Department for
Digital, Culture,
Media & Sport

Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security

May 2019

Consultation on the Government's regulatory proposals regarding consumer Internet of Things security.

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

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

Contents

General Information

Purpose of this consultation

The Department for Digital, Culture, Media and Sport (DCMS) is consulting on regulatory proposals regarding consumer Internet of Things security.

This consultation document is complementary to the consultation stage impact assessment "Mandating security requirements for consumer Internet of Things (IoT) products".

Issued: 01/05/2019

Respond by: 05/06/2019

Enquiries to:

Email: securebydesign@culture.gov.uk

Address: Department for Digital, Culture, Media and Sport, 4th Floor, 100 Parliament Street, London, SW1A 2BQ

Consultation reference: Consultation on regulatory proposals regarding consumer Internet of Things security

Who is this consultation for?

- Device Manufacturers: The entity that creates an assembled final internet-connected product. A final product may contain the products of many other different manufacturers.
- IoT Service Providers: Companies that provide services such as networks, cloud storage and data transfer which are packaged as part of IoT solutions. Internet-connected devices may be offered as part of the service.
- Mobile Application Developers: Entities that develop and provide applications which run on mobile devices. These are often offered as a way of interacting with devices as part of an IoT solution.
- Retailers: The sellers of internet-connected products and associated services to consumers.
- Those with a direct or indirect interest in the field of consumer IoT security, including consumer groups, academics and technical experts.

How to respond

Your response will be most useful if it is framed in direct response to the questions posed below, though further comments and evidence are also welcome.

Responses should be submitted electronically to securebydesign@culture.gov.uk or via post to Department for Digital, Culture, Media and Sport, 4th Floor, 100 Parliament Street, London, SW1A 2BQ

Additional copies:

You may make copies of this document without seeking permission. An electronic version can be found at https://www.gov.uk/government/collections/secure-by-design

Confidentiality and data protection

Information provided in response to this consultation, including personal information, may be subject to publication or disclosure in accordance with the access to information legislation (primarily the Freedom of Information Act 2000, the Data Protection Act 2018 and the Environmental Information Regulations 2004).

If you want information that you provide to be treated as confidential please say so clearly in writing when you send your response to the consultation. It would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded by us as a confidentiality request.

Quality assurance

This consultation has been carried out in accordance with the Government's Consultation Principles. If you have any complaints about the consultation process (as opposed to comments about the issues which are the subject of the consultation) please address them to: securebydesign@culture.gov.uk

Executive Summary

As the technological advances of the 21st century continue to accelerate, consumers are bringing more and more 'smart' devices (i.e. consumer IoT products) into their homes, such as smart TVs, internet connected toys, smart speakers and smart washing machines. The Internet of Things (IoT, also known as 'internet-connected' or 'smart' products) is already being used across a range of industries and it is delivering significant benefits to the lives of its users.

In the future, we expect an ever increasing number of more developed consumer Internet of Things products and services. These devices will be able to anticipate and meet their users' needs and will be able to tailor information specifically to them across everything from home energy to security. This will offer users the opportunity to live more fulfilling lives; saving time, effort and money.

As with all new technologies, there are risks. Right now, there are a large number of consumer IoT devices sold to consumers that lack even basic cyber security provisions. This situation is untenable. Often these vulnerable devices become the weakest point in an individual's network, and can undermine a user's privacy and personal safety. Compromised devices at scale can also pose a risk for the wider economy through distributed denial of service (DDOS) attacks such as Mirai Botnet in October 2016.

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

We have previously stated our preferred an approach whereby industry self-regulate to address these issues, but that we would consider regulation where necessary. In October 2018 we published a Code of Practice for IoT Security, alongside accompanying guidance, to help industry implement good security practices for consumer IoT.

Despite providing industry with these tools to help address these issues, we continue to see significant shortcomings in many products on the market.

We recognise that security is an important consideration for consumers. A recent survey of 6,482 consumers has shown that when purchasing a new consumer IoT product, 'security' is the third most important information category (higher than privacy or design) and among those who didn't rank 'security' as a top-four consideration, 72% said that they expected security to *already* be built into devices that were already on the market.[1] It's clear that there is currently a lack of transparency between what consumers *think* they are buying and what they are *actually* buying.

Our ambition is therefore to restore transparency within the market, and to ensure manufacturers are clear and transparent with consumers by sharing important information

[1] Consumer Internet of Things Security Labelling Survey Research Findings, *Harris Interactive*, March 2019.

about the cyber security of a device, meaning users can make more informed purchasing decisions.

Having worked with stakeholders, experts and the National Cyber Security Centre (NCSC), we are now consulting on proposals for new mandatory industry requirements to ensure consumer smart devices adhere to a basic level of security. The proposals set out in this document seek to better protect consumers' privacy and online security which can be put at risk by insecure devices.

We are mindful of the risk of dampening innovation and applying a strong burden on manufacturers of all shapes and sizes. This is why we have worked to define what baseline security looks like, in line with the 'top three' guidelines of the Code of Practice. Our ambition is for the following security requirements to be made mandatory in the UK. These are:

1. All IoT device passwords shall be unique and shall not be resettable to any universal factory default value.
2. The manufacturer shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues.
3. Manufacturers will explicitly state the minimum length of time for which the product will receive security updates.

Meeting these practical and implementable measures would protect consumers from the most significant risks (such as the Mirai attack in 2016). This would also restore transparency in the sector and allow consumers to identify products that will meet their needs over the lifespan of the product. In addition, mandating vulnerability disclosure policies will enable an effective feedback mechanism to operate, between the security research community and manufacturers.

One of the core aims of the consultation is to listen to feedback on the various implementation options we have developed in partnership with industry and stakeholders. These include the following three options:

- **Option A:** Mandate retailers to only sell consumer IoT products that have the IoT security label, with manufacturers to self declare and implement a security label on their consumer IoT products.
- **Option B:** Mandate retailers to only sell consumer IoT products that adhere to the top three guidelines, with the burden on manufacturers to self declare that their consumer IoT products adhere to the top three guidelines of the Code of Practice for IoT Security and the ETSI TS 103 645.
- **Option C:** Mandate that retailers only sell consumer IoT products with a label that evidences compliance with all 13 guidelines of the Code of Practice, with manufacturers expected to self declare and to ensure that the label is on the appropriate packaging.

Later this year, the security label will initially be run on a voluntary basis until regulation comes into force and the government will make a decision on which measures to take forward into legislation following analysis of the responses received through this consultation. We recognise that any regulation will need to mature over time, and additional information for this approach is within the consultation stage impact assessment ‘mandating security requirements for consumer IoT products’.

Introduction: Secure by Design

What is Consumer IoT?

For the purposes of this consultation and the consultation-stage Impact Assessment, we have defined consumer IoT products (i.e 'smart' or 'internet connected' products) as products that are connected to the internet and/or home network and associated services[2]. A non-exhaustive list of examples includes:

- Connected children's toys and baby monitors
- Connected safety-relevant products such as smoke detectors and door locks
- Smart cameras, TVs and speakers
- Wearable health trackers
- Connected home automation and alarm systems
- Connected appliances (e.g. washing machines, fridges)
- Smart home assistants

March 2018: Draft report

The UK Government published the Secure by Design: Improving the cyber security of consumer internet of things report on the 7 March 2018 which set out how we will work with industry to address the challenges of insecure consumer IoT.

The Secure by Design report advocated to remove the burden from consumers to securely configure their devices and instead ensure that strong security is built into IoT devices and services by design.

Following the report's publication on the 7 March 2018, we sought feedback on the report's draft Code of Practice and the other interventions proposed in the report through an informal consultation, which ended on the 25 April 2018.

October 2018: Code of Practice

In October 2018, the Government published the Code of Practice for Consumer IoT Security, a comprehensive mapping to existing guidance and standards and an update on other proposals, such as our work on a consumer labelling scheme.

The Code brings together 13 guidelines that are widely considered good practice in IoT security. The purpose of the Code is to support all parties involved in the development, manufacturing and sale of consumer IoT products.

The Code was developed with, including through an informal consultation, technical experts, the National Cyber Security Centre (NCSC) and a wide variety of other stakeholders, including industry and consumer groups, manufacturers, retailers and many other organisations.

[2] https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security#scope-of-applicability

To assist manufacturers to implement the Code, DCMS has also published a mapping document which links the 13 guidelines to existing standards, recommendations and guidance on IoT security and privacy from around the world. Whilst not exhaustive, it represents one of the largest collections of guidance on IoT security and privacy to date and is available to all.

February 2019: ETSI Technical Specification 103 645

In February 2019, ETSI, the European Standards Organisation, published Technical Specification 103 645, the first globally-applicable industry standard for consumer IoT security. This industry standard builds on the Code of Practice, but has been designed to work for European and wider global needs.[3] The standard is set to inform, at home and abroad, the development of regulation and industry-led certification schemes.

For businesses with an international supply chain and customer base, the standard provides an avenue to pursue a harmonised approach to implementing good security practice for their products.

[3] https://www.etsi.org/newsroom/press-releases/1549-2019-02-etsi-releases-first-globally-applicable-standard-for-consumer-iot-security

The ‘Top Three’ guidelines

Building on feedback from industry stakeholders and experts, we have discussed the practicalities of making all aspects of the Code of Practice mandatory. We recognise that implementing this would place a heavy burden on manufacturers, many of whom have extensive international supply chains. This burden would be felt more by smaller organisations, and could dampen innovation.

In light of the urgent needs, we have sought to identify a practical solution that could be implemented sooner, that could protect consumers and the wider economy, whilst also ensuring growth across the sector.

We have consulted with experts at the NCSC and across the public and private sector to determine which aspects of the Code of Practice for Consumer IoT Security should be made mandatory in the first instance, balancing the need to deliver an effective baseline that protects consumers whilst also minimising the additional burden on industry. In this process, we have determined this focus as aspects of the ‘top three guidelines’ within the Code of Practice for Consumer IoT Security.

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

From an enforcement perspective, these requirements are easier to test - products either meet these requirements or they do not. Meeting these practical and implementable measures would protect consumers from many of the most significant and numerate risks (such as the Mirai botnet attack in 2016). This would also restore transparency in the sector and allow consumers to identify products that meet basic security provisions over the course of time that they intend to use it for. In addition, mandating vulnerability disclosure policies will enable an effective feedback mechanism to operate, between the security research community and manufacturers.

Over the coming years, we will continue to review the threat landscape and the need for higher security practices to be mandated. We will continue to consult with industry and will assess the practicalities of adding security provisions in legislation. It is our intention to mandate further requirements from the Code as part of staged approach to regulation.

Designing a Security Label

The Government previously announced that we will review options to create a labelling scheme for consumer IoT products to aid consumer-purchasing decisions and to facilitate consumer trust in manufacturers that adhere to the Code.

This is important because consumers are currently expected to conduct pre-purchase research or review product information in store to find information on the security features of different IoT products before deciding which device to purchase. This presents a wide array of issues because many consumers do not have the technical expertise to know what security features should be built into their devices. Moreover, a significant amount of manufacturers do not provide this information online or within product documentation.[4]

The labelling scheme is designed to help consumers make more informed decisions when purchasing consumer IoT devices. It has been developed in consultation with NCSC, the Department for Business, Energy and Industrial Strategy (BEIS), Home Office and external stakeholders, such as industry bodies, manufacturers, international governments, retailers, consumer associations, academics and IoT experts.

As part of the labelling project, DCMS set-up a working group to develop and test our labelling proposals. DCMS worked extensively with PETRAS, an academic consortium, to fund and compile evidence to inform our work. This included a literature review, a consumer survey, a study to evaluate what security information is provided with devices.[5]

The label design has also been created based on an additional survey (funded by DCMS and) conducted by Harris Interactive which involved 6,482 consumers. This report has been published alongside this consultation.[6] Further information on the evidence and rationale for the security label is outlined within the consultation stage impact assessment 'Mandating security requirements for consumer IoT products'.

The label is based on aspects of the 'top three' guidelines explained previously. To qualify for a 'positive label', manufacturers will need to self-certify that their devices' passwords are unique and are not resettable to any universal factory setting and that they have implemented a vulnerability disclosure policy. Manufacturers will also need to explicitly state the minimum length of time (month and year) for which the device will receive security updates (Dec 2021 has been used as an example). Manufacturers will still have the opportunity to extend the support period for their devices, however we would expect them to communicate this to their customers.

---

[4] PETRAS Report, 'What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?', December 2018. https://osf.io/preprints/socarxiv/63zkt/

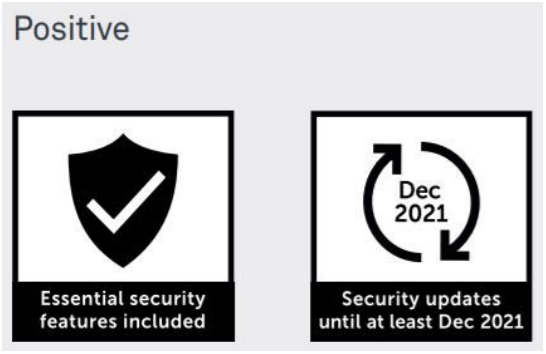
[5] DCMS also funded Make it Clear to examine the prominence of labelling on product packaging and product websites.

[6] Consumer Internet of Things Security Labelling Survey Research Findings, *Harris Interactive*, March 2019.

The draft designs for the labelling scheme that we are consulting on can be found below. We are conscious of trademark requirements surrounding the use of generic icons and are currently seeking legal advice on this. We considered creating unique shapes for each icon, however we assessed that this would create strong challenges in explaining the meaning of the label to UK consumers.

Additionally, the Harris Interactive survey included a question which asked if the icons were suitable for the proposed criteria. 92% stated that the shield and arrows were the best designs for the label. The highest alternative option (a padlock) was suggested by less than 1%.

We welcome feedback on the designs and will consider making modifications to the label design following the consultation before launching it as a voluntary scheme later this year.



Regulatory proposals

We had previously stated that our preference was for industry to self-regulate, adopt high standards voluntarily and improve the level of transparency with consumers regarding the standard of in-built cyber security measures. As the sector has grown, so too has the risk to individuals and the wider economy.

Our ambition is to protect citizens who use these devices, to protect the wider economy from a coordinated attack and to support the long term growth of the IoT sector. As such, we see an urgent need for the good practice set out in the October 2018 Code of Practice for Consumer IoT Security, and more recently in ETSI's Technical Specification 103 645, to be made mandatory.

As part of this process, we are now consulting on a number of options for guidelines in the Code of Practice to be made mandatory that ensure all consumer IoT devices adhere to a basic level of security. These options are set out in the Consultation Stage Impact Assessment "Mandating security requirements for consumer IoT products".

Proposals for implementation:

Building on our work, in collaboration with industry and core stakeholders, to identify the 'top three' guidelines and develop the security label, we have set out the following proposals within the consultation stage impact assessment.

- **Option A** (preferred option): Mandate retailers to only sell consumer IoT products that have the IoT security label, with manufacturers to self assess and implement a security label on their consumer IoT products.
- **Option B:** Mandate retailers to only sell consumer IoT products that adhere to the top three guidelines, with manufacturers to self assess that their consumer IoT products adhere to the 'top three guidelines' of the Code of Practice for IoT Security.
- **Option C:** Mandate that retailers only sell consumer IoT products with a label that evidences compliance with all 13 guidelines of the Code of Practice, with manufacturers expected to self assess and to ensure that the label is on the appropriate product packaging.

The security label will initially be run on a voluntary basis until regulation comes into force when Parliamentary time allows.

DCMS recognises the importance of a product label in restoring transparency within the sector. The proposed product label is based on an extensive range of evidence and has been thoroughly tested with consumers.

The clear evidence is that consumers care a great deal about the cyber security of their IoT products and wish to make informed decisions. We recognise the challenge in not over-burdening consumers with too much information, and also the risk of dampening innovation by overburdening industry with a long set of guidelines.

Following the consultation, if the label forms part of our regulatory proposals, we would consider mandating usage guidelines to ensure that the label is clearly signposted to consumers both on physical products and on product websites.

DCMS will ensure that future timelines will give sufficient time to retailers to ensure that they are not adversely affected by any of these proposals. This will also provide manufacturers with the time to make changes to their organisational processes and supply chain.

Regulatory Structure

We intend to create Primary legislation, when Parliamentary time allows, that gives the Secretary of State for DCMS the ability to set the requirements for a mandated labelling scheme and/or to set security requirements for devices on sale in the UK. These requirements would be set out in Secondary legislation.

The Government's intention is to add, in small steps, further guidelines from the Code of Practice to the security requirements. This would only take place following further formal or informal consultation with stakeholders and analysis of the impact of such changes.

Next Steps

Following this consultation, the government will make a decision on which measures to take forward into legislation following analysis of the responses received. The measures we will take forward can be one of the options proposed here or a combination of these options. A final impact assessment will be published alongside the decision.

Once the chosen option has matured, we will review whether to mandate beyond the 'top three' requirements at a later date and in what format this is implemented.[7]

[7] Further information can be found in the impact assessment report on page 24.

Catalogue of consultation questions

We welcome your comments and feedback on all of the proposals and evidence put forward within the consultation stage impact assessment. To help structure your responses, please refer to the below table of questions as a guide.

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 13 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.