerability management from disclosure through patching, including clear EOL/EOS (end of life / End of support).

Cybersecurity by default means that within the different security options, the settings of a connected product or associated service must apply as a default configuration the most secure option. In addition, the requirements arising from privacy regulation, in particular the GDPR (General Data Protection Regulation[17]), should be taken into consideration.

[15] Article 169 of the Treaty on the functioning of the European Union (TFEU);
[16] The concept of 'Security by design and by default' has been introduced in the Regulation for a Cybersecurity Act but a definition was not provided by the European legislators;
[17] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

As examples:

- if a product has connectivity features, the connectivity should have appropriate confidentiality protection by default;
- IoT devices should not have any hard-coded passwords (i.e. a password that cannot be changed);
- Confidentiality protection of personal data (i.e. data that can be used to identify an individual) in storage and while in transit over the network;
- IoT devices should require the consumer to change any default password, prior to connecting to the internet. Campaigns to raise awareness should encourage consumers to systematically check their passwords against specific password control services so that previously breached passwords are not used;
- Due to its reliability and high-level of security, two-factor authentication systems should be made widely available to consumers (e.g. for any online accounts required by the IoT device or cloud service which is used to monitor or control IoT devices).

To ensure a high-level of security by design and by default, an appropriate set of minimum requirements should be established according to the level of cybersecurity needed for the product and the associated service within its particular environment. Any connected product and associated service placed in the market should be bound by such requirements. Such a horizontal and binding framework could be a complementary element to existing legislation such as the Cybersecurity Act, General Data Protection Regulation and the European Electronic Communication Code.[18]

b) Certification

The 'Cybersecurity Act' will put in place a framework for the creation of EU cybersecurity certification schemes. According to this Regulation, ENISA will be entrusted with the task of preparing, at the request of the European Commission or the Members States, candidate cybersecurity certification schemes.

Whether these schemes will cover consumer products and how remains to be seen. In any case, the introduction of certification schemes for the certification of various types of consumer IoT products and associated services will be a lengthy process and due to its voluntary nature, its uptake by businesses remains unclear.

Despite the voluntary nature of these schemes, it is important to highlight that under the Cybersecurity Act, manufacturers of certified products will have an obligation to provide cybersecurity related information to consumers. For example, consumers who purchase a certified product will have to be informed about the cybersecurity support policy (i.e., how long the end-user can expect to receive security updates or patches) of the manufacturer. Furthermore, consumers will also receive recommendations on how to securely configure their devices.[19]

Certification however also comes with the risk of impeding a rapid pace of innovation in developing new products/services, as new versions might require time and costs for re- or new certification. To avoid such detriment for consumers, consumer IoT certification schemes must address these risks.

Finally, European standards that ensure interoperability and promote well integrated safety and cybersecurity practices should be the baseline for the certification schemes.

[18] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast);
[19] Article 55 of the Cybersecurity Act;

Questions of governance regarding the representation of consumer stakeholders in the development of certification schemes are addressed below in point 3.a).

c) The Lifecycle of cybersecurity, enabling sustainable software ecosystems and the importance of software updates

Apart from the problem that consumer IoT products often lack the most basic security features, they are also not updated or cannot be updated, which exposes consumers to numerous cybersecurity risks without any hope of ever being able to secure their systems.

An important element of the principle of cybersecurity by design and by default is the requirement for products to be continuously updated throughout their expected lifespan and according to the reasonable expectations of the consumer. To achieve that, manufacturers should be required to ensure that the software of their connected product and associated service is updated to respond to emerging vulnerabilities during the expected lifespan of product whenever this is needed to guarantee that a product remains safe and secure.

The effort to maintain connected products continuously secured is important because many cyberattacks are only possible precisely because the security protections of connected products are inadequate, outdated, or the necessary security updates have not been rapidly provided.

To make sure that it is easy for consumers to keep their products up-to-date, it is important to guarantee that cybersecurity updates are not bound to the general updates of the devices' operating systems (OS). Bundling of general software updates together with cybersecurity updates is a widespread practice that can be problematic for consumers. An important reason being, that the urgency of a given cybersecurity update is determined by the risk it places upon society in general. For instance, a cybersecurity update for a critical vulnerability that exposes a widely deployed IoT product to a botnet attack is understood as urgent (particularly in the face of debilitating attacks from IoT botnets in the past). It is also important to ensure that the development and timely release of cybersecurity updates is not restricted from any otherwise established release schedule for software updates. Additionally, consumers can have good reasons not to want to install the latest OS (e.g. it might have a negative impact on the devices' battery, slow down the performance of their product, etc) but they would of course want to install security updates to keep their products secure.

"Self-standing" security updates are also essential to avoid early obsolescence. When devices become unsupported for OS versions, consumers are often confronted with a dilemma: either buy a new device or keep the old one without proper cybersecurity updates. Thus, whilst taking into account the legitimate expectations of consumers as to the lifespan of the product, manufacturer and providers should continue to serve consumers with security updates for products that do not have the latest OS update (as much/long as it is technically possible).

Consumers should be informed at the time of the purchase about the manufacturers' end-of-support policy for that specific product and its associated service. This information should take in consideration the expected lifespan of the product and should include information regarding the date when manufacturers will no longer provide security patches.[20]

At present, it is often not clear 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. Suppliers must explain the reason of the update and its impact on the product, and importantly, must

[20] As mentioned in point 2.b), the Cybersecurity Act obliges manufacturers or providers of certified products and services to provide information about their end-of-support policy to consumers;

never misuse the update for example to unilaterally change the conditions of the service. Consumers should also be informed about the consequences of not accepting a software update.

A new development in consumer sales law shows the way: under the Directives concerning contracts for the supply of digital content[21] and the sales of goods[22], sellers must in the future deliver IoT products that are supplied with updates as stipulated by the contract and according to the consumers' expectations. Hence, the seller must ensure that the consumer is informed of and supplied with updates, *including security updates*, which are necessary to keep the goods in conformity.

At the same time, products must be of the quality and provide features, including a security standard that is normal in goods of the same type and which the consumer can reasonably expect. If this fails, consumers have legal guarantee rights against the seller of that product. Consumers must be informed about the consequences of not accepting a software update, i.e. that the seller will not be liable for a lack of conformity resulting solely from the lack of the relevant update.

d) Right to tinker

It should be considered that in certain situations (e.g. after the end-of-life communication by the manufacturer), consumers should be allowed to repair and modify their own products to ensure their security. Such scenarios must waive the liabilities of the manufacturer for any related defect and establish proper legal safeguards against IPR infringement actions.

e) Connectivity profile should be available

Consumer products that fall in the IoT category are connected products. Their connectivity will typically be to a service accessible over wide-range (e.g. Internet) protocols and – optionally – to a smartphone application accessible over short-range protocols (e.g. Bluetooth, WLAN, etc.). In scenarios where IoT products are compromised and used in a distributed Denial-of-Service (DDoS) attack, it is the former type of connection that is exploited by malicious actors. Being able to discern the normal traffic of an IoT product from malicious traffic is an important enabler of containment policies and part of DDoS mitigation strategies.

To this end, it would be technically beneficial if IoT products came with profile information defining how their normal traffic patterns should look like (e.g. in terms of services they connect to over the Internet, etc.). Having this information would enable security monitoring to detect abnormal traffic emanating from IoT products. In the face of a DDoS attack, security response would then be able to take effective defensive action by containing malicious traffic as close to the source as possible.

f) Connectivity should have an on/off switch

Numerous products will soon show connectivity features, but not all these products need to be connected to perform their basic functions (e.g. a kettle, a fridge, etc.). It is therefore important to make sure that the connectivity of products, where the connectivity is not part of the main function/objective of the product, can be turned off easily, ideally by a dedicated hardware switch. Being able to disconnect connected products should be regarded as an essential cybersecurity feature

[21] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services;
[22] Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC;

because it eliminates the vulnerabilities that stem from the products' connectivity and reduces the complexity for the user.

The ability to disable connectivity at the hardware level may be accessible through a physical interface of the product, or, alternatively, through a dedicated remote control application (e.g. for products whose use involves embedding into other physical objects). The latter case may be also involve functional support of a communication gateway that is topologically proximal to the product and supports its connectivity to other products and services.

g) Interoperability of connected devices

There is a myriad of manufacturers of smart products. Consumers increasingly use connected devices and its associated services that are made or provided by different producers and service providers. Like with other technologies in the past, as the markets evolve, there is a risk that these products will be put into limited ecosystems.

Tight ecosystems can be problematic for consumers because they can reduce their choice in practice. For example, a consumer could have a smart fridge, a smart hub, a digital assistant, and smart locks that work all together within a common ecosystem. If the consumer then has to buy a digital assistant or a new connected device that is incompatible with the ecosystem, he will face a difficult dilemma. It is important that a good security standard is guaranteed for all products and at the same time that the ecosystems are interoperable also from a security standpoint. Fair information sharing, alerting and management of the respective stakeholders is essential.

Ensuring interoperability, primarily through appropriate standards, and reducing the problematic aspects of such ecosystems is therefore essential, also from a cybersecurity perspective. Consumers might want to substitute connected products in their homes with competing products that are more cybersecure, but to do that they must be sure that the products will work in no matter what ecosystem.

Consumers should therefore always be free to choose products without any fear of being locked-in to a software or hardware belonging to a specific manufacturer or service provider.

h) Liability

A key question for consumers with regard to IoT and cybersecurity is the issue of liability: "What happens if something goes wrong? Who can I turn to get redress?" (for example, if a door lock was hacked by burglars and the insurance doesn't pay for the damage, if an automated car crashed due to a cybersecurity attack, etc.).

The legal uncertainty for consumers as regards who is liable for any harm caused by connected products is high. This generates a lack of trust in IoT consumer products.

The EU legal framework for liability in this respect is the 1985 EU Product Liability Directive which covers IoT products. The directive is outdated and shows many shortcomings:

The directive is relevant if a *defective* product causes a damage. It stipulates that a product is 'defective' when it does not provide the 'safety which a person is entitled to expect' (Article 6). Thus, the Directive does not cover defects other than safety defects. Consequently, its scope would not cover cybersecurity flaws that do not pose a direct safety risk.

Another shortcoming is the fact that the Product Liability Directive follows a concept of 'damage', which relates to the consumer health and the destruction of items of property, rather than damage to the digital environment or disturbance of IT-systems or loss of data, time, or reputation.

In addition, the definition of liable persons under the Directive seems to be inappropriate. The directive focuses on manufacturers rather than on other professionals who can contribute to a lack of safety in case of IoT products, such as creators of digital content, operators of digital services, or programmers of software. Then, there is a problem about how to identify the liable person when the same product is made by several manufacturers and contributors.

Finally, a big problem for consumers is the need to prove the causation: under the Product Liability Directive, the injured person has to prove the damage, the defect and the causal relationship between the defect and the damage. This can be problematic in relation to systems that compromise multi-layered structures and use sophisticated communication means, such as consumer IoT products. More so when the stakeholders involved in the realization of that system differ significantly in terms of the complexity of involved products, market standing and access to resources.

Consequently, today, consumers that buy connected products have no legal certainty in case such a product would cause harm due to a cybersecurity flaw. The legal situation is unclear. Unclear rights for consumers often mean no rights, as the obstacles such as technical expert costs and length of a judicial procedure implying technology questions would be insurmountable in case of a presumed security failure.

A European cybersecurity policy should take the important role of a modern and fair liability regime into account which is essential for stimulating market development and for enhancing consumers' trust in connected products.

i) Raising awareness

Any mandatory regulatory measures should be complemented with raising awareness campaigns aimed at increasing consumers' "cybersecurity hygiene" as the overall level of cybersecurity of consumer IoT products will also depend on their users' sensibility to cybersecurity.

Consumer organisations are in regular contact with consumers and are generally perceived by consumers as being a trustworthy source of information. They are therefore well placed to inform consumers and to raise their awareness regarding the cybersecurity of their IoT products. Collaboration of consumer organisations with other stakeholders from industry or from authorities should be promoted.

In recent years, European consumer organisations have been actively raising consumers' awareness towards the security vulnerabilities of the products and services they use. Some examples of these campaigns can be found in point 4) of this opinion.

ENISA has a crucial role to play in advancing awareness building through its outreach activities.

j) Label

The Regulation for a Cybersecurity Act enables the creation of cybersecurity certification schemes to provide for labels or trust marks.[23] Labels are however not mandatory: it will be under the responsibility of ENISA, in cooperation with stakeholders and Member States' representatives, to decide whether to introduce a trust mark or label in a particular candidate certification scheme.

In addition to the possibility to introduce labels, as explained above[24], manufacturers or providers of *certified* products or services will have to provide information to the users on their support policy (e.g. how long they will provide for security updates).

The value of a label depends on the quality of its content and on the governance of the label scheme. Unfortunately, both these elements are unknown at this stage in what regards the cybersecurity of consumer IoT. One of the main reasons is that European standards related to cybersecurity for IoT products are still lacking and their development is at an initial stage.

In addition, it is important to underline that the meaning of certain labels, certifications or a trust mark is often unclear and confusing for consumers. CE marking is a good example: many consumers believe that CE marking means that a specific product has been tested to be safe. In reality, for many products, a CE marking is a declaration from the manufacturer, without third party assessment, that the product complies with EU legislation.

From the viewpoint of cybersecurity, an important aspect of any labelling scheme would be the accommodation of time. Cybersecurity is a dynamic property which, for any ICT product, depreciates with the passage of time. Occasionally bugs which could not be identified before the release of the product get discovered as times passes, some of which lead to a security vulnerability, thus decreasing the original level of cybersecurity assurances offered by the ICT product. Security patches released to mitigate disclosed vulnerabilities of the ICT product contribute to the maintenance of the original level of cybersecurity assurances. An efficient labelling scheme should account of these aspects and the effect they have on cybersecurity assurances.

k) Vulnerability disclosure

Manufacturers of consumer IoT products and associated services should put in place vulnerability management policies aimed at reducing the risks of security flaws for consumers.

These policies should include a mandatory notification to the users whenever the vulnerability represents a critical risk to their security and/or safety. Any notification should include a set of simple recommendations to minimise the risk of the vulnerability.

In this regard, the Cybersecurity Act obliges manufacturers of certified products to provide their contact information and accepted methods for receiving vulnerability information from end users or security researchers.[25]

[23] Article 54 (1) i) of the Cybersecurity Act;
[24] See Point 2.b;
[25] Article 55 (1) c) of the Cybersecurity Act;

3. What can ENISA do?

The aim of this part is to suggest measures ENISA can take to address the consumer concerns and needs as described above and advise other institutions and stakeholders in this respect.

As said above, devices and products in need of cybersecurity have made their way into everybody's home and life. Connected devices are part of our daily routine via smart homes, smart toys, smart cars etc. Cybersecurity is not only an issue for preventing economic harm and protecting us from health or safety risk but has also become an essential element of people's privacy.

This relatively new scenario needs to be better reflected in the way European (and national) institutions and bodies shape their policies and decision-making structures.

In particular, the importance of cybersecurity of consumer products for societal wellbeing should be acknowledged strongly. As the products that European consumers use become ever more reliant upon properly functioning services, so does the level of cybersecurity that these offer play a stronger role in installing trust in the Single Digital Market. We should work towards integrating consumers' interest (needs and expectations) systematically in policy making and in the corresponding institutional structures that aim at reaching out to stakeholders.

ENISA is mandated to develop and promote a culture of network and information security to the benefit of citizens and consumers.

a) The need to represent consumer interests adequately in ENISA and beyond:

ENISA Advisory Group (former ENISA Permanent Stakeholder group):

The current ENISA Advisory Group (AG)[26] is an example of a body that does not respond yet to the new challenges: currently only 1 out of 33 members (mandate November 2017 – November 2019) of the group comes from an organisation with the main mandate to represent consumer interests.

In accordance with the new rules of the Cybersecurity Act, the ENISA Advisory Group shall now ensure a balance composition between the different stakeholder groups.

In order to start the process of better integrating the consumer dimension into ENISA's work, the ENISA Advisory Group decided to establish a consumer issues working group which aims at providing information and expertise on consumers' needs and expectations to ENISA and the European Commission which can then be better reflected in ENISA's workstreams, and which should also inform the European Commission and other institutions and stakeholders.

Stakeholder Cybersecurity Certification Group:

The Cybersecurity Act creates a new Stakeholder Group whose main purpose is to advise ENISA on strategic issues related to the Cybersecurity Certification schemes.

It is important that consumer experts are accepted as a member of this new stakeholder group and are systematically and regularly consulted by ENISA during the preparation of a certification scheme. European standards used as the basis for those schemes should also be developed with the participation and contribution of European consumers' representatives.

[26] Following the entry into force of the Cybersecurity Act, the Permanent Stakeholder Group was renamed ENISA Advisory group;

In order to be able to provide valuable input, the provision of consumers' expertise should be financially supported by the EU institutions, similar to the functioning of the EU's eco-design policy implementation.

Takeaways from point a) to be included into ENISA's workstream:

- ENISA should formally recognise the establishment of the AG working group and set aside funding for research and events on consumer relevant topics organised by members of that group for or in co-operation with ENISA. Target groups for the events should include both ENISA staff and relevant stakeholders.

- The Management Board (MB) of ENISA should regularly invite members of the Advisory Group and should ask systematically to include consumer representatives in such a delegation. We also suggest that once a year MB representative and the ENISA Advisory group representatives meet to specifically discuss consumer concerns.

- In any consumer relevant event that ENISA organises or co-organises, consumer representatives should be included as speakers by default.

- The reform of ENISA under the proposed Cybersecurity Act improves the balance of the composition of the ENISA Advisory Group. ENISA and its management should push to improve the situation by ensuring that sufficient nominations will be presented. A stakeholder mapping should be undertaken by ENISA to understand better, which representatives should be on the ENISA Advisory Group and to pro-actively invite them to become a candidate for membership of the ENISA Advisory Group.

- ENISA should ensure that under the new certification structure, consumer representatives will be sufficiently involved right from the start and throughout.

b) The need to address the lack of consumer security in the Internet of Things

As stated above, the EU legal framework does not provide a basis to address the widespread lack of security measures, particularly in the Internet of Things and connected products. The Cybersecurity Act does not address this problem either.

Therefore, it is imperative that other measures are undertaken as a matter of priority at a European level to respond to the lack of sufficient cybersecurity in the market.

While we recognise the role of consumer awareness (developed in points 2.i) and 3.c)), the manufacturers, vendors and service providers should take their responsibility to enhance cybersecurity of products, sharing their findings and innovation with an active contribution in the development of European standards to guarantee that citizens and consumers have equal levels of security and safety for IoT products and services placed on the Market.

Guidelines and codes of conduct should be explored more deeply. For example, in October 2018, the United Kingdom's Government, with the support of consumer organisation Which? published a Code of Practice for Consumer IoT Security addressed at manufacturers and service providers to improve the security of their devices during the product development. While the Code is voluntary at this stage, the UK Government recently announced its plan to regulate the security of consumer IoT products and

opened a consultation process.[27] The Code served as the basis for the creation of ETSI TS 103 645, the first technical standard for cybersecurity in the consumer Internet of Things.[28]

Existing regulatory solutions should also serve as an example. In September 2018, California became the first state to adopt a law aimed at improving the cybersecurity of IoT products. It requires manufacturers to adopt a set of baseline security requirements (e.g. a unique password per device manufactured).[29]

Takeaways for point b) to be included in the ENISA's workstream:

- The consumer working group in ENISA should put together criteria for an EU Code of Conduct to ensure the security in consumer IoT products.

- The AG consumer working group should have the means to invite interested parties as external experts to establish such criteria and the governance of the code.

c) The need to address the lack of consumer (and business) awareness

Consumer awareness and knowledge of the need to look for cybersecure technology and respective products is only slowly increasing. Likewise, many "traditional" companies are not used to connected products which they start to produce and /or to sell, for example the toy industry.

Takeaways from point c) to be included into ENISA's workstream:

- ENISA should increase its spending for consumer awareness and co-operate with consumer organisations and national authorities to implement education and awareness raising programmes.

- Similarly, SMEs should be trained on cybersecurity. ENISA should co-operate with DG Growth on potential projects.

- In light of the requirement for manufacturers and service providers of certified products/services to provide cybersecurity information for end-users established in Article 55 of the Cybersecurity Act[30], ENISA should carry out research to identify a comprehensive design of consumer information and recommendations for best practices for providing it to end-users;

- For individual certification schemes for consumers products/services, where a "**label or mark**" is used and the conditions are established in the certification scheme (according to Article 54 Cybersecurity Act), ENISA should provide for preliminary qualitative testing of such labels to ensure they are well designed and tested for effectiveness, so that end-users correctly understand the meaning of the label or mark. This action should be linked to the aforementioned consumer awareness measures.

[27] Ref.: https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security
[28] Ref.: https://www.etsi.org/committee?id=1549
[29] Ref.: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
[30] For more information, see Point 2.b).

4. Selection of cybersecurity campaigns and articles from European Consumer Organisations

FORBRUKERRÅDET (Norway)
Smartwatches present serious security and privacy flaws
Connected health devices do not meet security and data protection standards
Internet-connected toys fail to safeguard basic consumer rights, security and privacy
Opaque and abusive data usage policy for wristbands

STIFTUNG WARENTEST (Germany)
Connected Cars: Die Apps der Auto-hersteller sind Daten-schnüffler
Tracking: Wie unser Surf-verhalten über-wacht wird – und was dagegen hilft
Smart Toys: Wie vernetzte Spielkameraden Kinder aushorchen
Smart Home: Acht Einsteiger-Systeme im Vergleich
Babycams: Wie sicher ist die Über-tragung?
Smart TV und Daten-schutz: Spion im Wohn-zimmer – wenn der Fernseher zurück-schaut
Smartphones: Data protection tested

TEST-ACHATS (Belgium)
Les caméras de surveillance ne sont pas toujours sûres
Maison connectée, maison en danger !
Cher Saint-Nicolas, je ne veux pas de robots dans mes souliers
Jouets connectés : mieux vaut éviter !
Cybercriminalité et arnaques sur internet
50% des magasins en ligne peuvent être hackés

UFC – QUE CHOISIR (France)
Même une fois le Wi-Fi désactivé, vous êtes pisté
Vigilance sur les objets connectés
Des outils avides de données personnelles

WHICH? (United Kingdom)
24% of Brits plan on buying a smart home device
Hyper optic router 'at risk of being hacked'
Less than half of ransomware victims get their files back
Easy-to-hack smart devices targeted by government
Government and NHS websites fall victim to cryptojacking hack
700,000 malicious Android apps found in Google Play store last year
Cryptojacking: how your PC can be hacked to mine Bitcoin for others
Security report finds ransomware rise of 93%
iOS 11.3 stops iPhone slowdown, but should you upgrade?
Which? criticises Apple's lack of transparency over slowing down iPhones
Spectre and Meltdown threats – one week on, what's been fixed?
Apple facing lawsuits for slowing down older iPhones
Intel Meltdown processor security flaw – what you need to know
Apple security flaw: what to do if you're affected
A quarter of UK households now contain a smart home device
Which? issues child safety warning on connected toys
Half of camera apps tested reveal personal data unnecessarily
Which? calls for collective redress following data breaches

WPA2 hack: what you need to know, and what you need to do
Yahoo hack: three billion accounts affected
Could my baby monitor get hacked?
Samsung smart TVs software update renders some unusable
76% of Brits are scared of the smart home
CCleaner malware hack: what it is and what you need to do
Virgin urges Super Hub 2 password change
Could your smart home be hacked?
Why I'm sick of software updates