CarnegieUK TRUST

CHANGING MINDS • CHANGING LIVES

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

June 2019

1. We welcome the Government's intention to enshrine the existing Code of Practice for IoT Security within a regulatory framework and commend the objectives to "restore transparency within the market and to ensure manufacturers are clear and transparent with consumers by sharing important information about the cyber security of a device, meaning users can make more informed purchasing decisions".

2. As the authors of Carnegie UK Trust's detailed proposal for a statutory duty of care to reduce harm on social media[1], which has informed the Government's recent proposals in its Online Harms White Paper, we see Codes of Practice such as this and the ICO's Age Appropriate Design Code as important steps in moving towards a system-level approach to addressing digital harms. A systems-level approach is proactive, precautionary and proportionate and is designed to take the responsibility away from users to protect themselves from what are otherwise reasonably foreseeable harms.

3. We are therefore responding to this consultation from the perspective of our interest in the wider online harm reduction agenda and the implementation of a statutory duty of care. As such, we do not have specific detail to provide on every aspect of the consultation's questions but have focused on some areas which we feel are particularly notable.

4. As we set out in our work, computer code sets the conditions on which the internet is used and the same applies to internet-connected devices; code is the architecture of cyberspace and this, combined with business decisions (such as those that shape the collection and use of personal data) affects what people do online and how their data is used. The same is true in relation to the design of Internet of Things (IoT) devices. The environment within which harm occurs is defined by code that the service providers have actively chosen to deploy, their terms of service or contract with the user and the resources that service providers deploy to enforce that.

5. We observe in our work that, if services providers chose to prioritise the reduction of online harm to vulnerable users, they "could choose not to deploy risky services without safeguards or they could develop effective tools to influence risk of harm if they choose to deploy them." The same is true of safeguards to ensure cyber security, data protection and protection of the privacy of users of connected devices. Service providers can deploy tools to deliver these aspects and mandatory Codes of Practice, like this and the Age Appropriate Design Code, show clearly what these choices look like.

1 See our full detailed paper (April 2019) along with our original blog posts and other materials here: https://www.carnegieuktrust.org.uk/project/harm-reduction-in-social-media/

6. The 'by design' approach is an effective mechanism to draw attention to the fact that these choices can and should be taken into account in service design, not bolted on as an afterthought. In making the IoT Secure by Design Code mandatory, the Govenrment is acknowledging that, up to this point, those choices have not – in general – been made voluntarily by service providers. Regulation is often necessary to deliver system change; in this regard, we see the this Code and the ICO's code as important forerunners of the wider regulatory system, underpinned by codes of practice, that is envisaged in the DCMS Online Harms White Paper.[2] DCMS will need to play an important strategic role going forward to ensure that the various Codes, enacted under different legislative instruments and overseen by different regulatory or enforcement bodies, are complementary and mutually reinforcing, that compliance burdens for industry are minimised and that – where particular products or services fall under multiple different codes of practice – that their obligations are clearly defined and information on compliance, or otherwise, is shared effectively between the responsible regulatory or enforcement bodies.

7. We set out below some specific observations and comments on the consultation questions.

## Implementing the "top three" guidelines

8. We recognise the concerns that have been raised by manufacturers re the burdens that would be created by implementing all the aspects of the existing code of practice and the decision to focus on the "top three" guidelines as an initial baseline to both protect consumers and minimise the additional burden on industry. On the vulnerability disclosure policy, this will need careful drafting as in legal terms it is linked with the concept of authorisation, or lack of authorisation in the offence of unauthorised access. The requirement to have a policy implies consent, but this needs to be expressly stated and the policy should specify the type/level of access agreed. These points matter particularly in relation to the compatibility of this policy with the Computer Misuse Act 1990 (CMA) as the actions of finding and disclosing a vulnerability can be an s1 CMA offence.

9. We welcome the intention that further requirements from the existing code will be mandated via regulation in a staged approach.

10. However, we would argue that this staged approach should apply to both large and small manufacturers and there should be no exemption for smaller or newer forms as the mandatory elements are rolled out. While it is true that post-hoc implementation measures will be felt "more by smaller organisations", we do not agree that this is a reason to exempt them nor do we agree with the view that embedding "by design" measures "dampens innovation".

11. On the innovation point, the implementation of a code such as this would have the effect of developing a market in responsible tech throughout the whole supply chain for connected products, with a level playing field in terms of regulatory compliance obligations for each player.

12. On the size point, in our work to develop a duty of care for online harm reduction, we initially felt that this should apply to firms of a significant size (measured in terms of users) and exempt smaller or newer companies. We received lots of feedback from stakeholders, particularly those representing children's rights and, as we set out in our April paper:

2 Our detailed view on the proposals in the White Paper, particularly the differences between the "duty of code" regime that we envisaged and that described by the Government, will be published soon.

*We therefore came to a view that there should be no de minimis user/customer threshold for the duty of care. Some groups are sufficiently vulnerable (e.g. children) that any business aiming a service at them should take an appropriate level of care, no matter what its size or newness to market. Beyond child protection, basic design and resourcing errors in a growth stage have caused substantial problems for larger services. Much of the debate on AI ethics attempts to bake in ethical behaviour at the outset. The GDPR emphasis on privacy by design also sets basic design conditions for all services, regardless of size. We are struck that in other areas even the smallest businesses have to take steps to ensure basic safety levels – the smallest sandwich shops have to follow food hygiene rules. In both these cases, risks are assessed in advance by the companies concerned within a framework with a regulator.i*

*We note that Parliament made two major statutory duties of care we that we discuss above (Occupiers Liability 1959 and HSAW 1974) above apply almost pervasively, not substantially constrained by size of unit nor by a pre-assessment of the level of danger.*[3]

13. The safety and security of connected toys used by children is of an increasing concern – both in terms of data privacy and protection, as well as the risk of hacking and contact with children from strangers – and has been raised in campaigns by consumers organisations and that Which? has played an important role in developing the Code of Practice.[4] Given the seriousness of the threats to children if IoT devices are compromised and the particular risk posed when new-to-market toys become "must-haves", we would strongly recommend that baseline security measures and the phased approach to mandating all the elements of the Code of Practice are not applied differently according to the size or newness of the manufacturer.

## Security label and regulatory proposals

14. We have no strong views on the design of the security label proposed but welcome this as a positive step to provide clarity and transparency to consumers at the point of purchase on the security of the device and the timescale for ongoing security updates. Significant economic detriments for consumers are emerging when manufacturers fail to provide security updates for smart and connected devices beyond a limited period of time. With more and more domestic appliances and home devices having a "smart" element, whether consumers require it – or indeed want it – the risk of harms occurring when these products are no longer supported or secure is significant; often the only choice to protect their security and data is to replace the device even the "non-smart" elements are still functioning, effectively a form of built-in obsolescence. If manufacturers have to be clear about the timeframe for that support on a product label, customers will be able to make informed choices about the value for money of the device at the time of purchase and consumer pressure for change from the industry is likely to grow. This will be particularly important where appliances, like smart meters, are mandated. And the duty of care approach also has an application here, whereby manufacturers should be obliged to act in a precautionary manner, monitoring and responding to threats and risks to users as they emerge.

15. We agree with your recommended option (A) to mandate retailers in the first instance not to sell consumer IoT products without a security label, as this will provide greater clarity and consistency to consumers and a much clearer context than the other two options for both manufacturers and

3 https://d1ssu070pg2v9i.cloudfront.net/pex/carnegie_uk_trust/2019/04/08091652/Online-harm-reduction-a-statutory-duty-of-care-and-regulator.pdf

4 https://www.consumersinternational.org/what-we-do/consumer-protection/safer-products/connected-toys/; https://www.which.co.uk/news/2017/11/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys/

retailers can comply with the regulations. We would urge the Government – as with proposals in the Online Harms White Paper – to move quickly to secure Parliamentary time for Primary legislation so that the mandated labelling scheme can be implemented, and for the secondary legislation to follow soon after. We have no strong views on which enforcement agency should be responsible for the oversight of the code, but it will need to have auditing powers if the code is to rely on self-certification; this could be modelled on the GDPR approach, where controllers have to retain records so that they can provide evidence of compliance if asked.

16. We are happy to provide further information on any of the above.

Carnegie UK Trust
Contact: maeve@carnegieuk.org