Response to DCMS

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

On behalf of the UK Computing Research Committee, UKCRC.

Prepared by: Professor Chris Johnson,
School of Computing Science, University of Glasgow, Glasgow, G12 8RZ.
http://www.dcs.gla.ac.uk/~johnson

The UK CRC is an Expert Panel of all three UK Professional Bodies in Computing: the British Computer Society (BCS), the Institution of Engineering and Technology (IET), and the Council of Professors and Heads of Computing (CPHC). It was formed in November 2000 as a policy committee for computing research in the UK. Members of UKCRC are leading researchers who each have an established international reputation in computing. Our response thus covers UK research in computing, which is internationally strong and vigorous, and a major national asset. This response has been prepared after a widespread consultation amongst the membership of UKCRC and, as such, is an independent response on behalf of UKCRC and does not necessarily reflect the official opinion or position of the BCS or the IET.

Acknowledgement: particular thanks are due to Ann Blandford, David de Roure, Julie McCann, Martyn Thomas and Jeremey Watson in the compilation of this response.

Response

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?

   [1.1] Yes, the Government should take powers to regulate the security of consumer IoT products. We also agree with the broad approach although there remain significant questions about the implementation.

   [1.2] The definition of IoT devices raises significant concerns; "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". The proposed definition does not capture a large array of "smart" devices that are not directly connected to the Internet but that use alternate (e.g., Bluetooth) communications that may or may not interact with home networks. As a specific instance, a host of mobile devices including activity trackers and high-end headphones use short range Bluetooth communications to interact with Internet enabled devices through which data can be collected about user behaviour and through which firmware updates can be directly applied although the devices themselves are not

directly connected to the Internet using TCP/IP. Similar comments can be made about devices that exploit a plethora of alternate protocols including LoRa. These examples are likely to become more complex and more common through the development of edge devices for example exploiting ad hoc connections to 5G devices. Further work is, therefore, required to provide coherent and sustainable definitions.

[1.3] It is unclear what appeal mechanisms will be implemented or who will implement these regulations – potentially it could be Ofcom but they are not resourced to do this at present. There is a danger that these issues may compromise the wider objectives of the proposals especially as their implementation is likely to coincide with wider measures to reduce digital harm that could impose significant additional regulatory burdens on a small number of suitably qualified individuals.

[1.4] What happens in the case of a company that fails to meet the patching requirements – for example, by arguing that the device does not need to be updated or in more complex situations where the company ceases trading. The consumer would potentially still assume that their device was secure even though it was no longer being supported. Is there a need for a requirement that the consumer or regulator can determine the patch level of the device?

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?

[2.1] Yes, these provisions are appropriate but as in Question (1) they also lack an appropriate level of detail.

[2.2] Having an appropriate point of contact for security researchers is an important step forward but the onus should not only be on the manufacturers. Researchers should also abide by a code of ethical conduct that, for example, requires consultation with the NCSC before their findings are published.

[2.3] It is unclear how to enforce these requirements on the large number of overseas retailers and manufacturers who ship products either direct to consumers or through electronic market places.

[2.4] It should still be possible for researchers to buy devices that do not meet these requirements – in particular the named point of contact, from overseas sellers in order to have access to the latest technology.

[2.5] The guidelines should further require that IoT vendors provide a secure download channel for firmware upgrades; meeting requirements for hashing etc to be specified by the NCSC.

[2.6] There may be significant cost benefits to UK companies if any subsequent regulations remain compatible with EU Directive 2019/771, which says that goods

with digital components must have these components maintained for a reasonable expected lifetime, and a minimum of two years. This expands the scope beyond security updates; an approach that we would support in terms of meeting consumer expectations from new generations of programmable devices.

[2.7] Additional consideration might also be given to legacy devices and infrastructure. Consumer IoT devices are unlike other consumer products that we might buy off the shelf. They connect with other devices in order to work, and those other devices become weak links. There is a vast IT estate of legacy IT which they will interwork with. This limited guarantee also needs to be in the messaging somewhere.

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, the labels seem appropriate. However, there should also be protection against rival labelling systems that create confusion to consumers – as evidence, the recent studies into consumer confusion over the interpretation of the "Green Dot" recycling labelling provides strong insights into what can go wrong[1].

   [3.2] Additional provisions might consider the ease by which a patch could be applied? A device might earn the patching label but not deserve it in terms of the number of updates that are actually applied by the end-user. UK Universities have considerable expertise in assessing whether or not particular groups of users can perform these and related tasks.

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] This seems broadly appropriate although there might be a concern that the positive labels engender too much complacency on the part of consumers? The steps proposed here are necessary but not sufficient to provide long term consumer protection; especially given the many other legacy infrastructures that IoT devices depend upon.

   [4.2] How should consumers respond to devices that lack these labels? By parallel, the EC or FCC marks for electromagnetic compatibility are "invisible" to the majority of consumers. The number of people who would check for their presence when buying a product is close to zero; there is an assumption that these checks will be carried out by regulatory bodies.

[1] https://resource.co/article/citizens-confused-ambiguous-recycling-information-says-study

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] This seems appropriate – but with some consideration for the practicalities that arise when products are distributed in the UK for manufacturers who are based in other jurisdictions. In such cases, it seems appropriate that the re-seller could act as the point of contact for responsible disclosure with time limits by which a response should be received (see answer [2.2]). Most consumer IoT devices source components from the USA or China; without such considerations the proposals will be ineffective.

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.

[6.1] There is a concern that without adequate consideration of the practical issues raised in this response (e.g., indirect IoT connectivity of edge devices, third-party sales, ability of users to install patches, appropriate resourcing of regulatory bodies) that these proposals will be ignored and that the reputation of associated government agencies will be tarnished.

[6.2] The proposals seem to be silent on expectations for UK industry selling IoT devices in other markets. It would seem appropriate to expect that the three top guidelines be required for devices sold from the UK as well as devices being sold into the UK.

[6.3] Our response to [2.6] stressed the need to address not just security but also the wider aspects of longevity and product support. These are relevant in terms of any impact assessment considering that consumer IoT devices will already be covered by EU Directive 2019/771. Security and reliability both contributed to dependability . Many people now use IoT devices that have not been tested over durations greater than 6 months. The proposals might be more explicit about the interactions between security patches and wider upgrades that could introduce un-intended vulnerabilities with trade-offs between security and, say, performance.

[6.4] Associated with [6.3] is the "homebrew" and "jail-break" culture in which some consumers will choose to disable services on IoT devices. Any regulatory proposals should provide protection to the vendor in such circumstances – without impairing the ability of UK researchers to conduct legitimate studies into future technologies.

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] As with other similar legislation, there should be a period of grace within which existing stock should gradually be replaced by devices meeting the new requirements. The duration of this period should be determined in consultation between the regulatory agency and the companies affected.

[7.2] In any event, there will have to be the ability for retailers to relabel products that were not specifically designed for the UK market but that do meet the top three requirements.

[7.3] The issues extend beyond exiting IoT devices to the legacy components and infrastructures that consumers will continue to rely upon, this is raised in [2.7].

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

   [8.1] There are well justified concerns that the costs of both meeting the requirements and of funding the necessary regulatory supervision/appeal process will be passed to the UK consumer. These will only be justified if the public derive a corresponding degree of protection against emerging cyber threats to IoT devices. The recent NAO report into progress and cost-effectiveness of the National cyber security strategy stresses the need for government to derive appropriate metrics that evidence the utility of these and similar interventions in the market[2].

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 should be able to meet the main requirements of the proposals at minimum cost providing there is sufficient time to phase in compliance. However, unless the potential inequality described in response [2.3] is addressed then these UK companies may be at a considerable competitive disadvantage to overseas suppliers in terms of the range of devices that they can market in the UK.

   [9.2] The proposals are silent on the position of UK companies selling devices that do not meet the guidance into other markets, see [6.2].

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.

    [10.1] Ofcom seems well placed to be the default regulator for these proposals as the existing body responsible for communications services. However, they already have considerable and broad responsibilities covering both communications infrastructure and content, as described in their most recent annual report which sets out their priority for 2019-20 to enable "strong, secure networks: we will work with communications companies to help ensure their networks are strong, secure and protected against outages or cyberattacks" [3]. They are working to meet their significant new requirements under the NIS Directive. Ofcom potentially also face

[2] https://www.nao.org.uk/report/progress-of-the-2016-2021-national-cyber-security-programme/
[3] https://www.ofcom.org.uk/__data/assets/pdf_file/0020/141914/statement-ofcom-annual-plan-2019-20.pdf

new duties following, for instance, the DCMS consultation on digital harm. If they were to be identified as the regulator it seems appropriate to conduct a more systematic review of their responsibilities and their ability to meet a growing range of expectations from central government.

[10.2] As part of the regulatory review proposed in [10.1] some consideration should be given to the development of a national cyber regulator modelled on aspects of the HSE. Focussing technical expertise and working hand in hand with the NCSC, which should continue to be independent of specific regulatory responsibilities.

[10.3] Further questions can be raised beyond the role of the regulator and any associated enforcement actions. In particular, we would highlight concerns over the installation and maintenance of IoT devices. There is an increasing market for companies who specialise in the installation of particular types of consumer IoT devices – in particular, home security appliances and "smart doorbells". We can see this trend developing as devices and services become. Ore sophisticated and more integrated – with third-party companies offering to install and maintain mesh IoT networks. These companies are not considered within the proposals. Who do people call when their Consumer IoT fails? How will Consumer IoT product recalls be handled? We can expect the proposed intervention to prompt the ecosystem to adapt. Associated issues for consideration include the future development of consumer cyber risk assessment, and any associated cyber-insurance to mitigate residual risks.

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.

[11.1] The UK Computing research Community stands ready to assist in the implementation of these provisions – for example, to establish an evidence base that demonstrates the utility of the proposals in terms of the protection provided to UK consumers. We are also well-equipped to provide guidance on user-centred patching/reporting mechanisms.

[11.2] The impact assessment provides only a very limited analysis of the consequences for the IoT supply chain. Many consumer products integrate components from a range of third-party manufacturers who may themselves not meet the three top guidelines. The onus will be on the last supplier to guarantee their assemblies. Are these integrators in a position to guarantee everything they source? It seems likely that they might be able to demonstrate compliance with the proposals in terms of their activities but not meet the true spirit of the three guidelines in terms of the entire IoT device architecture. A parallel could be drawn

with the continuing difficulty that catering companies have in ensuring that their supply chain is free of particular allergens.

12. We welcome any additional feedback not already captured above.

[12.1] We would reiterate the importance of ongoing review, already recognised within the proposals. Given the speed of innovation and deployment in the IoT domain, critical refinement will be more important here than in other regulatory settings. The speed of emergent social processes is illustrated by changes in social media. We anticipate similar emergence as people engage creatively (and subversively) deploying Consumer IoT.

[12.2] We would stress the potential role that CS research can play in supporting the implementation and refinement of these proposals. In cybersecurity we work hard to build systems that are robust and secure, and we also think about what happens when they break (or are broken). We create testbeds and we run simulations. We are researching the applications and implications of AI for IoT (e.g. Petras 2). Hence as noted can also provide a great deal of expertise to help with the Consumer IoT regulatory proposals. UK computing research is world leading and has the scope to identify future trends and possibilities that often is denied to the Consumer IoT industry by market pressures.

[12.3] This set of proposals looks at device by device approval. It seems to say little about security as a more systemic concept – earlier paragraphs have emphasised the interactions between secure devices and insecure infrastructures or legacy components. Any regulatory intervention might also consider the development of reference environments enabling IoT vendors to assess interactions with representative cross-sections of existing devices and architectures.