Response to

Proposals for Regulating Consumer Smart Product Cyber Security - Call for Views[1]

On behalf of the UK Computing Research Committee, UKCRC.

Prepared by: Professor Chris Johnson,
Pro Vice Chancellor, Engineering and Physical Sciences,
Queen's University Belfast.
c.w.johnson@qub.ac.uk

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.

1) Are you responding as an individual or on behalf of an organisation?

b) Organisation

2) [if individual] Which of the following statements best describes you?

e) Academic

3) [if organisation] Which of the following statements best describes your organisation? Please select all that apply

c) Cyber security provider

d) An academic or educational institution

4) [if organisation] Which of the following best describes your organisation?

a) UK only based organisation [conditional follow-up - which country is your organisation's head office based in? England / Scotland / Wales / Northern Ireland – ALL Regions]

[1] https://www.gov.uk/government/publications/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views

5) [if organisation] Which one of the following best describes the sector of your organisation?

m) Education / Academia

6) [if organisation] Including yourself, how many people work for your organisation across the UK as a whole? Please estimate if you are unsure.

e) 1,000 or more

7) [if organisation] What is the name of the organisation you are responding on behalf of?

UK Computing Research Committee, UKCRC

8) Are you happy to be contacted to discuss your response and supporting evidence?

Yes

9) [if yes to 8] Please provide a contact name and email address below.

Professor Chris Johnson,
Pro Vice Chancellor, Engineering and Physical Sciences,
Queen's University Belfast.
c.w.johnson@qub.ac.uk

10) To what extent do you agree or disagree that the following categories of conventional IT products should be included within the scope of the proposed regulation?

a) Laptops [scale from strongly disagree to strongly agree].
Disagree

b) PCs [scale from strongly disagree to strongly agree]
Disagree

c) Smartphones [scale from strongly disagree to strongly agree]
Neutral

Please explain the reasons for your answers to the above question:

We have reservations about the inclusion of desktops and laptops - at least, without some qualification and nuance, because they tend to have much more separable hardware and software than most other classes of device (which tend to come as a single package, and where major software changes are more rare). Although there are benefits from including them in the scope, especially in terms of consistency, it opens many potential concerns in terms of establishing the particular version of a device being considered.

Simple example: is a RaspberryPi a desktop computer? It appears to be (plug in an HDMI display, keyboard, and mouse, and it behaves a lot like any Linux box). Applying the requirements (as laid out so far) to a RaspberryPi would probably be counter-productive and perverse, not least because they mostly apply to the OS in that case, which is designed to be easily user-replaceable.

11) The ambition of this regulation is to establish a robust baseline across all smart connected products and to protect consumers and the wider economy from a range of harms. Please detail any unintended impacts that this proposed regulation would have, beyond the ambition stated above, to your organisation / the wider economy.

Please think about the proposed definitions of ‘Producers’, ‘Distributors’ and any other organisations in the consumer smart product supply chain when answering this question. Please clearly state which types of organisation you are referring to in your response.

a) Producers

b) Distributors

c) Other organisations (please specify)

d) Wider economy

Concerns arise at the margins of these definitions, particularly for devices in kit form, or build-your-own (or bring-your-own software). The responsibilities of different parties (Producers, Distributors and Consumers – especially researchers and hobbyists) will be ambiguous. Those are edge-cases and could be excluded from explicit consideration by focussing on 'shrink-wrap' products. However, this would exclude second-hand/re-sale, both of which seem to be overlooked entirely. There is a growing market in legacy consumer products – including retro games consoles.

Is the regulatory burden on very small-scale producers or distributors proportionate? It would be unfortunate for any legislation to have the effect of outlawing either niche businesses or start-ups.

Clarity and careful thought are needed regarding roles in a global e-commerce context. Section 4.4 raises more questions than it answers. In-scope devices can, for example, be purchased from overseas via platforms like Amazon and eBay where the role of the platform in the import process is not particularly transparent to the end user. Users can and do also buy electronics online from vendors without a UK presence: clarity about the intended impact of these regulations on those cases is most desirable (does it potentially sanction someone who buys a Gizmo from AliBaba or GearBest.com and gives it to their neighbour?).

What would happen if a consumer deliberately chose to install software on their device that violated the requirements of these provisions – this is a common activity where "mods" are available to a host of consumer devices.

Although we broadly support the proposals, we are concerned at the lack of clarity over responsibility for regulatory intervention. We do not think that any of the six existing bodies, listed in section 5.7, has sufficient technical experience or staffing to take on these responsibilities. The side-effects of inadequate support for implementation might have an impact on the wider UK economy with delays in the provision of advice, on approvals and on appeals.

We also have concerns under "c) Other organisations" where UK Universities might wish to obtain devices that do not meet the present requirements for consumer products because – inter alia they are needed for wider research in cyber security or because they embed leading edge functionality but are not supported by all the distribution infrastructure etc that might be required under the proposed legislation. The Universities could be interpreted as consumers and the distributor/producers might refuse to supply the devices if they felt they would be liable under the legislation.

12) Please share your views on the suggested supplementary guidance to help businesses to implement the proposed security requirements provided in Section 4 - Obligations. Are there any other forms of guidance you feel should be included?

It is very surprising that the proposals contain no mention of the NCSC. We can envisage situations in which they may be needed to supplement any guidance mentioned under Section 4. In particular, there is a need for support when distributors/manufacturers may be notified of a vulnerability but where there is insufficient detail to identify and then mitigate the concern; this might be the case where criminal actors threaten disclosure of vulnerabilities.

NCSC has considerable experience of developing and maintaining guidance and they remain the primary reference for incident response/recovery. It would be useful to clarify the relationship between any proposed regulatory organisation and the advice/guidance to be provided by NCSC in order to promote coordination and avoid unnecessary duplication.

The requirements on disposal might usefully include guidance on how to overwrite any sensitive information prior to disposal and eventually an obligation to provide an interface which allows this. There are many documented cases of information breaches connected with data remaining on devices after disposal[2].

13) The proposed approach suggests using a broad definition of network-connectable product classes which could be in scope and specifying specific categories of products that are out of scope.

a) Do you agree or disagree with this suggested approach? Please explain your answer.

This seems appropriate. The assumption would be that products would, by default, be within scope. However, as noted in previous sections this may delay the marketing of innovative products within the UK until suppliers and distributors have met these requirements.

The exclusions need to be very carefully considered for the growing classes of device that cross different categories of use – in particular, a range of sensing technologies have been approved for clinical use but can also be bought more widely to support assisted living and care in the community.

b) Please share any views you have on alternative wording, approaches, or ways to improve the proposed approach.

In practice, the utility of either approach depends on the specific definition of a product class and whether or not it is regularly reviewed to limit unnecessary exclusions or situations where, for instance, UK research organisations may have difficulty in sourcing key technologies.

Using a broad definition of network-connectable product classes which could be in scope means that the requirement will be so generic that they may be hard to interpret for new products and services; for instance, where distributors provide services over third party hardware that can over-write default passwords etc.

14) Please outline below any further feedback on the security requirements, as set out in section 3.3 of the Call for Views.

Requirement 2 (to have a point of contact for disclosing vulnerabilities) provides no onus to act on the vulnerability report other than acknowledging receipt and providing status updates. This could be strengthened to include, at a minimum, an obligation to inform the regulator and NCSC and to post a notification of resolution or escalation within 6 weeks. If no resolution is accepted within 6 months to a year, there should also be a requirement to notify customers with the possibility that they seek financial compensation. These issues are raised tangentially again in Box 6 – perhaps they could be integrated more directly.

[2] https://www.recycleit4u.co.uk/services/mobile-phone-and-tablet-secure-data-destruction/

Requirement 3 seems rather weak – nor is there an explanation of how to resolve the tension with requirement 2 that might arise when a vulnerability leads to the withdrawal of a device before the period of support expires. The supporting prose seems clearer – especially means of automatically ceasing network connectivity after their support period ends.

Great care may be needed over the interpretation of "transparency". Many existing consumer agreements contain important information about data protection and privacy that is "hidden" within many paragraphs of arcane language. In consequence, a broad range of consumer protection legislation has failed to have the intended impact on digital products and services[3].

15) This proposal requires an exchange of information between 'Producers' and 'Distributors' in the supply chain to confirm compliance:

4.2 - Box 6 - Draft proposal and example guidance content for 'Producer obligations'
"A prohibition on a 'Producer' from supplying or making a product within scope available in the UK market unless the product is compliant with the security requirements."

This places an obligation on 'Producers' to evidence compliance with the security requirements to the 'Distributors'.

a) Should this information exchange approach set out in box 6 be adopted? Please explain your answer.

b) Should 'Distributors' also have obligations as part of this information exchange? Please explain your answer.

While we agree that "The market for assurance schemes is still in its infancy and while this is changing with the introduction of new products, it would not be appropriate to mandate a method of assurance at this time"; indicative guidance should be provided to UK companies on acceptable means of compliance. The UK should also engage with research organisations and international standards bodies to identify effective means of assurance and help ensure that the costs associated with compliance are not only placed on UK consumers.

Further issues arise when consumers report concerns to the distributor – it is unclear whether there is a transitive obligation on the distributor to then report to the manufacturer. What happens if the manufacturer does not respond to a particular incident report? Presumably if the regulator believes the manufacturer has not met the intention behind these requirements it would lead to enforcement actions not just on the immediate distributor but

[3] https://ec.europa.eu/info/sites/info/files/terms_and_conditions_final_report_en.pdf

on ALL UK distributors of that product and of ALL products that might share affected components/software.

Related to the discussion in Q11, it's not clear that this direction of information-flow (producer to distributor) fits all cases: if an online marketplace is a distributor, the end-user making a personal import is someway between the consumer and a producer (under the definition in Box 5).

16) The proposed approach intends to include entities who supply or make products available online, e.g.those who act as a marketplace, a platform for consumer sales online or provide either first or third party sales. Do you agree with this approach? Please explain your answer.

Yes this approach seems sensible. We have noted the consequent difficulty in enforcing the requirements. There is a danger that this undermines the credibility of the initiative if the regulator cannot influence the behaviour of those vendors and manufacturers. For instance, UK consumers may attempt to purchase products from suppliers who in good faith are unaware of the requirements that they face when shipping to the UK; many of these transactions are not governed by UK law at the time of payment. Similarly, what happens when the apparent UK representatives of a company are employed by a different legal entity to that fulfilling the transaction? These situations are partially addressed in the existing requirements but it has to be recognised that the last 2-3 years have seen a rapidly growing market mechanisms for on-line transactions that are often opaque to the consumer.[4]

17) Should the definitions such as ‘Producer’ and ‘Distributor’ (see box 5 and 7) in existing product safety regulations (such as the Radio Equipment Regulations 2017, and the General Product Safety Regulations 2005), be used as a basis for the definitions in this proposal?

if no - please provide details of any alternative approaches that could be considered

Our concerns over these definitions have been raised in previous sections. The requirements place obligations on a range of parties to a particular transaction yet each of these roles can be instantiated in a myriad of ways across different electronic marketplaces.

One of the greatest concerns with previous attempts to regulate digital marketplaces has been the technical inability to enforce the intent behind the proposed regulations – the proposals to regulate on-line pornography are a strong illustration of this. Unless the boundary cases mentioned in this

[4] https://www.bbc.co.uk/news/technology-53759932?intlink_from_url=https://www.bbc.co.uk/news/technology&link_location=live-reporting-story

response are considered then there is a danger of further undermining the credibility of many laudable attempts to protect the public.

18) Box 10 describes a suite of example corrective measures and sanctions which could be made available to the enforcement body in the event of non-compliance. These are listed below (see Box 10 for further details):

Voluntary and Corrective Measures
Compliance Notice
Undertaking
Enforcement Order
Security Notice
Forfeiture & Destruction
Administrative Penalties
Financial Penalty

a) Is this proposed suite of corrective measures and sanctions proportionate overall? Please explain your answer.

The suite of corrective measures is too complex and should be simplified. With so many potential degrees of response there is a danger of legal challenge over consistency. Gicven the potential scope of these measures for connected devices, the complex market structures across multiple jurisdictions clarity and simplicity will be essential. A three tier approach based on a subset of these enforcement actions should be sufficient.

b) Are each of the potential measures above an effective response or deterrent to non-compliance? Please explain for each of the 8 proposed measures.

Voluntary and Corrective Measures – yes as an appropriate first step.
Compliance Notice – no could be covered within the voluntary and corrective measures notice.
Undertaking – no, covered in part by voluntary and corrective measures.
Enforcement Order – yes an appropriate second step.
Security Notice – yes, final suit of enforcement actions. Augmented by possible civil actions?
Forfeiture & Destruction – no, could be part of security notice.
Administrative Penalties – no, court sanction necessary especially for companies overseas.
Financial Penalty – no, could be covered in security notice?

19) Are there significant barriers that would prevent your organisation from becoming compliant with the security requirements within the suggested timescales for compliance (detailed in Box 9 and summarised below)?

Security requirement 1
Ban universal default passwords - 9 months

> Yes. We represent UK research in Computing Science, we would welcome exemptions that enable us to procure non-compliant devices for security research and in some cases to ensure access to leading edge equipment that might not be supported by the market mechanisms envisaged in these proposals.

Security requirement 2
Implement a means to manage reports of vulnerabilities (providing a publicly available vulnerability disclosure policy which includes at least contact information for the reporting of issues, and information on timelines for initial acknowledgement of receipt and status updates until the resolution of the reported issues) - 3 months

> Yes. We already have mechanisms for reporting concerns, for instance through JANET and via the NCSC. However, a number of UK research projects also provide access to innovative technologies and devices – for instance as part of research trials for assisted living that would not be covered by existing healthcare regulations. In such circumstances, UKRI might need to, and probably should, establish a unified reporting mechanisms.

Security requirement 3
Provide transparency on for how long, at a minimum, the products will receive security updates - 6 months

> Yes. In many research projects, the focus is on innovation that may lead to new products and services driving improvements in the UK economy. In these higher TRLs, other safeguards may be put in place to protect the users involved in a trial but there may not be resources to provide security updates within the timeframe of the trials. Installing those updates may trigger further problems – for example, altering experimental controls. The costs associated with implementing these requirements in a research setting should be considered – the existing definitions of may already exclude them but it is not clear that this is the case for all UK research from an initial reading of the proposals.

[if Yes, what are the barriers for implementation to the suggested timescales, how much time would be required for your organisation to become compliant with the security requirements (in months) and could these barriers be mitigated?]

> Exemptions for research providing there is a formally documented security risk assessment and the outcomes are explained to all users/consumers involved in a trial.

20) Please provide details of any additional costs to your organisation that would result from implementing each of the security requirements in our proposed approach:

If your organisation is both a ‘Producer’ and ‘Distributor’ of consumer smart products, please indicate explicitly which aspect of your organisation’s operations these costs / benefits would impact in your answers. Please also indicate whether the costs cited are one-off, or would be incurred annually.

a) Ban universal default passwords

> Delays in obtaining new technologies and potential bans on obtaining devices that might otherwise support cyber security research. We represent UK research in Computing Science, we would welcome exemptions that enable us to procure non-compliant devices for security research and in some cases to ensure access to leading edge equipment that might not be supported by the market mechanisms envisaged in these proposals.

b) Providing a means to manage reports of vulnerabilities (providing a publicly available vulnerability disclosure policy which includes at least contact information for the reporting of issues, and information on timelines for initial acknowledgement of receipt and status updates until the resolution of the reported issues)

> See question 19, part b)

c) Provide transparency on for how long, at a minimum, the product will receive security updates

> See question 19, part c)

d) Please provide details of any benefits to your organisation that would result from the implementation of these security requirements.

> These proposals raise particular challenges for UK Computing research but they are welcome. Although the proposed measures do not fit easily within the context of, for instance, UKRI funded projects, the underlying concerns deserve greater thought. Agencies such as ARPA are likely to encourage larger scale trials of new innovative and network enabled technologies. Exemptions could be used to promote research and innovation but would only be appropriate if risks were clearly identified and mitigations put in place to safeguard the public.

21) Please estimate any additional reporting impacts or costs to your organisation resulting from:

a) The proposed obligation for ‘Producers’ to demonstrate compliance with the security requirements to ‘Distributors’;

> These are broadly the same as in section 20 – where UK computing research projects wish to field new, leading-edge technologies they might be perceived to be acting in the role of distributors but without any of the expertise or experience that might be

expected of companies working in more conventional distribution and sales. Leading edge research could be delayed or abandoned in the delays that might arise while assurances were obtained from producers.

b) The requirement for 'Distributors' to process information from 'Producers';

When answering this question, where possible, please clearly describe any costs or wider impacts, including job roles, the estimated number of hours of staff time associated with each job role, total cost estimates per product line (specifying whether one-off or annual) and overall estimated total annual cost to your organisation.

Most but not all UK Computing Research organisations should be in a situation to process and interpret the data provided by producers. However, as mentioned above a lack of familiarity of acceptable means of compliance and the multiplicity of candidate regulatory agencies creates a host of concerns for us.

c) Are there any ways we could tailor our approach to mitigate these reporting impacts?

In the US, many of these objections can be addressed through Code of Federal Regulation (CFR) waivers that are routinely awarded in areas of national strategic importance and these should be used much more widely to support research and innovation post-Brexit.

22) To what extent do you agree with the proposed approach within 5.6 Enforcement body considerations?

a) Do you agree with the approach in Box 12 (Considerations for designating an enforcement body)?

The outline proposals seem good but we note that none of the proposed agencies has both the competency AND the resources to meet all the obligations identified here for them. Also, we are concerned that any failure to achieve the intentions in these proposals will further undermine public confidence ion our ability to protect against potential security threats.

b) Are you supportive of the approach in Box 13 (Example powers for the enforcement body)?

Yes but greater clarity is needed in the relationship with the NCSC and a more focussed approach to the available actions for non-compliance would be needed.