techUK response to Department for Digital, Culture, Media & Sport

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

10 St Bride Street
London
EC4A 4AD
T 020 7331 2000
F 020 7331 2040
www.techuk.org

Contact: Tom Henderson | Programme Manager IoT
E: Tom.Henderson@techuk.org

Contact: Dan Patefield | Programme Manager, Cyber and Defence
E: Dan.Patefield@techUK.org
About techUK

techUK represents the companies and technologies that are defining today the world that we will live in tomorrow. The tech industry is creating jobs and growth across the UK. Over 900 companies are members of techUK. Collectively they employ more than 700,000 people, about half of all tech sector jobs in the UK. These companies range from leading FTSE 100 companies to new innovative start-ups. The majority of our members are small and medium sized businesses.

Introduction

techUK welcomes the opportunity to respond to the consultation carried out by the Department for Digital, Culture, Media and Sport (DCMS) on the regulatory proposals for consumer Internet of Things (IoT) cybersecurity. This follows the Government’s voluntary Secure by Design Code of Practice for consumer IoT security launched last year, which techUK had worked quite closely with DCMS in developing.

The Code advocates for stronger cyber security measures to be built into smart products right from the design stage and we are pleased that the security requirements outlined in this consultation are consistent with last year’s Code of Practice, as well as key industry standards that already exist for consumer IoT. techUK sees this an important step in helping to stamp out poor security practices in the sector, which can act as a significant barrier on the take-up of consumer IoT devices.¹

The principles behind this consultation therefore have the potential to positively impact the security of devices made across the world and we are pleased to see the Government work with international partners to ensure a consistent international approach to IoT security. Indeed it is vital that these proposals ensure harmony with other EU markets, supporting UK business rather than adding complexity in terms of standards or customer communication. Following engagement with techUK members we have developed this response which outlines our thoughts on the approach DCMS should take, including relaying some concerns from our members around the current regulatory approach and labelling scheme proposals. These are outlined in detail throughout the document and techUK would welcome any further engagement with DCMS going forward.

Response

Consultation Questions: Feedback on regulatory approach and labelling scheme

Regulatory Approach

¹ In techUK’s 2018 State of the Connected Home report, 16% of respondents stated that poor security was a significant barrier to them adopting a consumer IoT device
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 requirement for consumer IoT products?

To a certain extent, we agree that government should take powers to promote the importance of the security of consumer IoT products, particularly as it is not at all clear that market forces will entirely pay for improvements to IoT security. Indeed, we agree that it is a good thing to encourage industry to take cyber security risks seriously and there is a great deal of interest from the UK tech industry in finding a solution that makes consumer IoT products more trustworthy. Our members understand that enhanced security leads to greater confidence in the IoT ecosystem and recognise the importance of protected consumer interests, acknowledging that consumers are generally not able to assess IoT cyber security risks themselves, regardless of whether a device is secure or not.

Moreover, we believe that enhancing the level of confidence that consumers can place in the security of IoT products could have positive economic implications, increasing sale revenues to the benefit of our members. However, our support for the regulatory proposals and legislative approach contained in the consultation is limited due to several reasons.

Firstly, the definition of consumer IoT products should be more tightly defined as the definition in the consultation states that it covers any product that is “connected to the internet and/or home network and associated services”. This seems overly broad and could do with tightening in order to provide industry with greater clarity for assessing future regulatory proposals, with a recognition that different aspects of consumer IoT devices entail entirely different cyber security vulnerabilities and risks. Indeed, some members have suggested that the definitions need to be refocused on product characteristics and associated risks, rather than a blanket application to products themselves. More clarity around these issues will be essential during the implementation process.

Secondly, many of our members in the retail space feel that the consultation document puts too much of an emphasis on the role that retailers can play, with some doubting that retailers will be able to efficiently leverage the security objectives of the government. According to the consultation document, retailers would need to ensure that IoT products are compliant based on either manufacturers’ self-declaration or through the use of a label. However, in addition to the very significant cost of implementation that this would require, it is unclear how government expects retailers to themselves verify whether the features provided with in the IoT products meet specific security requirements. Furthermore, for the online retailers operating outside of the UK, the proposals will create different regulatory security regimes for different regions – creating significant implementation issues, especially since many online retail platforms provide a gateway to a global customer base for start-ups and SMEs. For platforms that are merely facilitating a sale, liability will be hard to implement.

We would urge that the Government works in collaboration with international partners to help inform and create a global approach, otherwise the proposals risk adding new burdens to UK-based, international actors who already have high levels of compliance.

Thirdly, the consultation document should openly recognise that some of the products covered by the proposed regulation are already regulated to a degree. For example, the processing of personal data generated from the use of such products must be done in compliance with the General Data Protection Regulation (GDPR) and other data protection laws. Furthermore, there are already existing regulatory mechanisms that relate to IoT and that provide international
harmonisation such as the Radio Equipment Directive (RED) which is already transposed into UK statute.

Lastly, many members have expressed disappointment in the timing allocated to respond to this consultation and the subsequent legislative timetable outlined. In particular, more time should be made available for industry to review the proposals, make the necessary arrangements to attain the granular economic evidence in line with the government’s requests and work with government to identify what appropriate measures should be in place for industry to self-declare compliance in an easy and adaptable format depending on the needs of each company. This timeline is particularly taxing given that the voluntary scheme which industry were engaging with has not been in operation long enough to ascertain its effectiveness. As such, techUK would suggest that this consultation be considered an initial one, with coordinated engagement thereafter giving industry sufficient time to conduct and coordinate the relevant activities internally.

Saying that, our members are broadly supportive of an approach that prioritises the top three security guidelines, contained in last year’s Code of Practice, as a measure of defining what good, baseline security looks like. In comparison to the other ten guidelines in the Code, the top three are easier to test compliance against and would prevent a large number of cyber-attacks.

Of the three guidelines, however, the requirement that “manufacturers explicitly state the minimum length of time for which (a) product will receive security updates” is the most contentious. IoT products are, by design, connected to the internet and generally updated with the latest security updates once they are put in use. In other words, an IoT product can be sold without embedded updated security features that are downloaded as soon as the IoT product is connected to the relevant App/Internet website.

Furthermore, due to supply chain issues, some companies may not be able to accurately ascertain at the point of design the length of time a product would receive security updates. Given that support dates may be extended, it would be difficult for the manufacturer to update the packaging of a product that is already part of the product inventory of an online retailer.

One alternative could be for the wording to be changed to “manufacturers explicitly stating a minimum security support period for a product” or, as some members have argued, for the timescale to be removed entirely in favour of a commitment to providing a “security update policy”. It is important that manufacturers are able to decide themselves how they will provide a device with security updates rather than focusing solely on a perceived “end of life” date. This can also create an incentive for companies to differentiate themselves from competitors through a meaningful and robust approach to security.

It should also be noted that some of our members dispute the idea that the top three guidelines, as currently drafted, can easily be implemented by IoT manufacturers and would provide enough of a benefit to consumers. Many feel that the guidelines will need to evolve over time, which could make a “static” label confusing and ineffective.

For example, the guideline on passwords may not be needed in the near future due to changes in the way in which devices authenticate, with many providers creating alternatives to passwords. Already, industry is seeing many cloud connected products rely on certificate-based authentication instead of passwords. As such, some members have suggested that Government works closely with organisations like techUK to define and maintain this guideline practically on a rolling basis.

Finally, some members have expressed concerns around the lack of a clear link between the three mandated guidelines and the wider IoT security landscape, including the other ten principles used in the Code of Practice. By focusing on the three top guidelines, and failing to mention the others entirely, there is a risk that consumers will believe that they are sufficiently protected simply if a product meets the three guidelines. Though it should be noted that elements of the other ten
principles require further clarification and amendments, it is important for government to continue referencing the wider code in its education and awareness campaign to consumers.

**Labelling Scheme**

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.**

TechUK members understand the need to educate consumers on the security of individual IoT products, as many consumers do not have the technical expertise to differentiate between good and bad security. However, many members have expressed concern at the labelling scheme contained within the consultation due to the practicalities of implementing such a label and the associated costs for manufacturers.

It is stated that the proposed label would currently be printed on the packaging of any consumer IoT product and online. IoT consumer devices include a vastly diverse range of products, of different functions, sizes and prices. The associated costs placed upon industry to accommodate the label could be significant and members have expressed concern that the effects on consumer behaviour may be minimal as it is debatable whether consumers would be discouraged from buying a product with poor security simply because of a label.

Due to the short consultation period, it is hard to gather empirical evidence on this. On the contrary, it may take a high-profile security scare, breach or scandal to change consumption habits associated with popular products. Additionally, without enough publicity, the labelling system proposals may not fully enable consumers to identify and place value in the security of IoT products – therefore if the labelling scheme is pursued then we would strongly support efforts for a Government sponsored marketing scheme.

Furthermore, in the modern retail environment, consumers increasingly purchase goods without seeing the packaging labels until after the point of sale. In addition, product packaging and labelling are usually discarded following a purchase, which under the proposals in the consultation will leave consumers without a reliable way to verify and prove how they are entitled to security updates. This somewhat undermines the case for a physical label and supports the notion that there may be other options available that would be at least equally effective.

For example, some members have suggested the sole use of an online label that would allow organisations to highlight good practice, whilst not being as burdensome on manufacturers. This would avoid complexity for organisations trading in different jurisdictions by removing the need for multiple types of packaging (often on very small products with limited space) whilst also allowing companies to easily trade under different regimes without incurring too many extra costs.

Some members have also suggested that Government engages with previous research into e-labelling commissioned by Digital Europe and the Mobile Wireless Forum - “Research into e-labelling schemes outside the EU.”

On the design of the label itself, the majority of techUK members have expressed concerns on the requirement to state on the label an estimated date for security updates and on the potential use of the negative label. Through doing so, it could be seen to imply that the date reflects the
product’s “end of life”, much like a sell-by-date does, or suggest that a product is “insecure” as soon as the date expires, which is not the case. Most IoT products will not become defunct at the point of security updates not being available and could in fact be perfectly secure for many years following. IoT products consist of numerous components from different suppliers, over which the manufacturer does not have influence, such as the operating platform. The simplicity of stating a date or support period therefore does not take into consideration the different needs of different products or that the same product could have different software updates and timelines depending on when they are made.

Furthermore, it is not sufficiently clear how such support would be monitored. Tracking this information for several products of an inventory will be a challenge for both manufacturers and retailers and there is a risk that the date until when the updates will be available might expire before the products are sold.

In addition, if a manufacturer or third-party provider were to go out of business, what would the status of its products be? The purpose of ‘secure by design’ is in part to build and foster trust in IoT products, but this approach to the label could end up accidentally threatening and undermining consumer trust in particular products that are perfectly workable and secure.

Forcing companies to create new labelling requirements will only go so far if consumers are not aware of them or do not have the understanding or knowledge. The Government should work with consumer groups and civil society to look at the best ways to increase customer awareness around product security measures. This should be done before any new labelling requirements are implemented.

Of the different options to mandate either retailers or manufacturers, though some members have expressed strong support for ‘Option A’ due to the reasons discussed above in relation to concerns around the potential labels, more techUK members have viewed ‘Option B’ as the least problematic approach. This would still mandate retailers to only sell consumer IoT products that adhere to the top three guidelines, thus improving consumer IoT security.

Others, however, are not in favour of putting responsibility on retailers at all as such an approach would not be able to check the accuracy of the manufacturer’s security verification in the context of the self-asserted label. Self-declaration does not guarantee that the IoT products are safe and the guidelines can be interpreted and implemented differently. Any weakness on a labelled IoT product would automatically undermine the value of the label.

One suggested approach could be for companies to self-certify as a whole, pledging that all future IoT products produced will adhere to the three security guidelines, rather than self-certifying product by product. This would, in particular, reduce the burden for companies that sell multiple IoT products and give consumers confidence in using brands that take a holistic approach to security.

Impact of 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.
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.

techUK members, rather than techUK itself, are much better placed to individually provide the relevant evidence and statistics in order to effectively answer this question. However, a significant number of techUK members have expressed concerns around the timeframes laid out in this consultation. Five weeks is not sufficient time for industry to put together the useful, exhaustive evidence base which DCMS is looking for. techUK would strongly urge DCMS to extend the period by which this evidence can be offered.

Particularly for large international organisations, bringing together the people and data sets responsible for this information can be a time-consuming, complex process, therefore a function should be set up in order for DCMS to continue receiving this information after the official consultation has concluded. Indeed, this underlines the multitude of costs that there are to industry in implementing some of these measures, as some members have incurred costs in bringing together staff and resources across wide supply chains in order to merely estimate the effects that the proposals will have on them.

**Enforcement**

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.
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.

techUK welcomes DCMS’ intentions to implement a ‘grace period’ which will allow manufacturers and retailers alike to transition into a new regulatory regime. However, the significant impact that these proposals would have on existing non-labelled consumer IoT stock is further evidence of why a labelling approach may not work in practice. There is a very real scenario that legacy products that have not been labelled become wasted stock, sitting in warehouses after the grace period has ended - even if they do comply with the top three security requirements. There may also be the unintended consequence of the regulation forcing retailers to sell supposedly “unsecure” products in flash sales before the regulation is enforced. It is clear that if government does pursue a labelling approach, it will need to carefully manage how messages are communicated to consumers during the grace period as some unlabelled products may instantly be seen as insecure when they are not.

With the above in mind, techUK calls on government to provide a longer grace period. One suggestion could be for companies to self-certify as a whole through a voluntary scheme that would run for two to three years, with legislation coming afterwards. This will give industry time to provide better evidence relating to how the scheme has affected consumer behaviour, would allow for the completion of existing long-term contracts in the supply chain and also give retailers enough time to sell existing, non-labelled stock without being penalised by the legislation.

On costs associated for retailers, techUK members will submit individual first-hand evidence which will be of more use to DCMS than anecdotal evidence. Nevertheless, we firmly believe that any scenario by which existing stock were arbitrarily removed from shelves would be unnecessary and particularly costly for SMEs. techUK urges DCMS to ensure that its proposals do not stifle competition and innovation, dissuading new entrants who do not have the resources to easily modify approaches in the UK alone. techUK would be keen to help DCMS engage with SMEs in this regard and look more closely at potential challenges unique to them.

techUK does not have a strong opinion on who would be best placed to undertake enforcement of this process. However, it is clear that any organisation taking on these responsibilities should be given sufficient time and resources to effectively prepare for implementation. They need to have time to build up a sufficient skill set to understand and enforce the complexity of IoT security and to also have the right internal infrastructure set up to deal before it is established as the enforcer. As with other regulatory changes, this should include a period of intensive engagement with industry, creating a two-way dialogue and ensuring a smooth transition as we enter the new framework.