AMDEA™
The Association of Manufacturers of Domestic Appliances

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

AMDEA response - due 5 June 2019

By email to: securebydesign@culture.gov.uk

Consultation questions: feedback on regulatory approach and labelling scheme

AMDEA is the UK trade association for manufacturers of domestic appliances, from large white goods through vacuum cleaners to the vast range of small appliances on the market. Our 36 members represent over 80% of the UK domestic appliance market, rising to 95% for large white goods.

As a trade body, AMDEA is not able to address commercial matters or commit individual companies to participating in voluntary schemes.

We lament the extremely short timescale for response to this consultation, especially in the light of its insistence on the provision of evidence. However, we have consulted our members; encouraged them to respond individually; and can comment as follows.

We would be very happy to discuss any of the issues in more detail.

Summary

AMDEA does agree that cybersecurity is becoming ever-more important for domestic appliances, both with regard to products that are enabled for consumers to control remotely (whether they choose to use this function or not), e.g. by apps on smart phones, as well as products that offer demand-side response to signals initiated by energy utilities.

AMDEA does not agree that the UK should consider introducing primary legislation before the UK has actually left the EU. A new EU Cybersecurity Act has recently been approved and we would hope that DCMS is fully cognisant of the impact that this will have on products supplied to the European market.

AMDEA does not agree that there should be a requirement, whether mandatory or voluntary, to affix any kind of marking to a product. AMDEA members may be willing to provide the "positive" information proposed by DCMS on their UK-facing websites and supply this information to UK retailers:

however, this is a commercial matter for each member organisation. Our members see no logic in proposing the display of “negative” information.

In terms of a voluntary scheme, some AMDEA members may be prepared to join such a scheme under certain conditions, to be agreed with government. In this regard, they would wish the following to be taken into account:

1) Any such voluntary scheme would need to be compatible with the current and forthcoming EU cybersecurity legislation.

2) Any such scheme must not require manufacturers to affix a marking on their products. Information should be provided to consumers via the manufacturer’s own UK-facing web site (where available) and manufacturers could be required to make this information available to UK based retailers.

In general, AMDEA members do not favour government’s preferred Option 1 but might be in favour of an approach based on Option 2.

The rational for these answers is given in either the introductory section below or in answers to specific questions.

Introduction

a) Introducing UK legislation

AMDEA notes that the UK is not alone in recognising the need for cybersecurity. In particular, the EU has a number of legislative measures either in force, soon to come into force, or already under discussion. Currently the UK is still part of the EU, and we would not wish to see any divergence between the UK regulatory framework and that existing in the rest of the EU. We understand the UK Government wanting to plan its cybersecurity strategy in case we do leave the EU without a new trade deal, but we certainly would not wish any new UK-specific measures to come into force before the date of exit. Indeed, given the very large cross-border trade in domestic appliances between the UK and the EU, we would also not wish any future UK legislation to be significantly different to that which applies in the EU.

b) Introducing a physical label to be affixed to products

A key feature of this proposal is the introduction of a labelling scheme. It may be thought that labels are inexpensive and are useful for consumers. AMDEA certainly does not agree with the first proposition and has grave doubts concerning the second contention. We would also comment, in passing, that it would add to the volume of packaging waste, as mentioned in our response to Defra’s recent consultation on reforming the UK packaging producer responsibility system.

Products placed on the UK market are usually the same as those placed on the continental European market and are invariably identical to those placed on the EU market in Ireland. This is because the mains voltage and frequency across the UK and EU is the same, with only a variation in mains plug and possibly a variation in user instructions to cope with language variations – but

even those differences are not present between the UK and Ireland. We trust that it is understood that a UK-specific label would require manufacturers to create special control procedures, in addition to the marking itself, to separate UK products from those supplied to the EU, and then keep them separated. Such activities do not come at a low cost.

The energy labelling introduced decades ago to inform consumers about the energy usage of products has been a great success, but it is essentially a communication tool made available at the point of sale.

There are product markings for safety, defined by safety standards, to inform users of precautions to be taken, but other markings are typically not intended for consumers (including the CE marking). Unless the meaning of a marking is clearly and repeatedly explained, consumers will not understand what it means and the greater the number of markings the greater will be the level of confusion by consumers.

In fact, the marking introduced with the Terminal Equipment Directive (91/263/EEC) to indicate that the product was suitable for connection to the public telecommunications network was poorly understood by consumers and was abandoned when this Directive was replaced in 1999.

In short, AMDEA does not see any benefit in introducing a labelling requirement for products but does see multiple reasons for not doing so.

c) Retailer obligations

All three government options “mandate retailers to only sell consumer IoT products” that meet specific criteria. However, the consultation does not define what DCMS means by the term retailer. We presume that this term is intended to encompass both “bricks and mortar” companies and distance sellers but does it also include on-line marketplaces?

In any case, a customer in the UK could easily place an order for a product sold by a distance seller in another EU Member State. We fail to see how the UK could enforce UK requirements on such ‘remote’ distance sellers and, since they could well be supplying locally sourced products, they would not carry the proposed UK marking (which AMDEA considers impractical in any case).

d) Enforcing any scheme, whether voluntary or mandatory

Clearly, if a scheme is to win the trust of consumers, it must be enforced effectively.

Equally, if the Government wishes to protect manufacturers and retailers that are complying with any voluntary or mandatory provision from those who are not concerned with compliance, then the measures must be enforced appropriately.

However, the consultation does not provide any clear indication as to which body would undertake this enforcement. This is a matter for the Government to propose, first and foremost, within any new legislative provision concerning a

mandatory provision. Even a voluntary scheme would require some degree of enforcement by some organisation or other if it is not to quickly be discredited by parties that sign up to a scheme without any intention of being bound by it.

e) Agreement with the 'top three' guidelines of the Code of Practice:

AMDEA considers this to be a matter for individual members, since each company has their own commercial considerations and practices to consider. However, we would make the following remarks:

i) The consultation asks for all IoT device passwords to be unique and not be resettable to any universal factory default value. But actually, this is not in line with the ETSI TS, which does not explicitly require the use of passwords as the only way of setting up a secure communications path. Indeed, other means of providing secure communications may be just as secure but may not require a human being to input characters into a keyboard or the like. Therefore, any subsequent legislation should only describe the required outcome; it should not specify the means by which that outcome must be achieved (this could be demonstrated by compliance with an appropriate standard).

ii) In point 2, our members would like greater clarity concerning what would constitute a public point of contact – would there have to be a separate e-mail/telephone number etc. for reporting cybersecurity issues?

iii) Similarly, it is not clear what is meant by "security update" in point 3. For instance, there will typically be at least two layers of software that could have security implications. Usually, this can be broken down into the operating system chosen by the manufacturer and an application layer on top of that operating system. The operating system is unlikely to be under the control of the appliance manufacturer and so they would not be in a position to provide an end-date for that part of their product. In addition, there could also be vulnerabilities within the firmware associated with the microprocessors and other hardware used to provide the functional control within the product and communication interface (e.g. Wi-Fi provided by an integrated RF module) – again, these devices and their associated software/firmware are typically provided by third parties: how long firmware updates will be available is therefore often not under the control of the appliance manufacturer. In any case, the requirement for a software updates policy, without a specified time period, is a sufficient requirement. It is important that the manufacturer be able to decide how they will provide a device with security updates rather than focusing solely on a perceived "end of life" date or even a support period. This creates an incentive for companies to differentiate themselves from their competitors. We believe that it is the ability to update software that is the information that the consumer needs and an individual company's approach to this should be publicly available to the consumer.

There may also be a considerable time lag between the product being supplied and it being sold to a consumer, meaning that any original time limit would be diminished for the end user.

A further consideration on this “guideline” is how it will be enforced, since stating a date into the future is one thing but being held to account if that date is not honoured is another.

Further clarity is required on this point.

Questions

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?

As stated in our introduction, AMDEA does not agree that the UK should introduce regulatory measures while we are still members of the EU. Indeed, we suspect that to do so would result in the UK breaching its Treaty obligations.

We do agree that there is an important role for the UK Government, and other governments, to play in helping to encourage the development of standards and understanding of cybersecurity. However, our view is that industry is best placed to keep abreast of this fast-moving area of technology and so it is for them to drive improvements. Governments should provide a broad framework to protect consumers and provide an even playing field for manufacturers.

Given that over 80% of the large white goods sold in the EU are manufactured in Europe, this is a key consideration. We would also point out that for certain categories of large white good there is no, or very little, UK manufacture, so the Government would be attempting to impose additional requirements on imports, something that would make new trade deals more difficult to negotiate after Brexit.

Even if the UK fails to agree a future trading relationship with the EU there would seem to be no valid reason why the UK would not want to align with the rest of this continent on consumer protection issues.

We would have no objection to a requirement to self-declare compliance, as long as there was adequate market surveillance to ensure that compliant manufacturers are not disadvantaged by having to compete with non-compliant suppliers ignoring the legislation with impunity.

In respect of proposing requirements on retailers, the Government needs to address the fact that customers are turning more and more to distance sellers, particularly those that are internet based. In the current marketplace a customer in the UK could easily place an order for a product sold by a distance seller in another EU Member State. We do not see how the UK could ensure that such products would carry the proposed UK marking.

But in any case, we cannot agree that yet another label for products that may already in some cases be too small to display existing ones, would be either sensible or indeed effective.

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?

As explained in our introduction, it is by no means certain that all three of these would be relevant to all the domestic appliances currently on the market. Some of our members are already embracing advances in AI and other cyber technology in their products while others are still only just beginning. If these are the baseline requirements some of our members would not necessarily be able to declare compliance, even though they do take the cybersecurity of their products extremely seriously.

However, developing international standards will ensure that in future all such products will have to exceed these requirements so any UK-scheme based on these criteria would be short-lived. There may therefore be little incentive for many manufacturers to engage.

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.

No. A physical label is impractical, expensive and will have minimal impact on consumer awareness, even if the Government were to run a major consumer information campaign. We are aware of a number of other product labelling schemes being proposed by other government departments and our response to them is the same.

There is already a plethora of markings required for products. While adding yet more to large appliances is logistically possible, this is not the case for smaller items which would not have room for a physical label. We could support the use of a symbol on-line as a declaration of conformity, providing that the terms of use were well-defined, and the correct usage enforced.

There is an additional cost for compliant companies, whether or not facing unfair competition from non-compliant suppliers, a cost that will be passed on to consumers. We understand that your survey suggested that consumers were willing to pay this premium as, when asked, they often express willingness to pay more for energy saving, higher taxes to fund the NHS etc. Experience suggests that this willingness does not translate to actual purchasing decisions – our survey for International Product Safety Week in 2018 found that over a quarter[1] of consumers were willing to buy on-line a

[1] YouGov Plc. Total sample size was 2072 adults. Fieldwork was undertaken between 17-18 October 2018. The survey was carried out online. The figures have been weighted and are representative of all GB adults (aged 18+). 26% said they were fairly likely and 3% very likely to buy from a seller they did not know if their product was the cheapest.

brand they had never heard of because that particular product was the cheapest on offer.

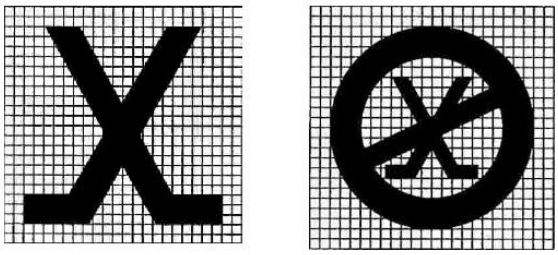
We see no logic in proposing a negative marking - the product is either compliant with a label or non-compliant without – a negative label would be an odd thing for any manufacturer to adopt.

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.

   No. We do not agree with the principle of having a label at all. If the Government wants to impose requirements for declarations of minimum cybersecurity measures that should be via an on-line declaration and in the instruction booklet. It could be possible to use the proposed symbol or similar, subject to a public information campaign to ensure that it was understood by retailers and consumers.

   We previously mentioned the marking introduced for the original Terminal Equipment Directive (a symbol to indicate suitability for connection to the public telecommunications network) which was no longer included after its first revision because it was agreed that it was poorly understood by consumers. It too had a “positive” and “negative” version:



   The legislation also required the last two digits of the year in which the CE marking was affixed and a star symbol to indicate the energy performance. The UK equivalent legislation was http://www.legislation.gov.uk/uksi/1992/2423/schedule/3/made.

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.

   No. We do not agree with the principle of having a label at all. We are also unsure how retailers could refuse to sell unlabelled products or why any manufacturer would affix/use the negative version.

   We are sure that the Government recognises that some companies have procedures in place to ensure compliance with legislation and reputable manufacturers want protection from those that do not.

In terms of a declared commitment to meet certain (revised) criteria, that could be imposed as a requirement on retailers, who would then require it of their suppliers There remains the issue of how effectively such a requirement, voluntary or mandatory, could be enforced.

And, as previously stated, there are evolving international standards and legislation that will impose basic requirements on the future design of such products anyway. International harmonisation must be a priority to ensure that there is no unnecessary burden placed on businesses, since the vast majority of companies will not supply consumer goods only in the UK.

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 cybersecurity 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.

It is our experience that impact assessments cannot accurately predict associated costs as they are based on attempting to foretell the future. For instance, g) could only assess what is available at this point in time. As well as the cost of creating and supplying a physical label, there are training costs to ensure that retailers' staff can explain the labelling and performance to consumers. Not to mention the need for adequate market surveillance and enforcement.

In respect of the other points:

a) Although all the proposals are based on manufacturers supplying labels and retailers checking if such labels have been affixed, we were unable to see where in the impact assessment these costs have been estimated. Furthermore, options other than affixing physical labels onto products (such as providing information at the point of sale) were not assessed. Therefore, we consider that the impact assessment is significantly lacking in these key areas.

b) The impact on competition has two aspects: the impact on those manufacturers currently supplying the UK market of an additional requirement for UK-destined products only; and the additional costs of compliance where poor enforcement means that those extra costs put compliant manufacturers at a commercial disadvantage.

c) e) f) h) i) j) k) m) AMDEA cannot comment on costs. Individual members may be able to supply estimates.

Our sector operates at a global level and any specific requirements for the UK market are a barrier to trade. They may not be a technical barrier challengeable by other EU Members States or WTO members, but they are an additional burden, and therefore cost, for those manufacturers supplying the UK market. Such costs will affect the price of the product to the consumer and/or the profitability of that product. Where the additional burden/costs deter some suppliers from the UK market, there will be less choice for consumers (and more innovative products will be marketed elsewhere first) which will also put upward pressure on prices. Without effective market surveillance non-compliant product will still be available and will inevitably be cheaper for the consumer to buy.

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.

New legislation cannot be applied retrospectively. Existing stock will clear the market in time. New requirements would have to be imposed for new products placed on the market after a certain date.

For any residual stock it would have to be explained that the new legislation did not mean that existing products were unsafe. As any implementation date drew nearer retailers would find it increasingly difficult to sell existing stock at full price. There needs to be more clarity on how the Government proposes to implement such legislation and how it intends to communicate it.

Since there is often a considerable gap between a product being placed on the market and the consumer's purchase of it, an on-line declaration could be revised, if required, in a way that a physical label could not.

And, with a virtual declaration there seems to be no reason why a manufacturer could not subsequently declare compliance for products made available prior to the introduction of the requirement.

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

We cannot comment on estimated costs. Our members may choose to do so in any individual response to this consultation.

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.

See reply to Q8. However, all additional legislative requirements are more burdensome for micro businesses as they are unable to absorb costs as readily as larger companies.

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.

This is a matter for DCMS to consider before proposing new legislative or "voluntary" requirements.

The Radio Equipment Regulations 2017 are enforced by Trading Standards and Ofcom. However, the Office for Product Safety and Standards currently incorporates the market surveillance agency formerly known as NMRO which deals with compliance with Ecodesign and Energy Labelling among other things. They would seem to be the most appropriate body to deal with enforcement of cybersecurity for connected products. You may also wish to

consider the findings of their ongoing project looking at the potential fire safety risks posed by connected appliances vulnerable to cyber-attack.

Radio equipment compliance with e.g. ETSI standards is normally the purview of Ofcom but we do not consider that such a division of labour is advisable - for our members' products the greatest threat of a cybersecurity breach is that the safe functioning of that product could be compromised.

In terms of penalties there could no doubt be proposals for civil sanctions to include hefty fines in addition to possible criminal prosecutions. However, it is not clear where the resources for such enforcement activity would be found as, in our view, UK market surveillance is currently poorly resourced and under-funded.

In conclusion:

Cybersecurity is a rapidly developing area of concern for legislators and standards makers around the world. It is not a UK-specific issue.

Brexit could potentially have a major impact on the availability of goods imported to the UK. And while the majority of domestic appliances sold in the UK are imported, we do have a number of members who export such products to the EU and the rest of the world who would also not want to have to differentiate their UK-destined product from the rest.

Consumers are already faced with multiple product markings and labels that they do not necessarily even notice.

We appreciate the efforts that DCMS are making to promote cybersecurity for consumer products, but we urge them to consider these in the light of other work on these issues being undertaken at a wider level. Any measures, even voluntary ones, should be compatible with the NIS Directive, the incoming Cybersecurity Act and other EU legislation.

Sian Lewis

Acting Chief Executive