The Institution of Engineering and Technology

Response to DCMS

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

Feedback on the regulatory approach and labelling scheme:

In summary, The IET support the need for legislation to provide consumers with a meaningful level of protection against cyber related loss (information theft, denial of service, compromise of privacy etc) as a modern day parallel to existing legislation protecting dangerous physical and electrical aspects of product design.

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

1.1 The IET agree that the Government should take powers to regulate the security of consumer IoT products. More consumer protection is required in this area. We feel the scope of the proposed regulation is broad enough and it should also apply equally to home network infrastructure equipment itself such as consumer routers and modems to which the IoT devices will be connected.

1.2 The proposed approach is for manufacturer self-assessment and labelling of devices which is acceptable, an independent approval scheme based on assessment of submitted evidence would be more robust but rather impractical at scale.

1.3 However we think the proposed measures are sufficiently technically proscriptive to ensure manufacturers adopt best practice.

1.4 It is possible to achieve a proscriptive requirement whilst also ensuring flexibility for the manufacturer in how they implement the requirements. Examples might be:

1.4.1 Secure all user interface and device to server communication with TLS encryption minimum 2048-Bit RSA or 224-Bit ECDSA certificate keys.

1.4.2 Be designed for 'plug and play' using standard defined network ports, e.g. TCP 443 for HTTPS communication.

1.4.3 All communication to internet servers to be "push" initiated by the device and maintained through "keep alives", not to require opening of inbound consumer firewall ports or port forwarding.

1.4.4 Must provide a clear description of all device interactions, their purpose, and an overview of the data stored in any cloud platforms.

1.5 More understanding and classification will be needed before any new regulation is proposed. It is unclear who will implement these at this time.

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

2.1 The provision on device factory reset would require careful management. It must be possible for a user to easily factory reset the device as a troubleshooting measure. Allowing devices to ship in a default "provisioning" state which requires setting of a strong unique password during initial setup by the user before any features are activated would be an acceptable compromise, factory reset would then revert to this provisioning state and disable all device features until re-configured.

2.2 On vulnerability management, the proposals do not go far enough, although providing a public point of contact would be welcomed, a requirement for proactive notification would be preferable. An effective measure would be to require manufacturers to maintain registration for all IoT devices unless users clearly opt-out and then directly notify users of vulnerabilities affecting their devices.

2.3 The minimum supported lifetime for security updates would be a positive development but we don't think the proposals go far enough. For IoT devices linked to an OEM managed cloud service an effective stance would be to require the manufacturer to continue to provide security related updates for as long as their service continues to operate and supports connections from the device in question.

2.4 It is also worth thinking about the environmental grounds because the proposed top three security provisions will prevent any form of legitimate sale/transfer or reuse by another user if there is no easy way to restore products to a factory state and known password.

2.5 The consequence is likely to be large volumes of product sent to landfill rather than repurposed by another user. Whilst manufacturers may prefer this to exploit built-in obsolescence to sell more product, it doesn't serve the best interests of consumers or the planet.

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.

3.1 Yes, we agree with the use of the security label. The label might be beneficial to consumers in making an informed choice but becomes somewhat redundant if legislation would require retailers to only sell compliant products.

3.2 The security requirements framework itself is the key component then. If legislation is put in place consumers would rightly expect products they purchase through genuine market retailers to be compliant without requiring a label.

3.3 There is perhaps a risk of the label providing a false confidence in a product by being misapplied by unscrupulous oversees manufacturers of poor-quality devices, much in the same way as has been seen for some time with the "CE" marking and other marks.

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.

4.1 The labelling seems suitable and would seem to be understandable to the average consumer.

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.

5.1 The retailer must also have a responsibility for the products they sell along the same lines as the current consumer rights act.

5.2 Mandatory requirements on what evidence / documentation manufacturers must make available to retailers and what validation retailers must undertake before selling IoT products to ensure compliance might be more effective and would ensure retailers have fulfilled their obligations for due diligence.

5.3 This must be carefully managed, as is seen with consumer rights cases for product defects retailers all too often try to redirect customers to a manufacturer despite their obligations under the legislation, there is a risk a similar situation here.

5.4 There must be effective channel for consumers to seek assistance where the retailer attempts to avoid their responsibility.

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.

6.1 No response

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.

7.1 Existing consumer IoT products that are on the market and their manufacturers should be granted a grace period to update their products to be in line with the new proposals.

7.2 The duration should be determined by the regulatory body and manufacturers effected.

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

8.1 The additional costs of implementing this regulatory approach within the secondary market may well be passed on to the consumer.

8.2 If the implementation largely ensures security and safe use of products then this may well be justified.

8.3 Government should give thought to the effect of the market following implementation.

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.

9.1 Small and micro businesses in the UK should be able to meet the proposals at a minimal cost if there is an adequate phased timeframe.

9.2 Consideration should be given to overseas manufacturers that ship products direct to the consumer and how this may affect these small and micro businesses that are, if they do not align to these regulatory proposals.

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.

10.1 OfCom seem to be best placed as the UK agency to undertake enforcement as they currently look after communication services. However, they do currently have a broad remit.

10.2 As per Q5, retailers could play a supporting role, have the most market power to demand and ensure that manufacturers provide products with robust security.

10.3 As with any product or service the party responsible for the point of sale and provision to the customer must bear the ultimate professional responsibility for the quality and suitability of the product for its intended purpose.

10.3 Whilst the legislation must place mandatory requirements on the manufacturer for the quality of their products and services, the responsibility and requirement for the sale should fall to the entity acting as the retailer, this may still be the manufacturer in some cases. The retailer would then be responsible for reflecting this requirement in their contractual agreements and procurement language with suppliers to provide a legal route to address failings in products supplied to them.

10.4 We think this framework placing responsibility largely on the retailer for due diligence would provide the best protection to the consumer and alleviate the capacity on Ofcom as there is more likely to be a UK based entity at the end of the supply chain on which enforcement can be undertaken, otherwise non-domestic manufacturers might evade the requirements.

10.5 For example, this is not uncommon with European manufacturers providing business computing equipment to UK markets which is not compliant with the Plugs and Sockets Safety regulations.

Further Feedback:

11. Please provide any additional comments on the consultation stage impact assessment, the regulatory options set out and the proposed labelling scheme.

11.1 The IET are ready to support the consultation stage impact assessment. With a membership of 167,000 members globally (115,000 in the UK), we are able to send communications to engineers and technicians who work in this space and provide expertise from our expert thought leadership panels if needed.

11.2 The Minister Margot James launched this consultation at our IOT Conference at Savoy Place London and is familiar with our activity.