Dear Norman,

Thank you for your letter dated 27 February 2019 regarding consumer smart devices and the regulations they are subject to.

The Department for Digital, Culture, Media and Sport (DCMS) and the Department for Business, Energy and Industrial Strategy (BEIS) are taking a comprehensive set of steps that aim to ensure that smart devices are secure and to better protect consumers’ privacy and online security in an increasingly digital world.

Below we have set out some of the activities being carried out across Government following evidence received by the Science and Technology Committee from Dr Emma Williams.

DCMS Secure by Design Programme

Within her evidence, Dr Williams refers to the Secure by Design review. DCMS commenced the review in early 2017, and it has since developed into a programme of interventions, covering internet-connected consumer products within its scope.

As you note in your letter, our ambition is to move the burden away from consumers being expected to expertly secure their smart devices and instead ensure that strong cyber security is built into these products by design.

To date, the Secure by Design programme has achieved the following milestones:

- Our Secure by Design policy report, published in March 2018, sets out the risks posed by insecure Internet of Things (IoT) devices and services and makes the case for Government intervention. An informal consultation on the report and its proposed policy interventions was undertaken. The report was informed by close collaboration with the National Cyber Security Centre (NCSC) and an independently chaired Expert Advisory Group.

1 https://www.gov.uk/government/publications/secure-by-design-report
In October 2018, we published the Code of Practice for Consumer IoT Security, which sets out 13 steps for manufacturers to secure their products. As the first government globally to publish such guidelines, and with its translation into several languages, the Code has achieved significant international recognition. Three manufacturers of smart devices, HP Inc, Centrica Hive Ltd and Green Energy Options (geo) Ltd, pledged to implement the Code of Practice for many of the products they will develop in the future. We also published guidance for consumers purchasing smart devices for the home.

The Code of Practice is the basis of the first globally-applicable industry standard on consumer IoT security, which was developed through ETSI, the European Standards Organisation. Published in February 2019 as ETSI Technical Specification 103 645, the standard is set to inform, at home and abroad, the development of regulation and industry-led certification schemes.

Looking ahead, the Secure by Design programme will continue to carry out actions that seek to improve the security of consumer smart devices. This includes:

1. Regulation: In our response to the Secure by Design informal consultation we stated the Government’s ambition for appropriate aspects of the Code of Practice to become legally enforceable. DCMS are investigating which aspects of regulatory change are necessary to ensure that baseline security is built into smart products and that this is properly signposted to consumers. We aim to develop regulation that achieves effective outcomes for consumers, whilst keeping additional burden on businesses minimal. Regulatory interventions will also need to be designed to be able to keep pace with changing technology. Further, our ambition is to ensure that consumers have access to important information about the cyber security of a device so that they can make more informed decisions when purchasing smart products. We will be consulting on these proposals in Spring 2019.

In her committee evidence, Dr Emma Williams mentioned the General Data Protection Regulation (GDPR). It is important to note that where products such as smart devices are collecting personal data, organisations that process such information must comply with the GDPR/Data Protection Act 2018.

2. Promoting good security practice: DCMS is driving forward implementation of the guidelines within the Code of Practice. To that end, Margot James MP has invited leading IoT manufacturers to a roundtable meeting, which is to be hosted by the consumer body Which? in April.

---

3. International engagement: DCMS has been at the forefront of global efforts to improve the security of smart products. We will continue to engage closely with European partners, the Five Eyes alliance and beyond to pursue a harmonised global approach to improving IoT security.

As part of the activities set out above, DCMS has engaged with leading consumer groups, including Which?, Citizen’s Advice, the European Consumer Organisation (BEUC), the European Association for the Co-ordination of Consumer Representation in Standardisation (ANEC), the Internet Society and Consumer International.

DCMS has also worked closely with the PETRAS IoT Research Hub, a consortium of nine leading UK universities. We have commissioned several studies to inform Government’s policy interventions, and these have been published on GOV.UK. Additionally, DCMS have been working with the PETRAS/UCL Consumer Security Index project to inform our work on developing a labelling scheme for household smart devices.

BEIS programmes and projects

Turning to the steps BEIS is taking on cyber security in relation to smart devices: in 2017 the Smart Systems and Flexibility Plan was published jointly with Ofgem, and outlined 29 actions to deliver a smarter, more flexible energy system.\(^7\)

Smart meters are the foundation of an accessible smart energy system for consumers. The smart metering system has been developed in consultation with leading experts from within industry and Government to provide strong security controls. In addition, smart metering system security uses international standards and common industry good practices, e.g. encryption of sensitive data, protection from viruses and malware, access control, tamper alerts on meters, two-party authorisation of important messages to the meters and system monitoring.

In October 2018 we set out the Government’s intention to take powers to set regulatory requirements for certain smart appliances beyond smart meters, based on principles including interoperability, data privacy, and cyber-security.\(^8\) Concurrently, the joint BEIS-DfT Office for Low Emission Vehicles (OLEV) intends to regulate on the cyber security of electric vehicle charge-points through powers in the Automated and Electric Vehicles Act (Section 15). OLEV will consult on implementing requirements that all charge-points sold or installed in the UK have smart functionality, and robust cyber security will be a key part of this. BEIS and OLEV have also worked with the British Standards Institution (BSI) to review the current landscape of technical standards relating to smart appliances; following this review we are working with industry to ensure that appropriate technical standards are brought forward.\(^10\)

---

\(^6\) https://www.gov.uk/government/collections/secure-by-design
\(^7\) https://www.gov.uk/government/publications/upgrading-our-energy-system-smart-systems-and-flexibility-plan
\(^8\) https://www.gov.uk/government/consultations/proposals-regarding-setting-standards-for-smart-appliances
Additionally, we have commissioned work to assess the magnitude of the smart energy cyber security risk from smart devices up to 2030 and we are using this work to inform our policies on cyber security in the emerging smart energy system.

The Office for Product Safety and Standards at BEIS is also commissioning research to investigate possible consumer safety aspects of certain internet connected domestic appliances.

Government departments are working in close cooperation with the NCSC as the relevant Government experts in this field, and we are engaging across the board with external stakeholders on our proposals, including via public consultations. Continuing to engage with these stakeholders, including consumer groups and academics, will remain an important area of focus going forward.

We hope this response is helpful to the work of your committee and reassures you that we are working together across Government with the aim to ensure the security of smart devices.

KELLY TOLHURST MP
Minister for Small Business, Consumers & Corporate Responsibility

MARGOT JAMES MP
Minister for Minister for Digital and the Creative Industries