Guidance

The Product Security and Telecommunications Infrastructure (PSTI) Bill – product security factsheet

Product security factsheet accompanying the Product Security and Telecommunications Infrastructure Bill, outlining the problems the Bill will address and how.

From:
Department for Digital, Culture, Media & Sport (/government/organisations/department-for-digital-culture-media-sport)
Published
24 November 2021
Last updated
1 December 2021 —

Contents

What we are doing

Currently, connectable consumer products, such as smart TVs, smartphones and internet connected speakers, must comply with existing regulation to ensure that they will not directly cause physical harm from issues such as overheating, environmental damage or electrical interference. They are not, however, regulated to protect consumers from *cyber* harm such as loss of privacy and personal data. To close this regulatory gap, the Bill will:

- require manufacturers, importers and distributors to ensure that minimum security requirements are met in relation to consumer connectable products that are available to consumers; and
- provide a robust regulatory framework that can adapt and remain effective in the face of rapid technological advancement, the evolving techniques employed by malicious actors, and the broader international regulatory landscape.

The threats posed by insecure consumer connectable products

Consumer connectable products, such as Internet of Things (IoT) products, can be compromised at scale through a distributed denial-of-service (DDoS) attack, which uses a network of connected online products, known as a 'botnet', to attack infrastructure or networks. In 2016, malicious actors hacked into 300,000 products such as routers and smart cameras, as part of the 'Mirai' attack and used the products' collective computing power to attack major internet platforms and services, leaving much of the US East Coast without internet.

This form of attack will only become more common as adoption of these products increases, demonstrated during the Covid-19 pandemic. Kaspersky research (https://iottechnews.com/news/2021/sep/07/kaspersky-attacks-on-iot-devices-double-in-a-year/) shows that there were 1.5 billion attacks against IoT products in the first six months of 2021, which represented a 100% increase since the same period in 2020.

This is just one form of harm that can be caused by compromised consumer connectable products. Once compromised, these products can also:

Enable wider attacks: The connectable product with the lowest standard of security represents the most-likely entry point for an attacker to access data across the network. In 2018, attackers were able to compromise a connected thermometer in a fish tank that had a default password. The fish tank was in the lobby of a US casino, and attackers used this vulnerability to enter the network and access sensitive details, such as bank details.

Cause harm to the consumer: Given the growing adoption of devices with microphones and cameras embedded within them, compromising these can also be used for fraud. In Singapore in 2020, private security cameras were compromised and footage was shared with adult websites. In addition, devices with heating elements, such as white goods, or locking mechanisms, such as smart door locks, can cause physical harm, including domestic fires (https://www.which.co.uk/news/2020/10/cheap-smart-plugs-could-expose-you-to-hackers-or-even-cause-a-fire/), or be used by perpetrators of domestic violence (https://www.bbc.com/future/article/20200511-how-smart-home-devices-are-being-used-for-domestic-abuse).

The problem with the consumer connectable product market

Currently, the consumer connectable product market disincentivises the adoption of basic security features, since consumers overwhelmingly assume that products are already secure.

According to research (https://www.statista.com/statistics/1107269/average-number-connected-devices-uk-house/), the average UK household has nine consumer connectable products, and this is continuing to grow, with 67% of UK households purchasing an average of two additional products in light of Covid-19 (Ipsos Mori, 2021 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/978685/Consumer_Attitudes_Towards_IoT_Security_-_Research_Report.pdf)). Whilst consumers overwhelmingly expect that their connectable products are secure, fewer than 20% take action to address this (or know how to). This is understandable, given that few products have been found to come with information about security software and how often the software will be updated to mitigate attacks.

In part, this is because cybersecurity continues to be an afterthought for many manufacturers of connectable products, and consumers often expect that a product is secure. In a 2020 report by the Internet of Things Security Foundation, only 1 in 5 manufacturers maintained systems for the disclosure of security vulnerabilities. This threatens citizens' privacy, the security of a network, and adds to the growing risk of harms.

How we are going to do it

The range of consumer connectable products available is fast evolving. To ensure security requirements remain effective, up to date with evolving technologies, and consistent with international best practice, the Bill provides for security requirements to be specified by regulation.

The security requirements, to be set out in regulations, will:

- **Ban default passwords**. Products that come with default passwords are an easy target for cyber criminals.
- **Require products to have a vulnerability disclosure policy**. Security researchers regularly identify security flaws in products, but need a way to give notice to manufacturers of the risk they have identified, so that they can enable the manufacturer to act before

criminals can take advantage. The Bill will provide measures to help ensure any vulnerabilities in a product are identified and flagged.

- **Require transparency about the length of time for which the product will receive important security updates.** Consumers should know if their product will be supported with security updates, and if so, what the minimum length of time is that they can expect that support to continue.

Security requirements set out under this regime must be complied with by the manufacturers, importers and distributors of consumer connectable products. The Bill will also place duties on these persons to ensure a product is accompanied by a statement of compliance and to take action where there has been a compliance failure.

Products that will be included in the Bill

The Bill mandates that security requirements be complied with in relation to all consumer connectable products, though the Secretary of State for Digital, Culture, Media and Sport will have the ability to designate exceptions where appropriate in the future.

A consumer connectable product is an internet-connectable or network-connectable product. The government has stated that the security requirements will apply in relation to products including:

- smartphones
- connected cameras, TVs and speakers
- connected children's toys and baby monitors
- connected safety-relevant products such as smoke detectors and door locks
- Internet of Things base stations and hubs to which multiple devices connect
- wearable connected fitness trackers
- outdoor leisure products, such as handheld connected GPS devices that are not wearables
- connected home automation and alarm systems
- connected appliances, such as washing machines and fridges
- smart home assistants

How long manufacturers, importers and distributors will have to become compliant with this new legislation

The government is committed to ensuring that businesses are given an appropriate amount of time to adjust their business practices before instances of non-compliance are actively enforced against. Following Royal Assent of the Bill, the government will provide at least 12 months notice to enable manufacturers, importers and distributors to adjust their business practices before the legislative framework fully comes into force.

How this approach to legislation has developed

This Bill has been developed following a number of publications and rounds of engagement, including the Code of Practice (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf), a consultation and a call for views. DCMS has worked closely with industry, the National Cyber Security Centre, academia, standards bodies and representatives from other countries to develop our approach.

Our consultation outlined a number of options on how to translate the Code into enactable regulation. The response to this consultation (https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security) indicated clear support to mandate important security requirements through legislation, with support for the 'top three' principles as the initial baseline. Our 2021 government response (https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation) represented the next phase of this approach, outlining the scope of the legislation and confirming that compliance with standards specified by the Secretary of State can be considered equivalent to the implementation of security requirements, where appropriate.

How the consultation on regulatory proposals on consumer IoT security helped to shape the government's plans

Since the government first published its Code of Practice (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf) in 2018, it has intentionally adopted a consultative and collaborative approach with industry, academia, subject-matter experts, and other key stakeholders. A primary aim of this approach has been to ensure that interventions in this space are maximally effective whilst minimising impact on organisations involved in the manufacture and distribution of consumer connectable products.

Published 24 November 2021
Last updated 1 December 2021 + show all updates

1. 1 December 2021
   Added PDF versions of factsheets.
2. 24 November 2021
   First published.

Related content

- Product Security and Telecommunications Infrastructure (PSTI) Bill: Factsheets (/government/collections/the-product-security-and-telecommunications-infrastructure-psti-bill-factsheets)
- Secure by Design (/government/collections/secure-by-design)
- Secure by Design report (/government/publications/secure-by-design-report)
- Summary literature review on IoT security (/government/publications/summary-literature-review-on-iot-security)
- Regulating consumer smart product cyber security - government response (/government/publications/regulating-consumer-smart-product-cyber-security-government-response)

Collection

- Product Security and Telecommunications Infrastructure (PSTI) Bill: Factsheets (/government/collections/the-product-security-and-telecommunications-infrastructure-psti-bill-factsheets)

Explore the topic

- Communications and telecomms (/business/communications-and-telecomms)