Consumer smart-device security: moving towards increased regulation

Introduction

Following the conclusion of a public consultation process in 2019, the Department for Digital, Culture, Media & Sport ("DCMS") announced in early February 2020 that the UK government intends to draw up legislation aimed at ensuring that all consumer smart devices sold in the UK adhere to rigorous security requirements for the Internet of Things (IoT).

Conscious of the increasing number of consumer internet connected devices available on the UK market, the government has made it clear that it plans to take action to protect consumers from cyber- attacks and security breaches. In doing so, they've considered whether it's necessary to develop a robust regulatory framework governing the cybersecurity of consumer IoT devices.

A brief history

In March 2018, the DCMS published its "Secure by Design" report. This advocated the need for clear security guidelines and measures to be introduced to protect consumers, and for strong security features to be built into smart products at the product design stage. In particular, the report recommended a "fundamental shift in approach" by moving the burden away from consumers having to secure their IoT devices and placing it more squarely with manufacturers and others.

Following the report the DCMS published a voluntary "Code of Practice for Consumer IoT Security" in October 2018. This set out 13 outcome-focused "good practice" (but ultimately non-binding) guidelines for implementation by parties involved in the development and manufacture of consumer IoT to improve the cybersecurity of their devices.

In May 2019, the DCMS launched a public consultation advocating regulatory proposals for consumer IoT security. Stakeholders were invited to share their views on potential new mandatory industry requirements including a mandatory new labelling scheme for smart devices.

The result is the announcement of new legislation aimed at securing IoT devices from cyber-attacks, with manufacturers in particular required to apply various security controls to their devices.

The objectives of this legislation are to restore transparency within the UK market, ensure that manufacturers clearly communicate the security features of a device to consumers, and allow consumers to make more informed purchasing decisions. However a mandatory labelling scheme is not part of the current legislative proposals.

What will the new legislation look like?

The government has indicated that the new legislation will focus on three key security requirements for the manufacture and sale of IoT devices.

1. An end to default passwords: All consumer IoT device **passwords must be unique** and not resettable to any universal factory setting. Many IoT devices are sold by manufacturers with default usernames and passwords (for example, the username might be "admin" and the password "123456 ") with the expectation that consumers will change these prior to use. In practice, this often doesn't happen and the government's concern is that this leaves devices vulnerable to cyber-threats.
2. Nominating a point of contact for consumers: Manufacturers of consumer IoT devices must provide a **public point of contact** so that anyone can report a flaw or vulnerability, and these reports must be acted on in a timely manner.
3. Length of time of software support: Manufacturers of consumer IoT devices must **explicitly state** at the point of sale the minimum length of time for which devices will receive security updates (both online and in stores). The need for updates must be made clear to consumers and the updates should be easy to implement.

These three measures, aim to set a new standard for best-practice requirements for companies that manufacture and sell consumer smart devices.

Matt Warman, Digital and Broadband Minister at the DCMS, has said that the new legislation will "hold firms manufacturing and selling internet-connected devices to account and stop hackers threatening people's privacy and safety". He has also said that "it will mean robust security standards are built in from the design stage and not bolted on as an afterthought".

What does this mean for businesses?

It is currently expected that these requirements will apply to a wide range of consumer IoT devices, including:

- digital health products, smart watches and wearable health trackers;
- smart home assistants;
- connected home automation and safety products (eg smoke detectors, alarm systems and door locks);
- connected appliances (eg washing machines and fridges);
- connected children's toys and baby monitors and;
- smart cameras, TVs and speakers.

It's currently unclear how the three mandatory requirements are likely to be reflected in legislation, and when exactly the legislation will come into effect, but the UK government says it aims to deliver the legislation as soon as possible.

What is clear though is that, while the overarching aim of any new legislation will be to effectively protect consumers from the risks posed by cyber-threats, at the same time, this legislation will need to achieve a delicate balance between facilitating ease of implementation by businesses and supporting the long-term growth of IoT.

What about new labelling scheme?

Given the mixed responses and concerns raised during the consultation, it's likely to come as a relief to a number of businesses that the government has decided against moving ahead with its proposed mandatory security labelling scheme at this time. The objective of such a scheme would have been to communicate important security information to consumers and help consumers make more informed decisions when purchasing connected devices.

The government has deferred this plan for now, recognising the complexity of supply chain management and potential disruption to businesses as a result of affixing a label to physical products. Instead, it plans to obtain more stakeholder feedback and carry out further policy development in order to refine the proposals and determine the most appropriate way to communicate important security information and regulatory compliance to consumers.

Notably, it intends to examine an alternative option to the labelling scheme through which retailers would be responsible for providing information to the consumer at the point of sale (both online and in stores).

Comment

To ensure that it delivers a consistent, global approach to IoT security, the government has stated that it will:

- work with international partners and standards bodies, including the European Telecommunications Standards Institute (ETSI), in developing this legislation;
- encourage the adoption of the ETSI TS 103 645 standard, the first globally applicable industry standard on consumer IoT security, which establishes a security baseline for consumer smart devices and provides a basis for future IoT certification schemes;
- pursue a "staged approach" to regulation and, taking on board the responses received during the consultation, invite further stakeholder feedback to develop the regulatory proposals; it is hoped that this will provide businesses with reassurance and sufficient time to implement the proposals effectively and sustainably, and will enable regulation to keep pace with technological change and the cyber-threat landscape (importantly, this "staged approach" to regulation may involve the government mandating further security requirements for consumer IoT in the future, as and when appropriate) and;
- publish a final-stage regulatory impact assessment later in 2020, which we expect will shed further light on the government's regulatory proposals.

We are monitoring relevant developments in this area and encouraging manufacturers to keep an eye on further invitations from the government for stakeholder engagement, as their proposals take shape.

Lucy Ward
Consultant, London
T +44 20 7296 2898
lucy.ward@hoganlovells.com

Eshana Subherwal
Associate, London
T +44 20 7296 5443
eshana.subherwal@
hoganlovells.com