securebydesign@culture.gov.uk
Cyber Security Team,
Department for Digital, Culture, Media and Sport,
Level 4, 100 Parliament Street,
Westminster,
London, SW1A 2BQ

Date 5 June 2019
Reference Response to DCMS Consultation: Regulatory proposals for Consumer IoT security

Dear Sir/Madam,

The UK Chapter of the Internet Society (ISOC UK) welcomes the UK DCMS advancing useful ideas and practical options on IoT labelling. However in our view the IoT device market will be driven in this region by the European Union (EU) irrespective of UK brexit. If the UK was to proceed forward with labelling, ISOC UK would strongly argue that it really makes sense to do this as part of the EU and not UK alone.

The UK Chapter supports a light regulatory approach to IoT security whilst at the same time empowering end users to make a conscious choice about the features of a device they are purchasing. This is not the same as an enforcement culture that risks hindering the growth of IoT in the UK.

We support Option A, starting with regulation of the top 3 guidelines as a starting point. (Option A is: 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.)
Our interpretation of this option is that it is the manufacturer of the product that will affix the label to its product and that the role of a retailer will be purely of checking that the goods are labelled. Option A makes the task of a retailer easier to differentiate between products that have the label and products that do not have the label. Option A also makes is easier for an end user to determine if the product they are purchasing is compliant or not, bearing in mind a product could have a negative label attached and still satisfy Option A.

In addition to supporting Option A, the UK Chapter also supports Option B (Mandate retailers to only sell consumer IoT products that adhere to the top three guidelines, with 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.)
Our understanding is that Option A provides the labelling for a product, whether it adheres to the top three guidelines, whilst Option B mandates adherence to these top three guidelines.
In the future, depending on end user response, it could be possible to extend to all 15 guidelines. However, it would be important to first obtain end user and market feedback before proceeding further.

We recognise that products that are sold online are often sold cross-border, thus there would be no possibility to apply this regulation to products purchased directly from overseas. However, this free choice of purchasing option should be kept.

At present, we have no suggestion as to how enforcement should take place - but this should not add a burdensome cost to the product itself that would then trigger end users to prefer sourcing the product directly overseas.

There must also be focus on developing and supporting user capacity to secure their devices and manage their networks of devices. i.e., avoid a situation where the power to manage is regulated in such a way that manufacturers and intermediaries prevent users from having sufficient control.

Overall, we caution DCMS into implementing a system that will keep the market as open as possible and to make sure that neither the labelling nor the adherence to the guidelines translate into a locking-in of a user towards a particular manufacturer's products or services. Types of Consumer IoT devices that could previously function without being connected to the Internet (refrigerators, washing machines etc.) should be able to function safely after the period of software updates has expired and the manufacturer should not be able to turn off a device's primary functionality. We believe that this still remains to be detailed further for a satisfactory roll-out of proposals that could include a potential "IoT lifecycle programs".

Response to questions:

Labelling scheme

●Do you agree with the use of the security label (positive and negative) to communicate these requirements to consumers?

Yes.

However, a lot depends what "security" means:

- Reasonable passwords
- No default passwords
- Firmware update capability
- Support for updates for next 10 years
- Etc.

CE certification should require all of the above.

As the world of technology changes all the time, new attacks are discovered. The update capability is necessary, but preferably something that doesn't require a consumer to USB connect to every hundred IoT device they may have.

● Do you agree with the wording of the labelling design?

Yes

● 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)?

Yes. Internet's global nature makes things more complex, because

a. Things can connect to other places that have different regulation

b. IOT systems consist of gadgets on which everyone focuses so much and cloud parts that consumers legislators are not focusing nearly enough. Those cloud

c. " parts" data and metadata could again be found in other places

It is not easy to make mandates, however like electric appliances must have CE certification, the same should be done with IoT devices. However, the application or part of an application deployed with a device may be controlled by a third party anywhere in the world. The labelling scheme needs to be clear what security the user is being assured of and what the user needs to take further steps to assure themselves.

A danger with labelling is it can give a false sense of security. IoT can become very treacherous

●How best to approach issues associated with existing consumer IoT products on the market that, under these new proposals, will not have a label?

Regulated or voluntary mechanisms (i.e. labelling, certificates, mandated requirements) generally only apply after year 20XX (to be determined). Existing devices could still be sold until stocks run out. There should be the ability for a consumer to check the device details on a Web site, checking if it has gained a label since it was manufactured.

Though the consultation asks questions about labelling, it raises additional questions:
Should regulation and certification deal only with the device or also look at the cross-border data or also the cloud entity that provides much of the functionality that the consumer is after? In our view, Data produced by consumer IoT devices should be made accessible to end users thus allowing users to keep a copy of their data.

Finally, a fundamental step that does not appear to have been reached yet is the design and implementation of a test process/protocol that would be used by labs to test consumer IoT devices. Without such protocols, manufacturers could argue that their evaluation on whether a device/product satisfies the three guidelines is undefined and we might end up with mess of different test sets that are not uniform across manufacturers - and definitely not testable by establishments and labs that could be contracted to perform the evaluation of these products.

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:

We appreciate the efforts to make a cost benefit analysis for the proposed options. At the internet Society, we also wanted to better understand the economic aspects of consumer IoT security In line with our IoT Trust by Design Campaign and we commissioned an independent study conducted by Plum Consulting titled "The economics of the security of consumer-grade IoT products and services", that we believe will be a useful resource for the DCMS as well.

The report points out the main economic obstacles towards better consumer IoT security after a synopsis of the consumer IoT market and the current state of security- or lack thereof. First of all the asymmetrical level of information in consumers and manufacturers makes it difficult for the consumers to identify products with weak security, which results in investment in security not being seen as a competitive differentiator for manufacturers. Additionally, since the cost of security breaches are borne by the device owner or third parties rather than the manufacturer, the incentives for investing in security are misaligned due to these externalities. Because of these factors, combined by a number of cognitive biases of consumers, instead of including

effective security by design, which would cost extra, require specialised skills and slow down the process, manufacturers tend to prioritise reducing cost and quickly sending the devices to the market.

To incentivise manufacturers and shift consumer demand in the market for strong consumer IoT security there are various mechanisms to be taken by multiple stakeholders. These mechanisms also vary by their cost and difficulty of implementation with pros and cons of their own. The report provides a taxonomy and comes up with recommendations for the industry and policymakers to improve consumer IoT security; including prioritising consumer guidance, leveraging public procurement procedures for products with strong security, encouraging responsible vulnerability disclosures, developing a trustmark for secure consumer IoT devices, prosecuting misleading claims on security and prescribing a general set of security principles. From this perspective, mandated security requirements through regulation is considered as a last resort, only if all other initiatives fail to improve security in consumer IoT devices.

One key takeaway from the report is that improving consumer IoT security calls for actions from various stakeholders involved and all the recommended actions complement each other. The complex IoT ecosystem is only as strong as its weakest link and a collaborative approach to security is essential for success both on national and global level.

It is important to acknowledge that the risk from insecure consumer IoT devices is a global problem: while one country may take steps to keep insecure IoT devices off its domestic market, it will still face risks from insecure devices in other jurisdictions. Growth in connected devices across the world will likely lead to increased transnational liability, security and privacy issues, which existing legal cooperation frameworks may be ill- equipped to handle. Cross-national, regional and global multi-stakeholder efforts to enhance consumer IoT security should be encouraged where possible.

Kindest regards,

Olivier MJ Crépin-Leblond
ISOC UK England Chair

Further resources:

- Useful Internet Society Resources on Consumer IoT Security
- The Online Trust Alliance IoT Trust Framework
- *IoT Security for Policymakers*

- *The Economics of the Security of Consumer-Grade IoT Products and Services*

- *The Canadian Multistakeholder Process: Enhancing IoT Security Final Outcomes and Recommendations Report*