New smart devices cyber security laws one step closer

- Second reading of landmark Product Security and Telecoms Infrastructure Bill will prohibit UK sales of connectable digital products with poor cyber security

- Bill will speed up roll out of better mobile and broadband coverage by encouraging fairer and faster deals between landowners and mobile operators

MPs are set to debate a new world-leading law to keep consumers' phones, tablets, smart TVs, fitness trackers and other devices secure from cybercriminals.

It will place new cyber security requirements on the manufacturers and sellers of consumer tech which can connect to the internet or other devices.

Under the bill, easy-to-guess default passwords which come programmed into digital devices and present an easy target for cybercriminals will be banned.

Manufacturers will have to be more transparent to customers about the length of time products will receive security updates for connectable products and create a better public reporting system for vulnerabilities found in those products.

Failure to uphold the measures could result in fines □□of up to £10 million or four per cent global turnover, plus up to £20,000 per day in the case of an ongoing breach.

Ahead of introducing the bill in the House of Commons, Digital Secretary Nadine Dorries said:

> Whether it's your phone, smart speaker or fitness tracker, it's vital that these devices are kept secure from cybercriminals.
>
> Every product on our shelves has to meet all sorts of minimum requirements, like being fire resistant or a choking hazard and this is no different for the digital age where products can now carry a cyber security risk.
>
> We are legislating to protect people across the UK and keep pace with technology as it transforms our everyday lives.

The bill will give ministers powers to put new requirements on the manufacturers, importers and distributors of consumer tech devices. They include:

- Banning universal default passwords which are pre-set on devices – such as ‘password’ or ‘admin’ – and are an easy target for cyber criminals. Any preloaded product passwords will need to be unique and not resettable to universal factory settings.
- Requiring device manufacturers to be transparent with consumers about how long they’ll provide security updates for products so people are clearer when they buy. If a product will not receive any security updates the customer must be informed.
- Ensuring manufacturers have a readily available public point of contact to make it easier for software flaws and bugs to be reported.

□□The bill will also speed up the roll out of faster and more reliable broadband and mobile networks by making it easier for operators to upgrade and share infrastructure. The reforms will encourage quicker and more collaborative negotiations with landowners hosting the equipment with the aim of reducing instances of lengthy court action holding up the construction of infrastructure.

A regulator, to be announced at a later date, will oversee the new cyber security regime and ensure in-scope businesses comply with the measures in place. It will have the power to issue notices to companies requiring they comply with the security requirements, recall insecure products or stop selling or supplying them altogether.

The bill applies to ‘connectable’ products. This includes all devices which can access the internet such as smartphones, smart TVs, games consoles, security cameras and alarm systems, smart toys and baby monitors, smart home hubs and voice-activated assistants, and smart home appliances such as washing machines and fridges.

It also applies to products which can connect to multiple other devices but not directly to the internet. Examples include smart light bulbs, smart thermostats and wearable fitness trackers.

Matthew Evans, Director of Markets, techUK said:

> Industry has long supported the shared ambition to improve the cyber resilience of devices and has worked with DCMS across the Secure-By-Design agenda over the last five years.
>
> Most suppliers already adhere to the principles of the legislation and if implemented practically this will both protect consumers and ensure they have access to a wide range of connected devices.
>
> techUK also welcomes the Government’s efforts to reforming the Electronic Communications Code, which is essential to speeding up the rollout of gigabit and 5G infrastructure. Industry looks forward to further clarity on the amendments to the Code to ensure we can deliver the connectivity consumers and businesses need.

Hamish MacLeod, Chief Executive at Mobile UK, said:

> Mobile operators need a robust legal framework to meet the UK’s connectivity ambitions. The Electronic Communications Code as it stands is not working.
>
> Mobile operators welcome the measures within this Bill that will tackle this and will engage closely with Parliament to ensure that it delivers on this objective.

ENDS

Notes to Editors: