horizon
DIGITAL ECONOMY RESEARCH

Response to Consultation on the Government's Regulatory Proposals Regarding Consumer Internet of Things (IoT) Security

Submitted by Prof. Derek McAuley, Dr. Ansgar Koene and Dr. Jiahong Chen of Horizon Digital Economy Research Institute, University of Nottingham

4 June 2019

1. Horizon[1] is a Research Institute centred at The University of Nottingham and a Research Hub within the RCUK Digital Economy programme[2]. Horizon brings together researchers from a broad range of disciplines to investigate the opportunities and challenges arising from the increased use of digital technology in our everyday lives. Prof. McAuley is Director of Horizon and principal investigator of the EPSRC-funded DADA[3] (Defence Against Dark Artefacts) project, addressing smart home IoT network security, and its acceptability and usability issues. Dr. Koene led the research of the EPSRC-funded UnBias[4] (Emancipating Users Against Algorithmic Biases for a Trusted Digital Economy) project and is Research co-Investigator on the EPSRC-funded ReEnTrust[5] (Rebuilding and Enhancing Trust in Algorithms) project. Dr. Chen is a Research Fellow of Horizon, currently working on the DADA project.

Consultation questions: feedback on regulatory approach and labelling scheme

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. Yes, there is a pressing need for governmental intervention in the market of consumer IoT products. While there have been industrial initiatives in response to the constant concerns around the safety, security and privacy standards of internet-connected devices, recent incidents have shown that IoT devices remain highly susceptible to vulnerabilities that can be exploited to intrude on the user's privacy,[6] to have unauthorised control of the device,[7] and even to facilitate mass-scale attacks.[8] Not only do these matters affect individuals, but coordinated action using millions of devices needs to be considered a matter of national security concern.

3. Industrial self-regulation has clearly been insufficient to guarantee a high level of protection to consumers of IoT products. Another issue concerns products imported from foreign countries, which are not subject to self-regulatory initiatives or sectoral security standards. Such market failures make it necessary for the Government to introduce measures to regulate insecure consumer IoT products.

[1] http://www.horizon.ac.uk

[2] https://epsrc.ukri.org/research/ourportfolio/themes/digitaleconomy/

[3] https://www.horizon.ac.uk/project/defence-against-dark-artefacts/

[4] http://unbias.wp.horizon.ac.uk

[5] https://ReEnTrust.org

[6] https://www.dailymail.co.uk/sciencetech/article-5228017/Hackers-using-webcams-turn-people-slaves.htmlUK

[7] https://cryptovest.com/news/smart-devices-could-create-cryptomining-armies/

[8] https://www.zdnet.com/article/this-botnet-snares-your-smart-devices-to-perform-ddos-attacks/

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?

4. The 'top three' security provisions are necessary to ensure a minimum level of security for consumer IoT products, but they are far from adequate even only as a mandatory baseline. We are of the view that an appropriate set of baseline requirements should cover most, if not all, of the thirteen guidelines set out by the Code of Practice for Consumer IoT Security. (See answer to Question 5 below)

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.

5. The use of positive labels may help effectively communicate the compliance with these requirements to consumers. However, allowing negative labels would mean that the 'top three' security guidelines are not compulsory for consumer IoT products. This would not just run counter to the baseline nature of the three requirements but may also be misleading in that it may create the false impression that these requirements are simply extra safeguards, and that products not compliant with these requirements are 'still safe to use'. As noted above, allowing insecure devices with negative labels to be sold would not just pose threats to individual users, but also the security of the wider networks to which those devices are connected.

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.

6. No response.

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.

7. While it is essential to ensure that consumer IoT products without a security label cannot be sold in the first instance, this does not represent a satisfactory approach. Instead, the thirteen guidelines laid down by the Code of Practice provide a more complete set of standards for IoT security, and should be observed altogether as a mandatory requirement. Accordingly, Option C – i.e. requiring retailers to only sell consumer IoT products with a label that evidences compliance with all thirteen guidelines – is our preferred option.

8. We would like to point out that most of the ten guidelines additional to the 'top three' are already legally required under data protection law[9] and cybersecurity law[10]. For example, 'securely store

[9] Such as the GDPR, the ePrivacy Directive, the Data Protection Act 2018, and the Privacy and Electronic Communications (EC Directive) Regulations 2003.

[10] Such as the Cybersecurity Directive, the Network and Information Systems Regulations 2018, and the EU Cybersecurity Act (to be formally approved by the Council).

credentials and security-sensitive data',[11] 'communicate securely',[12] 'ensure that personal data is protected',[13] 'make it easier for consumers to delete personal data',[14] and 'validate input data'[15] are mandated by data protection law, whereas 'minimises exposed attack surfaces',[16] 'ensure software integrity',[17] and 'monitor system telemetry data'[18] are clearly required for alignment with the objectives of cybersecurity law.

9. This means the regulatory regime under Option C would not per se create a significant or disproportionate amount of compliance costs to responsible retailers or manufacturers who are already compliant with existing laws. Also, mandating the compliance with all thirteen requirements would also result in considerable benefits for consumers, promote public trust in IoT products, and build up an internationally-renowned reputation for the UK IoT industry.

Consultation questions: feedback on the impact of our proposals

10. As noted, we view that the impact on responsible manufacturers who will already be designing in line with these basic secure design principles is negligible; those who will not comply should rightly be blocked from retail sales.

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.

11. We are of the view that Trading Standards is best positioned to enforce the requirements set out in the regulatory regime, as they are already empowered to enforce consumer protection legislation under the Consumer Rights Act 2015. Under the CRA 2015, they have the powers to require information, to make a test purchase, to inspect products, and to bring proceedings against violations.[19] Such statutory powers as well as their experiences as consumer law enforcer would allow Trading Standards to effectively handle non-compliance with the guidelines laid down by the Code of Practice.

Consultation questions: further feedback

Please provide any additional comments on the consultation stage impact assessment, the regulatory options and the proposed labelling scheme.

We welcome any additional feedback not already captured above.

[11] See Article 5(1)(f) GDPR; Section 66 DPA 2018.
[12] See Article 5 ePrivacy Directive; Section 6 PEC Regulations 2003.
[13] See GDPR, DPA 2018.
[14] See Article 17 GDPR, Section 47 DPA 2018.
[15] See Article 5(1)(d) GDPR, Section 38 DPA 2018.
[16] See Article 51(i) Cybersecurity Act.
[17] See Article 51(j) Cybersecurity Act.
[18] See Article 51(d) Cybersecurity Act.
[19] See Schedule 5 Consumer Rights Act 2015.

12. We would like to stress that ‘consumer IoT product’ is a fairly broad concept that may cover a wide range of devices – ‘products that are connected to the internet and/or home network and associated services’ as defined by the Code of Practice. The diversity of products falling under such a broad definition means that some of the requirements are not applicable to all consumer IoT products. For example, some smart devices do not have password control but are configured by physical operations, to which the ‘no default passwords’ provision would not apply. Some devices may be configured only through a smart home hub or a third-party system, whose security level would depend on the design of the interfaces and the security measures of the controlling system. These circumstances should be taken into account when deciding on the appropriate regulatory requirements and enforcement approach imposed on different categories of consumer IoT products.
13. We would also like to make it clear that, while we support Option C as the best regulatory model, we are equally aware that certain requirements may function more as ‘best practices’ rather than ‘minimum requirements’, such as the ‘make installation and maintenance of devices easy’ provision. We urge policymakers to carefully consider the applicability of all thirteen requirements to a variety of devices, and where appropriate, provide exceptions and guidance for certain types of products in relation to the relevant particular requirements.