Government response to the “Regulatory proposals for consumer Internet of Things (IoT) security” consultation

Presented to Parliament by the Minister for Digital & Broadband, Department for Digital, Culture, Media & Sport by Command of Her Majesty

January 2020

CP 213

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at securebydesign@culture.gov.uk

ISBN 978-1-5286-1747-5

CCS0120944188

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the APS Group on behalf of the Controller of Her Majesty’s Stationery Office

The consultation and consultation stage Impact Assessment can both be found on the Secure by Design section of GOV.UK
https://www.gov.uk/government/collections/secure-by-design

Content

The Internet of Things (IoT) represents a new chapter of how technology is becoming more common in our homes, making people's lives easier and more enjoyable.

Forecasts vary, but some suggest that by 2025, there will be an estimated 75 billion internet connected devices worldwide.[1] Closer to home, it is also estimated that ownership of smart devices could rise from 10 to 15 devices per UK household this year.[2]

As these devices become a more integral aspect of daily lives for more people, there is a risk that any compromised vulnerability within a device could result in real harm. Therefore urgent joint Government and industry action is required to address these challenges.

The cyber security of these products is now an integral component of both the physical and online security of our homes. People want to trust their devices and how their data is being used. But we can only ensure widespread trust in the adoption of these new products if we demonstrate to the world that these technologies are built with the security and privacy of their users in mind. The most effective way to do this is to make sure the products that manufacturers produce are secure by design.

Many of the internet-connected devices currently on the market still lack even the most basic cyber security provisions. Over 90% of 331 manufacturers[3], supplying the UK market, reviewed in 2018 did not possess a comprehensive vulnerability disclosure programme up to the level we would expect. Breaches involving connected devices are increasingly becoming common, simply because manufacturers had not built important security requirements, such as using unique credentials, into their products.

Whilst the UK Government has previously encouraged industry to adopt a voluntary approach, it is now clear that decisive action is needed to ensure that strong cyber security is built into these products by design. Citizens' privacy and safety must not be put at risk

[1] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
[2] http://www.wrap.org.uk/sites/files/wrap/Data%20Eradication%20report%20Defra.pdf
[3]https://www.iotsecurityfoundation.org/less-than-10-of-consumer-iot-companies-follow-vulnerability-disclosure-guidelines/

because some manufacturers will not take responsibility for ensuring that security is built into their products before they reach UK consumers.

This is why we launched our consultation on regulation to secure consumer IoT in May 2019 to identify the best options to increase the cyber security baseline for consumer IoT. This built on the extensive work that we have done with industry to design a Code of Practice for Consumer IoT Security.[4] The Code of Practice is a collection of best practice security principles for connected devices, which my department published last year.

My department has also been leading efforts to create international alignment on IoT security, such as through supporting work by the European Telecommunications Standards Institute (ETSI) to develop the first global industry standard, TS 103 645.[5] Further afield, we have worked with the US, Canada, Australia and New Zealand to outline our shared commitment and approach to lifting the security of IoT devices in our respective domestic markets.[6]

We are advocating a robust and staged approach to enforcing these principles through regulation - starting with ensuring stronger security is built into products. But we will not stop there. When appropriate, we will advocate for further requirements to be mandated. I hope that this staged approach will provide manufacturers with sufficient time to implement the proposals effectively and sustainably.

I am conscious that our approach must also keep pace with technological change and innovation and, as part of our staged approach to regulation, we will also continue to review the Code of Practice for Consumer IoT Security every two years.

The UK Government looks forward to continuing to work with industry and all interested stakeholders to ensure that the UK is the safest place to be online.

Matt Warman MP

Minister for Digital and Broadband, Department for Digital, Culture, Media & Sport

[4] Code of Practice for Consumer IoT Security, October 2018 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

[5] Further work is now underway to create a European Standard, EN 303 645. We have also worked with seven other countries and various IoT experts to produce an international statement that highlights principles that align with our respective countries' frameworks to reinforce the need for global action to be taken on IoT security.

[6] https://www.gov.uk/government/publications/five-country-ministerial-communique/statement-of-intent-regarding-the-security-of-the-internet-of-things

1. Introduction

From December 2016 to February 2018, the UK Government conducted a review, in conjunction with the National Cyber Security Centre (NCSC), to identify proposals for improving the cyber security of consumer IoT products and associated services. This review came about because many ‘smart’ or internet-connected devices sold to consumers lack even basic cyber security safeguards.

The review sought to address two key risks:

1. How consumer security, privacy and safety is being undermined by the vulnerability of individual devices; and
2. How the wider economy faces an increasing threat of large scale cyber attacks launched from large volumes of insecure IoT devices.

As part of this review, the UK Government set up an Expert Advisory Group and engaged with over 100 stakeholders including industry, academics, retailers, consumers associations and international governments.

On the 7th of March 2018, the UK Government published the Secure by Design report[7]. This report included a draft Code of Practice, which set out thirteen outcome-led guidelines that manufacturers would need to implement in order to improve the cyber security of their consumer Internet of Things (IoT) products. The report advocated a fundamental shift in approach by moving the burden away from consumers having to secure their devices.

Following the March 2018 publication, the UK Government held an informal consultation from the 7th of March to the 25th of April 2018 and this feedback helped to refine the Code’s guidelines. Following engagement with NCSC, industry and external experts, the finalised Code of Practice for IoT Security[8] was published on the 14th of October 2018 alongside the UK Government’s response to the informal consultation[9].

To further support manufacturers in implementing the Code, the UK Government has published a mapping document[10] which maps the Code’s guidelines with existing UK and international recommendations and standards on IoT security. This document helps manufacturers understand how this Code sits within the broader standards landscape, and makes it simpler for them to implement the Code’s guidelines.

In May 2019 the UK Government launched a consultation on regulatory proposals for consumer IoT security[11], which concluded on the 5th of June 2019. The consultation set out the need to restore transparency within the market, particularly between manufacturers and

[7] https://www.gov.uk/government/publications/secure-by-design-report
[8] https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security
[9]https://www.gov.uk/government/publications/government-response-to-the-secure-by-design-informal-consultation
[10] https://iotsecuritymapping.uk/
[11]https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security

consumers through ensuring information about what security requirements are built into products is more clearly communicated. The UK Government is using the information provided in the consultation to refine our regulatory policy proposals further as per this document.

The regulatory proposals set out in the consultation advocated mandating the most important security requirements centred around aspects of the top three guidelines within the Code of Practice for Consumer IoT Security and the ETSI Technical Specification (TS) 103 645[12]. These are outlined below:

1. IoT device passwords must be unique and not resettable to any universal factory setting.
2. Manufacturers of IoT products provide a public point of contact as part of a vulnerability disclosure policy.
3. Manufacturers of IoT products explicitly state the minimum length of time for which the device will receive security updates.

Adhering to these three requirements is not a 'silver bullet' but they are the first practical step towards more secure devices. Achieving full market compliance with these three guidelines will ensure consumers are being given important protection against the most basic vulnerabilities, such as those which resulted in the Mirai Distributed Denial of Service ("DDOS") attack[13] in October 2016.

We recognise that security is also an important consideration for consumers. A recent survey of 6,482 consumers[14] has shown that when purchasing a new IoT product, 'security' is the third most important information factor (higher than privacy or design) for consumers. Among those who didn't rank 'security' as a top-four consideration, 72% said this was because they expected security to *already* be built into devices that were already on the market.[15] It is clear that there is currently an asymmetry between what consumers *think* they are buying and what they are *actually* buying.

The UK Government will continue to develop our proposals in light of feedback from the consultation to determine the appropriate approach to achieve our ambition of protecting consumers through improved device security whilst minimising the impact on industry. The UK Government is also conscious of the need to increase transparency surrounding relevant device security information for consumers so that they are able to make informed purchasing decisions.

The UK Government is advocating a staged approach to regulation, starting with mandating the most important security requirements (i.e. the top three guidelines), to increase the basic

[12] https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf
[13] https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html
[14] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/798543/Harris_Interactive_Consumer_IoT_Security_Labelling_Survey_Report.pdf
[15] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/798543/Harris_Interactive_Consumer_IoT_Security_Labelling_Survey_Report.pdf.

level of security within products. This is the start of the journey and the UK Government will look to increase the baseline and mandate further security requirements as and when appropriate.

2. Implementing the Code of Practice

The UK Government is leading efforts to collaborate globally, with governments and industry partners in IoT security, and will continue to work closely with international partners to ensure that guidelines drive global alignment across the IoT supply chain.

The product security requirements set out in our regulatory proposals are consistent with the Code of Practice for Consumer IoT Security and a key industry standard on consumer IoT security, ETSI Technical Specification 103 645[16], which is currently being transposed into a European Standard (EN)[17].

A draft of the EN was published in November 2019.[18] It builds on the UK's Code of Practice for Consumer IoT Security and other leading IoT security publications. When the UK leaves the EU, we will continue to contribute to the development of a global baseline on consumer IoT security, and continue to be a member of ETSI as it is a European, not an EU body.

On the 29th of July 2019, a joint ministerial statement between Australia, Canada, New Zealand, the US and UK was signed[19]. The statement sets out a commitment by all five nations to align our approaches to enhancing the security of IoT devices. We welcome complementary international efforts to improve the security of IoT. The UK Government has also recently signed an agreement to strengthen our partnership with Singapore on the security of internet-connected devices[20]. As part of our efforts to create international alignment, the UK Government has been working with partner countries in the IoT Security Policy Platform to publish a Statement which highlights common principles within international frameworks.[21]

[16] https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf. The draft version (2.0) undergoing ENAP is also public: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.00.00_20/en_303645v020000a.pdf

[17] The EN transposition process is detailed on https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=57991. In September 2019, ETSI made draft v.0.1.0 publicly available: https://docbox.etsi.org/CYBER/CYBER/Open/Latest_Drafts/CYBER-0048v010-EN-303645-public.pdf

[18] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.00.00_20/en_303645v020000a.pdf

[19] https://www.gov.uk/government/publications/five-country-ministerial-communique/statement-of-intent-regarding-the-security-of-the-internet-of-things

[20] https://www.gov.uk/government/news/secure-by-design-uk-singapore-iot-statement

[21] The IoT Platform was created by the Internet Society and includes members from different countries, organisations and industry experts. Further details can be found at: https://www.internetsociety.org/iot/iot-security-policy-platform/. The Statement has been translated into seven other languages.

3. The Consultation

The Secure by Design Consultation ran from the 1st of May 2019 to the 5th of June 2019, and closed with 60 formal written responses.

The consultation document set out substantive questions which centred around a number of aspects of our regulatory work. This included consulting on whether the Government should take powers to regulate the security of consumer IoT products. Other questions examined our core proposals on how best to implement important security requirements within consumer IoT products, mindful of the risk of dampening innovation and avoiding placing a strong burden on UK manufacturers and retailers. All questions were open questions with participants having the opportunity to provide free text responses.

Options under consideration for the consultation were:

- Option A: Mandate retailers to only sell consumer IoT products that have the IoT security label, with manufacturers to self assess and implement the security label on their consumer IoT products.
- Option B: Mandate retailers to only sell consumer IoT products that adhere to the top three guidelines of the Code of Practice, with manufacturers to self assess that their consumer IoT products adhere to the top three guidelines of the Code of Practice for Consumer IoT Security and the ETSI TS 103 645.
- Option C: Mandate retailers to only sell consumer IoT products that have the IoT security label which evidences compliance with all thirteen guidelines of the Code of Practice for Consumer IoT Security and ETSI TS 103 645, with manufacturers expected to self assess and implement the security label on their consumer IoT products.[22]

Part of our call for views was also intended to gather feedback on the details of a proposed voluntary labelling scheme, as a first step towards the first option outlined above, designed to help consumers make more informed decisions when purchasing consumer IoT devices.

[22] Further information on these options can be found in the Consultation Stage Impact Assessment

4. Consultation questions

Summaries and responses

For the free text questions, we have read every response and while we cannot reflect every point that was made by every respondent, we coded each response to identify common themes. We have, in the summaries below, provided an overview of the key or notable themes identified.

We have strived to provide a balanced overview, reflecting the range of views expressed in the consultation. To avoid repetition we have not necessarily responded to each question individually but have grouped some questions together that are on similar topics.

Q1: Do you agree that the Government should take powers to regulate on the security of consumer IoT products? If yes, do you agree with the proposed legislative approach?

Summary of responses

Number of responses: 49

Many respondents to this question demonstrated a preference for the government taking powers to regulate the security of consumer IoT products and the proposed legislative approach of mandating a minimum baseline. Some respondents stated the importance of government working to ensure alignment with existing international standards and wanted more information on the proposed self-certification process.

A number of respondents disagreed with the proposed legislative approach of mandating a security label. Others expressed that disruption or adverse impacts associated with any legislation should aim to be limited if legislation were to be introduced.

Government response

A worrying number of devices on the market still have basic flaws like default passwords, and too many manufacturers do not transparently communicate to their consumers how long the device will be supported by security updates or who to contact in the event of a vulnerability being identified. There is clear consensus that regulation in this space is needed in order to bring about sufficient change to protect citizens and the wider economy from harm.

As part of our policy development, we have taken on board respondents' feedback on what the defined roles and expectations of actors within the supply chain should be and what the implications could be for specific actors. We have commissioned further analysis work to understand and gather evidence on the impacts of the proposed regulatory approach on consumers, retailers, manufacturers and relevant actors within the supply chain.

As previously mentioned, it is important to note that in addition to developing our plans for regulation, we continue to be active in the international standards space. In order to protect UK citizens, and the broader economy from harm, we know that there will need to be alignment at an international level. In February 2019, ETSI published TS 103 645, based on the Code of Practice for Consumer IoT Security, this is the first globally applicable technical standard for consumer IoT security. ETSI are currently working on transposing the Technical Specification (TS) into a European Standard (EN)[23].

Q2. Do you agree that the 'top three' security provisions set out in the Impact Assessment form an appropriate mandatory baseline requirements for consumer IoT products?

Summary of responses

Number of responses: 49

Many respondents to this question agreed with the 'top three' security provisions as an appropriate baseline for consumer IoT products, in particular there were a number of respondents who were supportive of the requirement to remove default passwords. There were a few who agreed with only some of the provisions. It should also be noted that several respondents disagreed with some or all of the 'top three'.

Additionally, a few responses agreed with the 'top three', but with caveats in their responses, including the drafting of the legal text for introducing vulnerability disclosure policies (ensuring that it is in line with the Computer Misuse Act 1990).

Several respondents thought that the baseline should include all or more of the thirteen guidelines in the Code of Practice for Consumer IoT Security. This was for a variety of reasons, including that they thought the 'top three' did not go far enough to protect consumers; that other provisions were equally, or more, important; as well as commercial reasons. For example, one respondent commented that *"It is important for the UK government to also create mechanisms to ensure that companies who have signed up to all thirteen principles as set out in the Code of Practice can be recognised as leaders in their sectors, to avoid a race to the bottom where only those top three requirements are pursued, over any other."* Additionally, a perspective was raised in the feedback around the necessity for further checks, beyond adherence to the three most important guidelines, to be undertaken to verify the security of products before a product is sold by retailers. A further respondent noted that if all 13 guidelines of the Code of Practice were to be implemented these should only be applied where relevant to the products in question.

Whilst some respondents agreed with some or all of the 'top three', others thought that alternative provisions were more important for consumer safety and security. We heard from one individual, for example, who said that *"IoT devices should be assessed as to what risks it poses to the consumer, and therefore what guidelines it needs to comply with."*

Again, the importance of aligning baseline requirements with other EU and international standards and legislation was also expressed in a number of responses.

[23] https://docbox.etsi.org/CYBER/CYBER/Open/Latest_Drafts/CYBER-0048v010-EN-303645-public.pdf

Several respondents also expressed the need for a staged approach to regulation, where Government should consider mandating additional guidelines to increase the baseline level of security within consumer IoT products.

Government response

Based on the consultation feedback, the Government is satisfied that the three proposed security requirements are the correct ones to form the proposed mandatory baseline in the first instance. As previously announced, the Government intends to pursue a staged approach to regulation in this area. We are starting with focusing on the most important security requirements (the top three guidelines in Code/ETSI TS), but, through continuous stakeholder consultation, intend to mandate further security requirements in the future to ensure that regulation is keeping pace with emerging technology.

We would also encourage manufacturers to implement all thirteen guidelines of the Code of Practice for Consumer IoT Security within their products and processes, where appropriate.

The consultation feedback also highlighted the need for Government to consider additional options that should be undertaken to assess the security of products as part of our ambition to encourage transparency across the supply chain. To address this need, the Government will examine whether it is feasible for manufacturers to provide retailers with information on whether their products adhere to the additional ten guidelines in the Code of Practice/ETSI TS. As highlighted in the consultation responses, the Government recognises that certain guidelines will not be applicable to all consumer IoT devices and therefore there needs to be flexibility in how the remaining measures in the Code are met.

In regards to the wording of the security requirements, we are using the feedback received to inform our policy proposals and development of any legislative provisions to ensure that unintended consequences are limited. It should be noted that we are not mandating that an end of life policy for the product be published, but rather we are advocating that the product comes with information which states the minimum length of time for which it will receive security updates.

Q3. Do you agree with the use of the security label (denoting positive and negative security aspects) to communicate these requirements to consumers? Where possible, please provide evidence in support of your response.

Summary of responses

Number of responses: 46

There were a diverse range of opinions expressed in response to this question, from those who agreed with a mandatory label to those who disagreed with its use to communicate requirements to consumers. The most common response agreed to some extent with the concept of labelling, but with caveats to their answer. For example, a common view was that respondents agreed with positive labelling, but not negative labelling.

One reason for this was that respondents felt that negative labels could dampen innovation and create market barriers, as retailers are less likely to stock negatively labelled products. Others suggested that negative labelling could lead to consumers buying non-labelled foreign products, rather than those manufactured and/or sold in the UK with a negative label.

A respondent suggested that *"transparency is critical to the success of this endeavor. A label is a simple, effective way to communicate the manufacturer's commitment and product security rating, but it's also critical not to rely on a static label."*

Some respondents also expressed concerns that labelling could lead to complacency among consumers and overconfidence in the security of their products. One of the responses on this point suggested that *"the proposed labelling scheme clearly maintains the burden on consumers to ensure their privacy and security and as such is not the best option from the point of view of consumers."*

Other than those who disagreed with the mandatory label (Option A), a few respondents also highlighted a preference for the alternative options set out in the consultation.

Q4. Do you agree with the wording of the labelling design? If not, could you provide suggestions for alternative wording. Where possible please provide evidence alongside these suggestions.

<u>Summary of responses</u>

Number of responses: 34

More responses disagreed with the proposed wording than agreed. Several also notably disagreed with the physical presentation of the label. Some suggested using an online or 'live' label, rather than a static label, due to the dynamic nature of the cyber security environment, a theme that was also highlighted in responses to Question 3.

For example, one response was that *"A static one-size-fits-all label added as a tag to the product or a system cannot realistically cover the array of current and future IoT technologies and provide details on the potential risks attributable to them. Security cannot be simply and accurately gauged using conventional means, unlike an energy-efficiency label on a washing machine, for example."*

Q5. Do you agree with our recommended option to mandate retailers in the first instance to not sell consumer IoT products without a security label (Option A)? If not, could you state your preferred option, or provide suggestions for your alternative. Please provide evidence alongside these suggestions.

<u>Summary of responses</u>

Number of responses: 42

There were a broad range of opinions expressed in response to this question. A number of responses agreed with Option A, to mandate retailers only to sell consumer IoT products with a security label.

A respondent said that *"mandating retailers to not sell consumer IoT products without a security label is the best approach, as it ensures greater transparency and provides the* *necessary information enabling consumers to make an informed choice about selecting a specific IoT product."*

However, there were also a number of other responses that preferred Option B (to mandate that only products complying with the 'top three' guidelines are sold) as the most popular alternative regulatory option. An illustration of this can be seen through the following response whereby a stakeholder advised that *"there is a danger in pursuing Option A that the success of the labelling scheme outweighs the success of the core goal: to minimise the security risk of consumer IoT. Option B, which would mandate retailers to sell only products that meet the three security baseline, would go further in protecting customers from online threats."*

Another respondent said that *"the Government's suggested course of action, Option A, would not prevent insecure products from being sold and connected – as products could still be labelled as non-compliant and sold by retailers, or alternatively labelled as compliant when the manufacturer has not conducted a sufficient or reliable self-assessment exercise."*

Some responses also highlighted the importance of an adequate 'implementation grace period' to allow manufacturers to fully embed this legislation within their supply chain.

Q7. Do you have a view on how best to approach issues associated with existing consumer IoT products on the market that, under these new proposals, will not have a label?

Summary of responses

Number of responses: 25

Views on this topic were diverse. One theme is the need for an adjustment period before the regulation is enforced to give businesses enough time to implement the proposed changes, as well as clearly communicating to consumers that existing products without a label are not necessarily insecure.

A number of responses also suggested an online label for existing products, while others proposed labelling at the point of sale rather than on product packaging itself. Another, less recurrent view highlighted the potential unintended consequence of insecure products flooding the market before the regulations come into force.

Government response to questions 3, 4, 5 and 7 combined.

We have considered the responses carefully and taken on board the concerns of those who feel there are issues associated with a specific label being mandated to be placed on products. We recognise the complexity of supply chain management and potential disruption to business as a result of affixing a label to physical products.

Feedback questioned whether manufacturers would be willing to place a negative label on their products and the difficulty for retailers to take necessary steps to validate the manufacturer's claims in a voluntary scenario. As such, we will not proceed with launching the voluntary labelling scheme at this time and will undertake further policy development based on the feedback.

We note the concerns raised by some respondents as to how self assessment would work in practice, and who would be liable in the event of a false declaration of conformity. We are not advocating for a specific assessment process for manufacturers to follow, but rather encourage the supply chain to use tools and guidance already available, namely industry led assurance and certification schemes that best meet their price point and are consistent with the Code of Practice for Consumer IoT Security.

By not mandating a specific assessment approach, we are empowering manufacturers to undertake the relevant assessment process that is appropriate for their product. We feel that this approach will not only reduce costs for the manufacturer, but also help avoid some unintended barriers to market for conscientious manufacturers of all scales.

Responses to the consultation have also reinforced our view that consumers should not be expected to assess the security of the devices that they purchase. The information is not readily available or easily accessible, and many make the (incorrect) assumption that all devices are already ‘safe’ because they are for sale through trusted fora or marketplaces.

Taking the evidence into account, deeper consideration needs to be given to this issue. Consumers need to be confident about the security of their smart devices when buying the device. With this in mind, we are therefore conducting further policy development on how UK retailers (or those selling into the UK) can best evidence security information to consumers at the point of sale, whilst still ensuring minimum disruption for the supply chain.

Q6. The consultation stage Impact Assessment published alongside the consultation document explores the costs and benefits of the options considered for this policy. Do you agree with our analysis?

Summary of responses

Number of responses: 22

Many respondents to this question thought that there were missing costs and impacts from the analysis. Several thought that the estimated cost to businesses was too low, such as familiarisation costs, as well as the need to consider UK competitiveness in international markets.

However, responses provided very limited additional evidence or information on alternative costing figures.

Government response

Even though there was minimal feedback on the Government’s analysis of the issue, we still appreciate that this is an important issue when considering a proportionate regulatory response. Therefore, we will continue to engage with industry as our proposals develop and will be commissioning further evidence work over the coming months to better understand the impacts of all proposed regulatory options.

Q8. We welcome your views on the cost to businesses of implementing this regulatory approach within the secondary market. Please provide evidence.

Summary of responses

Number of responses: 11

Common themes in the responses to this question included the difficulty in monitoring goods sold in the secondary market, as well as the view that the costs associated with this regulatory approach will be greater for small and medium businesses, compared to larger businesses.

Government response

We will continue to engage with industry as our proposals develop and will be commissioning further evidence work over the coming months to better understand the impacts of all proposed regulatory options on secondary markets.

Q9. We welcome views on costs to small and micro businesses in the UK as a result of these regulatory proposals. In particular, consider how best to quantify the impact on profits of small and micro firms.

Summary of responses

Number of responses: 9

Responses generally demonstrated that the cost of complying with the regulatory proposals would likely disadvantage small and micro businesses, including start-ups.

However, another less common view was that costs should not be a barrier to small and micro businesses, provided that there was a sufficient adjustment period for the implementation of the regulatory proposals. Moreover, others thought that small and micro businesses should not be exempt from any regulation.

One respondent said that *"small and micro businesses should be able to meet the main requirements of the proposals at minimum cost providing there is sufficient time to phase in compliance."*

Government response

We will continue to engage with industry as our proposals develop and will be commissioning further evidence work over the coming months to better understand the impacts of all proposed regulatory options on small and micro firms.

Q10. Do you have a view on how best to enforce the requirements set out in both regulatory options? In particular, consider which UK agency is best placed to undertake enforcement and whether additional penalties would need to be set out to ensure that companies correctly use the labels.

Summary of responses

Number of responses: 21

Many respondents thought that Trading Standards should be responsible for enforcing regulatory proposals on consumer IoT devices. A few responses also suggested that Ofcom could be the enforcement agency.

In addition to this, several respondents expressed the opinion that the requirements should not be self-assessed.

"While self-certification of compliance with the standards appears to have strong support, it must be accompanied by a system of regular, independent checks which will reassure the public that the system is working well."

Government response

It is clear that respondents to the question felt that enforcement action would naturally fall within Trading Standards' existing role for consumer protection in the UK. We are mindful of placing more responsibility on existing UK agencies at a time when resources are prioritised on existing consumer protection priorities.

We have been working to better understand how this regulation could be effectively enforced through existing UK agencies and will continue to do so in the coming months.

5. Next steps

The UK Government takes the issue of consumer IoT security very seriously and appreciates the urgent need to move the expectation away from consumers securing their devices and instead ensure that strong cyber security is built into these products by design.

Taking the feedback on board from the consultation responses, we will conduct further stakeholder engagement to further develop our regulatory options based on the top three guidelines in the Code of Practice and ETSI TS. The Government will also undertake further work to determine the most appropriate way to communicate security information to consumers. This will involve examining an alternative option to the labelling scheme whereby retailers[24] would be responsible for providing information to the consumer at the point of sale (both online and in stores). This is because we want to ensure that those who manufacture, develop and stock IoT devices are clear and transparent with those that purchase them, sharing important information about the cyber security of these devices.

Our intention in the future will be to take a staged approach to mandating further security requirements, beyond the most important three guidelines indicated in this document, to ensure that regulation is keeping pace with technological change and the threat landscape. This staged approach will involve reviewing and amending as required the Code of Practice for Consumer IoT Security every two years. The consultation feedback and work that will be undertaken in the coming months will contribute to the Government publishing a final stage regulatory impact assessment later in 2020.

In the interim we will also be embedding and encouraging the adoption of the ETSI TS 103 645 standard and working on greater transparency. In addition, we continue to contribute to the development of European Standard (EN) 303 645.

[24] UK-based company who sells a consumer IoT product online or in-store or an international company who is selling products directly to UK consumers.

Annex A: Summary of consultation questions

Catalogue of consultation questions

The consultation document set out 12 substantive questions to explore the government's regulatory work on consumer IoT. All questions were open questions with participants having the opportunity to provide free text responses

Consultation Questions: Feedback on regulatory approach and labelling scheme	
1.	Do you agree that the Government should take powers to regulate on the security of consumer IoT products? If yes, do you agree with the proposed legislative approach?
2.	Do you agree that the ‘top three’ security provisions set out in the Impact Assessment form an appropriate mandatory baseline requirements for consumer IoT products?
3.	Do you agree with the use of the security label (positive and negative) to communicate these requirements to consumers? Where possible, please provide evidence in support of your response.
4.	Do you agree with the wording of the labelling design? If not, could you provide suggestions for alternative wording. Where possible please provide evidence alongside these suggestions.
5.	Do you agree with our recommended option to mandate retailers in the first instance to not sell consumer IoT products without a security label (Option A)? If not, could you state your preferred option, or provide suggestions for your alternative. Please provide evidence alongside these suggestions.

Consultation Questions: Feedback on the impact of our proposals	
6.	The consultation stage Impact Assessment published alongside the consultation document explores the costs and benefits of the options considered for this policy. Do you agree with our analysis? In particular, please consider the following, and provide analysis to back up your views: a) Direct costs determined to be in scope. b) Assessment of the impact on competition. c) Further evidence on the cost of cyber breaches to IoT consumers in the UK, and the incidence of attacks against IoT devices. d) Data and research on the number of IoT manufacturers and retailers which sell their goods on the UK market. e) Estimates for the number of hours and cost (e.g. consultants) it would take businesses of different sizes to familiarise with this legislation. f) Potential methods of self-assessment and the relative costs to business. g) Evidence on the average number of IoT products produced in the UK per business.

	h) Evidence on types of labelling and their respective costs. i) The likelihood that manufacturers would pass on labelling costs to consumers. j) Additional costs of staff time and any other costs incurred, such as training, required to comply with the regulation. k) Evidence on the cost of implementing each of the thirteen Code of Practice guidelines and any evidence or estimates of how many of the IoT products available on the market currently comply. l) On average, how often are existing IoT products redeveloped, how many new products IoT manufacturers produce per year, and the average number of products per manufacturer. m) Evidence on IoT cyber security breaches against UK consumers and their average cost. n) Evidence on the potential reduction in breaches as a result of implementing the different code of practice guidelines. o) Evidence on the predicted future path and nature of IoT attacks in the UK if nothing is done to increase security from its current level. p) The risks and uncertainties identified within the impact assessment.
7.	Do you have a view on how best to approach issues associated with existing consumer IoT products on the market that, under these new proposals, will not have a label? In particular, how could the proposed regulatory approach impact retailers who will have existing non-labelled consumer IoT in stock. Please provide evidence.
8.	We welcome your views on the cost to businesses of implementing this regulatory approach within the secondary market. Please provide evidence.
9.	We welcome views on costs to small and micro businesses in the UK as a result of these regulatory proposals. In particular, consider how best to quantify the impact on profits of small and micro firms. Please provide evidence.

Consultation Questions: Enforcement	
10.	Do you have a view on how best to enforce the requirements set out in both regulatory options? In particular, consider which UK agency is best placed to undertake enforcement and whether additional penalties would need to be set out to ensure that companies correctly use the labels. Where possible, please provide evidence.

Consultation Questions: Further feedback	
11.	Please provide any additional comments on the consultation stage impact assessment, the regulatory options set out and the proposed labelling scheme.
12.	We welcome any additional feedback not already captured above.

CCS0120944188

ISBN 978-1-5286-1747-5