WHICH? SUBMISSION TO THE CALL FOR VIEWS ON PROPOSALS FOR REGULATING CONSUMER SMART PRODUCT CYBER SECURITY

Introduction

Which? welcomes the opportunity to share its views on the proposals for regulating consumer smart product cyber security[1]. These proposals would see the introduction of legislation which mandates that consumer smart products must meet three requirements in order to be sold in the UK. The Call for Views additionally outlines the obligations that will be placed on industry in order to comply with the law, as well as the potential role of the enforcement body.

Which?'s testing has repeatedly exposed popular connected devices with serious security flaws and therefore we are supportive of the government's commitment to introduce mandatory standards. In this submission we have outlined our thoughts on the detail of how those requirements will be implemented in practice and would encourage the government to ensure it maintains momentum on bringing this regulation into effect.

Summary

- We welcome the government's commitment to regulate security provisions for connected devices in order to better protect consumers. We believe the introduction of these three requirements must be only the start of the government's ambition and we welcome the intention to use secondary legislation to allow for additional provisions to be included going forward. There would be value in government more proactively signalling their intent to expand the mandated requirements and should set out a pathway for doing so.

- The proposal to include the broad range of consumer products in scope is important and we support the approach outlined to ensure the scope remains up to date and new consumer products are captured as they come to market.

- We broadly support the proposed requirements but would emphasise the need to ensure they are implemented in a way that delivers the intended outcome of better protecting consumers. For requirement 2, this must provide a viable route through which manufacturers or other relevant entities can be notified of and, *essentially,* take action on security vulnerabilities identified; simply providing a vulnerability disclosure policy in itself is not a successful outcome.

- For requirement 3, success will be dependent on consumers being able to clearly understand the information that is being provided to them. As such we believe it is necessary that detailed guidance, which must be informed by consumer testing, is

[1] https://www.gov.uk/government/publications/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views

produced outlining what good practice looks like and consideration of this should be taken into account when enforcing this requirement.

- We very strongly support the inclusion of online actors in the obligations and consider this essential to the success of the regulation. Online marketplaces must play a proactive role in helping ensure consumers are protected from non-compliant products.

- It will be important to ensure the legislation appropriately captures the complexity of cross-border supply chains where platforms and sellers may be based in different countries and the different models for how online actors operate. We would welcome the opportunity for scrutiny of the legislation once drafted.

- Strong and effective enforcement will be essential. We support the enforcement body having a broad suite of enforcement powers so that it is able to take proportionate action against non-compliance and critically this must include the power to suspend or ban the sale of non-compliant products and to recall products where appropriate. This will be essential where other enforcement measures are not sufficiently correcting issues of non-compliance in a suitable timescale to prevent the continued purchasing of unsecure products by consumers.

- In appointing an enforcement body we would like to see a firm commitment from the government that they will provide the required resources, skills and expertise necessary to undertake this role effectively. Crucially the chosen body will need to be able to cooperate effectively with regulators in other jurisdictions and should be empowered to do so from the outset.

2. Scope of the regulation

In the main, we are supportive of the approach to the scope of the regulation as set out in the Call for Views. We believe it is important that the regulation covers the broad range of consumer smart products and that there is an essential need to ensure the scope remains up to date and new consumer products are captured as they come to market. If there is a requirement to re-open legislation in order to add new products then there is a risk that the regulation will fall behind market developments, leaving consumers at risk.

However, the government must be mindful that their proposed approach could lead to a lack of clarity in relation to some product areas. For example, automotive products (including electric vehicles) are specified as being out of scope, however would this additionally include aftermarket kit such as wifi hotspots or connected alarm upgrades? Similarly it would need to be clear what devices may be considered as exempt medical devices and what would need to be compliant with the requirements of the regulation. Connected hearing aids are one example which may fall into such a grey area. A possible solution could be for government to

use the proposed guidance, which can be quickly updated, to provide more clarity on what falls in and out of scope.

We note the Call for Views highlights that DCMS is compiling evidence to understand how security of other areas of technology could be improved, including routers. In our view router security is vital given it can act as a 'gateway' to the consumer's home. We therefore welcome this work and look forward to further details being published. It is not clear however where other networking devices that might commonly be purchased by consumers, such as mesh systems and extenders, as well as routers purchased 'off the shelf' from third parties will fall and again clarification is required to prevent products such as these falling through gaps.

We are supportive of the proposals to include conventional IT products (laptops, PCs and smartphones) within the scope of the regulation. In particular such products will benefit from the requirement to provide clear transparency about how long security update support will be provided for, through provision of a transparent 'end date' (see Requirement 3 below). An investigation[2] we undertook earlier this year found examples of Android devices being sold which were no longer being supported by updates or which were close to the end of their support period. Given the risks that may occur with consumers using unsupported devices, we believe transparency across the broad range of products used by consumers is essential.

3. Security Requirements

The introduction of regulation to mandate three requirements of the Code of Practice is an important first step in protecting consumers from the risks of unsecure connected devices. However we would strongly caution against these requirements being the limit of the government's ambition and believe it is therefore necessary that there is flexibility to introduce further requirements in due course. The proposal to use secondary legislation seems an effective way to do this. However we would welcome the opportunity to scrutinise the specifics of the legislation to ensure there is the appropriate balance between providing flexibility and being adequately robust. We believe there would be value in government more proactively signalling their intent to expand the number requirements that are mandated in the future and set out a pathway for doing so. This may encourage manufacturers to be more proactive now in aligning with the requirements of ETSI European Standard (EN) 303 645 v2.1.1 and thereby further ensuring protection for consumers.

The Call for Views is clear in emphasising that the precise wording and approach of each requirement is still to be finalised. Many of our comments on the requirements below therefore relate to practical consideration of how the requirements will be implemented with a focus on how they contribute to the overall intention of better protecting consumers from buying products with significant security vulnerabilities.

[2] https://press.which.co.uk/whichpressreleases/void-android-more-than-one-billion-android-devices-at-risk-of-hacking-attacks/

3.3 Proposed security requirements

Requirement 1 - Ban universal default passwords in consumer smart products

We are supportive of this requirement and broadly in agreement with the proposal set out. In particular we agree with the intention to ban passwords which although unique per device may still be easily guessable and believe this is an important element of the requirement. We would emphasise that there should be a programme of work to ensure the ongoing strengthening of provisions as necessary. In relation to this requirement that may consider requiring a more consistent approach to passwords being used.

Requirement 2 - Implement a means to manage reports of vulnerabilities

We are supportive of the inclusion of this requirement. However, it is essential that its implementation drives meaningful change in providing a viable route through which manufacturers or other relevant entities can be notified of (and where necessary take action on) security vulnerabilities. We do not see the provision of a vulnerability disclosure policy and relevant contact information in and of itself a successful outcome but rather it will be the action taken as a result of disclosures that will better protect consumers. In enforcing this requirement it will therefore be necessary for consideration to be made not only of whether the required information is provided but also that stated policies are being adhered to and there is proactive engagement (where required) to fix issues raised through the process.

In our own experience of investigating and disclosing security vulnerabilities we have at times encountered significant obstacles when trying to make relevant companies aware of our findings. In one case, the security report was translated into the manufacturers local language and we recruited an industry expert who was local to the region to raise the issues found with the relevant companies. Even in these circumstances we were unable to get a response from the companies involved. If the purpose of this requirement is to ultimately get vulnerabilities resolved the government must keep careful watch on how it is working in practice and ensure that it is delivering the outcomes intended. In addition it must ensure that responsibilities are implemented across the broad range of industry actors as we discuss in more detail below.

We are also aware that it can be consumers themselves who uncover vulnerabilities with devices they have bought and have seen evidence of issues being highlighted in customer reviews. Given consumers can be an important source of intelligence it should be considered how consumer findings can be incorporated into the requirement to manage reports of vulnerabilities. It is unlikely that consumers would be aware of the vulnerability disclosure process, which is mainly a technical approach to reporting, and therefore additional approaches may also need to be considered as part of an organisation's overall approach to vulnerability reporting.

Requirement 3 - Provide transparency on for how long, at a minimum, the product will receive security updates

The provision of security updates is a critically important component of protecting consumers from the risks of unsecure devices. However, the current lack of transparency about how long updates are provided means consumers are not able to make informed decisions at the point of purchase. We therefore strongly support the inclusion of this requirement in the regulations and highlight a number of important considerations for how this might be implemented.

The Call for Views proposes in the definition of 'defined support period' that this can be "expressed as a period or by an end date". We agree that the requirement must be for a specific amount of time. In a recent investigation[3] Which? undertook in relation to the support periods provided to a range of smart appliances, a number of manufacturers stated to us that updates would be offered for 'the life of the product' but would not say how long they would expect that to be. We would be severely concerned if similarly vague and unclear commitments were allowed under the regulation. Additionally, we have concerns that the proposals allow the support period to be expressed as a singular period of time. In order to be useful for consumers this would also need to specify when that period was applicable from given it won't relate to the day from which the device was purchased. There is a risk of confusing consumers if they believe they are going to receive updates for the full amount of time specified when in reality it will be dependent on how long after product launch they are buying the device. Consumers may have a false sense that their device is secure for longer than in practice and risk ongoing use of the product even once security updates have ended. A specified end date would provide much clearer information to the consumer and better allow them to make an informed decision at the point of purchase.

Ensuring update information is provided in a 'clear and transparent' form and in an 'accessible way' can be open to very broad interpretation. As for the other requirements we believe it is necessary to keep in mind the intended outcome which is to allow for more informed purchasing decisions to be made. The success of this requirement will therefore be dependent on consumers being able to clearly understand the information that is being provided to them. As such we believe it is necessary that guidance, which is informed by consumer testing, is produced on what good practice looks like and consideration of this is taken into account when enforcing this requirement. Which? would be happy to discuss with DCMS how it might be able to input to the development of good practice requirements.

In parallel to the regulatory requirements it will also be necessary for consumers to be much better educated about the importance of security updates and better informed about what action they can take when the support period ends. In a survey of consumers Which? conducted in January 2020, we asked whether it was true or false that manufacturers of

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

smart devices are required to provide security updates for the lifetime of a product (i.e. until it physically breaks). 49% of responders said that they didn't know with 27% stating that they believed this to be true. This highlights a general lack of awareness about the provision of updates and we are concerned that even once the requirement is implemented it may be limited in its success if consumers are unaware of this information (and therefore don't know to look for it), aren't clear on why the information is being provided, and don't know what it means for their product when the support period ends. We would therefore like to see a plan from the government as to how they will help educate consumers in order to maximise the benefits of this requirement.

Finally, the Call for Views is not clear on how this requirement will apply to second-hand sales of connected devices. At present this is a particularly relevant issue for smartphones with a recent investigation we undertook finding that significant numbers of smartphones being resold were no longer supported with security updates from manufacturers[4]. Without transparency at the point of sale consumers are at risk of buying unsupported phones without being aware. As secondary and refurbished markets may continue to grow for connected products it is important to ensure consumers can make clear decisions about the security update provisions of such devices.

4. Obligations

The nature and complexity of the global supply chain for connected products mean we consider it essential that obligations and responsibilities are appropriately shared across the different actors involved. We therefore broadly welcome the approach as set out in the Call for Views to implement obligations across a range of sector actors. However, ensuring the policy intentions are adequately captured in legislation will be crucial and we would therefore welcome further opportunity to scrutinise the definitions and obligated measures as they are refined and finalised.

We strongly support the inclusion of online actors, including online marketplaces, in the obligations and consider this essential to the success of the regulation. The Call for Views highlights that by far the majority of purchases for consumer smart products are made online and in addition Which? has found significant issues with unsecure products being made available through online marketplaces. It is therefore vital that these organisations play an active role in protecting their customers from non-compliant devices. Which? has previously highlighted issues with the lack of responsibility for online marketplaces in the context of product safety[5] and it is essential that similar issues are not replicated in regulation related to security of products.

4.2 Obligations on the 'Producer'

In the main we are happy with the obligations set out for producers and proposals to align the definition with that used in the General Product Safety Regulations 2005. However, the

[4] https://www.which.co.uk/news/2020/07/mobile-phones-recycling-and-security/
[5] https://www.which.co.uk/policy/consumers/5234/onlinemarketplaces

possible measures do not make clear the action that a producer would be required to take if they have made non-compliant products available and we believe clarity should be given on this so that manufacturers have an obligation to take proactive action when they have not met the required obligations.

More broadly, we think it is important not to lose sight of the fact that the mandated requirements will represent only a first step in protecting consumers from unsecure devices. We would welcome an update from the government about efforts to encourage uptake of security measures beyond the three discussed here. In the government's response to consultation[6] published in January 2020 it set out an intention to examine if it might be feasible for manufacturers to provide information on whether their products adhere to the additional ten guidelines of the Code of Practice/ETSI EN. Whilst that may be outside the scope of this Call for Views, it would be helpful if in their response government could set out their further thinking on this.

4.3 Obligations on the 'Distributor'

We welcome the proposal to place obligations on distributors of connected products along with the clearly stated intent to include within this those who act as a marketplace or a platform for consumer sales online.

To deliver on this aim, it is essential that the government make certain that the definition of distributor is explicit in capturing such entities and cannot be left open to interpretation. We are concerned that the proposals set out in the Call for Views do not do so sufficiently and believe there would be value in making specific reference in the definition to these, such as to entities that provide technology to allow for a product to be available on the market. Crucially, it must not be left to official guidance to clarify which entities are captured but must be explicitly clear in the text of the legislation itself. In determining the definition of 'distributor' it is essential that this adequately reflects the complexity of cross-border supply chains where platforms and sellers may be based in different countries - not necessarily in the UK/EU - and suitably captures the different models for how online actors operate, this includes online marketplaces, fulfilment houses and social media platforms amongst others. In addition to consideration of new regulation, the government must also reassure itself that existing regulation will not act to limit the responsibility of online actors in a way that would conflict with the policy intent of the Secure by Design proposals. Specifically, we would suggest that detailed consideration should be given to the provisions and exemptions set out in the Electronic Communications (EC Directive) Regulations 2002 to ensure that these would not act to prevent or limit the intended responsibilities outlined in the Secure by Design proposals.

[6] https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation

In regards to the obligations for distributors, as for producers, the proposals do not appear to provide clarity on the actions that would be required if a product for sale is identified as being non-compliant. We believe this is necessary in order to ensure that responsibilities are clear and the regulation should require a proactive approach from distributors to remove unsecure products from sale. Additionally we are concerned that the obligations relating to requirement 3 (provide transparency on for how long, at a minimum, the product will receive security updates) and the corresponding guidance to support this as set out in Box 8 is extremely limited in detail. This is not likely to be sufficient to ensure that this requirement is met in a way that is effective in informing and ultimately protecting consumers. As we have outlined above, the provision of this information needs to be clear and meaningful to consumers. We are concerned that if this requirement is left for each distributor to interpret it will result in information being provided in a way that is inconsistent, patchy and not necessarily effective at making consumers aware of the information they need and its implications. We would like to see more detailed requirements, which have been informed by consumer testing, in order to ensure this delivers the intended benefit.

4.4 Obligations for online actors

We consider it essential that the approach to regulation includes entities who supply or make products available online, such as those who act as a marketplace, a platform for consumer sales online or provide either first or third party sales. Which? has been actively testing the security of connected consumer products for a number of years. During this time, our investigations have repeatedly highlighted the prominence of products with security flaws being sold on online marketplaces.

We outlined in an investigation into wireless camera security in October 2019 (which was shared with DCMS at the time) the particular complexities that can exist within the supply chain of the connected product online market. This includes significant difficulties with identifying and contacting those involved with making devices in order to get issues fixed, problems identifying who has brought the products to market and the presence of counterfeit goods. As detailed in the report, the nature of the 'open-source' culture that operates in Shenzhen, where many of the connected products we have found on online marketplaces are made, means that there can be little connection between hardware and software developers and the sellers who bring them onto the market. Sellers may often have no knowledge of who developed the product. Whilst this means products can be brought to market very quickly, it also means there can be very little accountability for the security of the device from the supply chain. Where this is the case, it is essential that online marketplaces themselves play a proactive role in helping ensure consumers are protected from non-compliant products.

5. Proposed enforcement approach

Strong and effective enforcement will be essential to the success of this regulation in protecting consumers from unsecure, non-compliant connected products. The growing scale of the connected product sector and the complexity of the supply chain as highlighted above means it is necessary for the enforcement regime to have adequate resources, technical expertise and powers to appropriately investigate and take action against instances of non-compliance.

As we have highlighted throughout this response there are particular issues that are created by the complex and international nature of connected products being sold through online marketplaces. The development of a robust enforcement approach must therefore sufficiently take account of the challenges that will be faced in policing such a disparate system, particularly where entities are based outside of national jurisdictions. A key part of this will be to ensure that there is effective cooperation with regulators in other jurisdictions. Which? has previously considered such complexities in its work on product safety and we would strongly suggest that in developing an enforcement approach for IOT security, the government ensures that lessons are learnt from difficulties faced in the context of product safety. Our report 'Online Marketplaces and product safety[7]' sets out the issues in detail and we would be happy to discuss this further with the team at DCMS.

5.2 Enforcement timescales

We recognise the necessity of providing organisations with time to make required adjustments to their processes in order to become compliant. Whilst the proposals therefore seem reasonable we would highlight that for some product sectors in particular these devices sell in high volumes so any delays could result in a significant number of non-compliant products being sold and used by consumers. We would encourage the government to consider what steps can be taken in the interim to help protect consumers from at-risk products. This might include ways to encourage and highlight early adoption by producers and distributors, and ways to raise awareness amongst consumers about steps they can take to better protect themselves from the risks of unsecure products.

5.3 Enforcement roles and responsibilities

The Call for Views states that the enforcement body would intervene when a report of non-compliance is received, but that this could come from an investigation by the enforcement body. Could the government clarify if they therefore anticipate the enforcement body being proactive in investigating compliance as well as taking action when notified of non-compliance by third parties? Given the growing size of the sector we believe it will be essential for the enforcement body to do both and be adequately resourced to undertake its own proactive investigations rather than solely relying on being notified of issues by other organisations.

[7] https://www.which.co.uk/policy/consumers/5234/onlinemarketplaces

Additionally, it is important that the intention of this regulation to better protect consumers from the risks of unsecure connected products is kept front and centre in the development of the enforcement approach. For example, particularly in relation to Requirement 2 (implement a means to manage reports of vulnerabilities), it will not be compliance with this in and of itself that will necessarily protect consumers but rather how proactively and willingly producers respond to reports received. Equally for Requirement 3, there must be active consideration of how to best ensure transparency that is clear and useful to the consumer. Such considerations by the enforcement body will be necessary in ensuring the regulations are rigorous in improving security practices.

5.5 Example enforcement actions

We support the enforcement body having a broad suite of enforcement powers so that it is able to take proportionate action against non-compliance. These must provide effective deterrents and appropriate incentives for compliance and we agree with the need for the enforcement body to be able to apply sanctions and remedies which are proportionate to the seriousness of the risk. Critically the enforcement body should ultimately have the power to suspend or ban the sale of non-compliant products, and to recall products where appropriate, in order to protect consumers. This will be essential where other enforcement measures are not sufficiently correcting issues of non-compliance in a suitable timescale to prevent the continued purchasing of unsecure products by consumers.

Consideration must be given to how enforcement can be effective against brands which, when their product is identified as unsecure and removed from sale, simply replace it with a different but equally unsecure product. This is a practice we have seen in evidence on online marketplaces, particularly with white label goods. If the enforcement body takes a 'whack-a-mole' approach on a product by product basis this is likely to prove both ineffective and unnecessarily resource intensive.

We note that the right to redress for individuals is not considered within the suite of possible enforcement actions and would welcome the government setting out what consideration they have given to this. The Consumer Rights Act 2015 provides a consumer with redress where goods are not "fit for purpose" or not of "satisfactory quality" or "as described". While the Act does make clear that safety is a consideration in this, security is not a factor which is explicitly addressed. Our view therefore is that a consumer who buys a product which does meet the requirements of the Secure by Design regulation (for example, one which had a default password) but which otherwise functions as it should could have difficulties obtaining redress from a retailer on the basis that the product was not of satisfactory quality or fit for purpose. We would therefore welcome the government's thoughts on the rights that consumers would have in such circumstances to protect them against continuing to use a non-compliant product, even where enforcement action may have been taken to prohibit the ongoing sale of that product.

5.6 and 5.7 Enforcement body considerations

Identifying and appointing an appropriate enforcement body and ensuring they have the necessary tools, powers and consumer-focused approach will be critical to the success of this regulation given the challenges and complexities of the sector. We would like to see a firm commitment from the government that they will provide the appointed body with the required resources, skills and expertise necessary to undertake this role effectively. We believe this will require investment from the government as we do not think that any current regulatory body would be able to take on this role without such resources being made available to them. We would additionally highlight the need for the chosen enforcement body to be able to work closely and in collaboration with other enforcement functions and partners to share intelligence and best practices. Going forward this is likely to require increasing amounts of coordination at an international level and the enforcement body should be empowered to take on such a role from the outset.

The example powers set out in Box 13 all appear to be broadly sensible. However, powers relating to the enforcement body's ability to require distributors and producers to provide evidence of compliance and due diligence are not included in the proposals set out in this box. Equally not listed are powers relating to the ability for the enforcement body to impose penalties and sanctions where necessary. Both of these are clearly critical to the enforcement body's function. Given the early stage thinking to enforcement it would be useful for key stakeholders to have a further opportunity to scrutinise the preferred approach once it has been determined.

The Call for Views makes clear that no decisions have been taken with regards to potential candidates for the enforcement body. However it does outline discussions have been had with a range of existing enforcement bodies, including the Office for Product Safety and Standards (OPSS). We have no firm view at this stage as to a preferred organisation to take on this role, however would highlight our broader view that for the OPSS to be an effective enforcement body and have full public confidence, it should be made an independent arms length body which operates transparently and has a clear statutory duty to put consumer protection and public safety first. Further detail on this and our thinking more generally on reforms to the enforcement landscape is in our report 'Creating a successful enforcement system for UK consumers[8]'.

Which? is the largest consumer organisation in the UK with more than 1.3 million members and supporters. We operate as an independent, a-political, social enterprise working for all consumers and funded solely by our commercial ventures. We receive no government money, public donations, or other fundraising income. Which?'s mission is to make individuals as powerful as the organisations they have to deal with in their daily lives, by empowering them to make informed decisions and by campaigning to make people's lives fairer, simpler and safer.

For more information contact Laura McCrystal on laura.mccrystal@which.co.uk

[8] https://www.which.co.uk/policy/consumers/3851/ukenforcementsystems