



Department for
Digital, Culture
Media & Sport

DCMS Consultation: Regulatory proposals for Consumer IoT security

What is consumer IoT?



We have defined consumer IoT as **products that are connected to the internet and/or home network.**

A non-exhaustive list of examples includes:

- Connected children's toys and baby monitors
- Connected safety-relevant products such as smoke detectors and door locks
- Smart cameras, TVs and speakers
- Wearable health trackers
- Connected home automation and alarm systems
- Connected appliances (e.g. washing machines, fridges)
- Smart home assistants



Prevalence of consumer IoT



A 2018 survey of 3,750 consumers by Ofcom found that the most prevalent internet connected devices in the UK include:

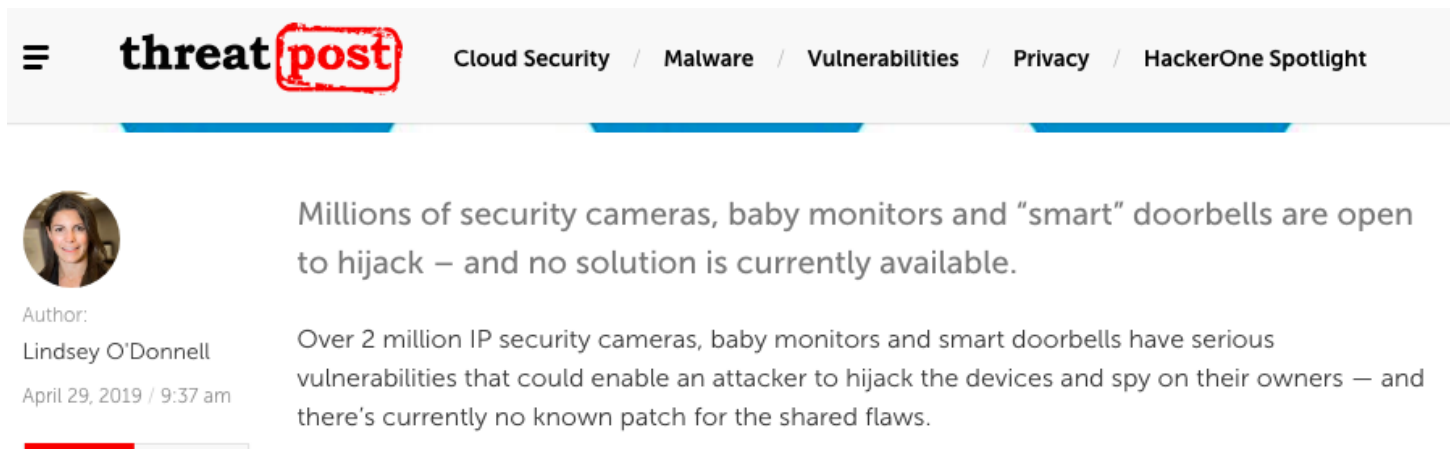
- Smart TVs – in 42% of households surveyed
- Wearable devices – in 20% of households, including fitness trackers that monitor factors such as physical activity and location
- Smart speakers – in 13% of households, which can react to voice commands and be used to control other devices.

UK household ownership of smart devices likely to rise from approximately 10 devices per household to 15 devices over the next 12 months.



Insecure IoT products on the market

- Large numbers of these devices are sold to consumers without even basic cyber security provisions.
- Insecure consumer IoT can lead to people's privacy and safety being undermined
- Consumers cannot differentiate between products with good or bad security.




Security is becoming increasingly important to consumers

2019 Harris Interactive Survey of 6,482 participants:

- 49% consider security features to be **important in their decision-making process** when they're buying smart devices behind cost (76%) and functionality (72%).
- 72% **believe that security features are already built into devices** when they are placed on the market, particularly in the case of big name brands.
- 59% of participants were **willing to pay a premium** of 5% for a smart product with a security label over an equivalent product without one. This drops to 40% of participants at a price premium of 10%.



Consultation launch 1st May 2019



PEN TEST PARTNERS
Penetration testing and security services

+44 20 3095 0500

About Services Events

So, the UK looks like it will be getting the best IoT legislation in the world, starting with a coherent plan for connected devices:

- Basic cyber security features to be built into products
- Consumers will get better information on how secure their devices are
- Consultation now launched ahead of potential legislation

the Guardian

Founded by readers

Subscribe →

Search jobs Dating Sign in Search

UK edition

Opinion Sport Culture Lifestyle More

Football UK politics Environment Education Society Science Tech Global development Cities Obituaries

Smart devices may have to carry labels showing how secure they are

Ministers consider proposals aiming to help consumers identify which products are more and which are less secure

Advertisement

Find your place today →

BBC ddd

News Sport Weather iPlayer Sounds

NEWS

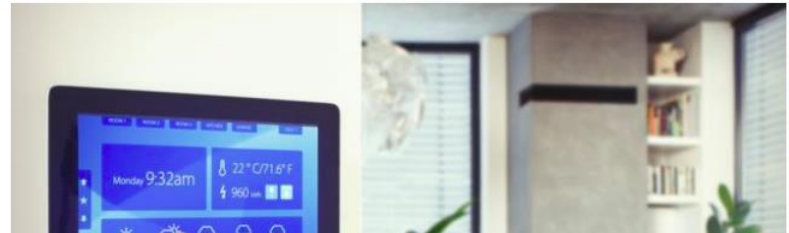
Home UK World Business Politics Tech Science Health Family & Education

Technology

Plan to secure internet of things with new law

1 May 2019

Facebook Messenger Twitter Email Share



Computer Weekly.com

IT Management Industry Sectors Technology Topics

Search Computer Weekly

UK gears up for new laws on IoT security

The UK plans to introduce measures to require that basic cyber security features are built into internet-connected devices

What have we published as part of the consultation?

<https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security>

- Consultation document (including draft labelling icons)
- Consultation Stage Regulatory Impact Assessment
- Labelling survey research findings (Harris Interactive)
- IoT Labelling online study (Make It Clear)



The screenshot shows the GOV.UK website interface. At the top is the GOV.UK logo and a search bar. Navigation links include Departments, Worldwide, How government works, Get involved, Publications, Consultations, Statistics, and News and communications. The breadcrumb trail reads: Home > Business and industry > Business regulation > Consumer rights and issues. The main heading is 'Open consultation' followed by 'Consultation on regulatory proposals on consumer IoT security'. Below this, it states 'Published 1 May 2019' and 'From: Department for Digital, Culture, Media & Sport'. A blue box on the left contains the 'Summary' section, which describes the consultation on regulatory proposals for IoT security and notes that the consultation closes at 11:59pm on 5 June 2019. On the right, under 'Related content', there is a link to a collection titled 'Secure by Design'.



Our approach to regulation

- We recognise industry concerns that mandating all 13 requirements of our Code of Practice for Consumer IoT Security at once would immediately place a heavy burden on manufacturers and retailers (e.g extensive international supply chains, non-compliant stock in warehouses).
- This burden would be felt more by smaller organisations, and could dampen innovation.



As part of what we are consulting on - **what** do we want to mandate?



Practical solution: the top 3 as a minimum baseline

- Sought to identify a practical solution that could be:
 - implemented sooner
 - could protect consumers and the wider economy
 - ensure growth across the sector.
- Balancing the need to deliver an **effective minimum baseline** that protects consumers whilst also minimising the additional burden on industry (including retailers). .
- **Our proposal - the focus should be placed on aspects of the ‘top three guidelines’ within the Code of Practice for Consumer IoT Security.**



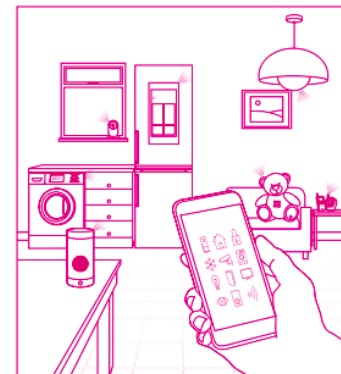
Aspects of the 'top three guidelines'



1. IoT device passwords must be **unique** and not resettable to any universal factory setting (i.e. no default passwords)
2. Manufacturers of IoT devices need to provide a **public point of contact** as part of a vulnerability disclosure policy
3. Manufacturers of IoT devices need to **explicitly state the minimum length of time** for which the product will receive security updates


Department for
Digital, Culture,
Media & Sport

Code of Practice for Consumer IoT Security



October 2018



Benefit of using these 3 requirements as a baseline for our regulatory options

- From an enforcement perspective, **easier to test compliance** - products (and companies) either meet these clearly set out requirements or they do not.
- Meeting these practical and implementable measures would protect consumers from many of the most significant and numerate risks (e.g. Mirai botnet attack in 2016).
- Restore **transparency** in the sector and allow consumers to identify products that meet basic security provisions over the course of time that they intend to use them for.
- Vulnerability disclosure needs a **clear feedback mechanism** to operate - between the security research community and manufacturers.

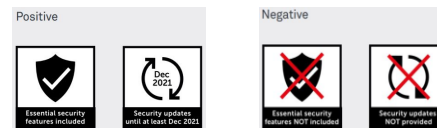


We are not only consulting on **what** we want to mandate, but **how** to deliver it.



Regulatory options *(within consultation document)*

Option A: Mandate retailers to **only sell consumer IoT products that have the IoT security label**, with manufacturers to self declare and implement a security label on their consumer IoT products.



Option B: Mandate retailers to **only sell consumer IoT products that adhere to the top three guidelines**, with manufacturers to self declare that their consumer IoT products adhere to the top three guidelines of the Code of Practice for IoT Security and the ETSI TS 103 645.



Option C: Mandate that retailers only sell consumer IoT products **with a label that evidences compliance with all 13 guidelines** of the Code of Practice, (and ETSI TS) with manufacturers expected to self declare and to ensure that the label is on the appropriate packaging



Why focus on retailers?

2019 Harris Interactive Survey of 6,482 participants:



- Retailer websites ranked by 37% of participants as the main source for purchasing smart devices, following by retailer stores (33% of participants).
- Those aged 65+ are significantly more likely than any other age group to visit a traditional retail store when purchasing smart devices (46% ranked retailer stores as their main source)
- Purchasing directly from manufacturers (either online or in-store) is less common.

Most manufacturers are abroad and outside of the UK's legal jurisdiction.



Why is the label an option?

- Consumers are currently expected to conduct pre-purchase research or review product information in store to find information on the security features of different IoT products before deciding which device to purchase.
- Many consumers do not have the technical expertise to know what security features should be built into their devices.
- Significant amount of manufacturers do not provide this information online or within product documentation.
- The labelling scheme is designed to help consumers make more informed decisions when purchasing consumer IoT devices.



The label option: positive vs negative

- Mandate retailers to only sell products that either contain a **positive or negative** label.
- Based on aspects of the 'top three' guidelines
- Clearly signposted to consumers both on physical products and on product websites.

Positive



Negative



Why these specific designs?

- Compiled extensive evidence to inform our work including a literature review, two consumer surveys and a study to evaluate what security information is provided with devices.
- Question in consumer survey asked if the icons were suitable for the proposed criteria - 92% stated that the shield and arrows were the best designs for the label. The highest alternative option (a padlock) was suggested by less than 1%.
- Considered creating unique shapes for each icon, however this would create strong challenges in explaining the meaning of the label to UK consumers.
- Aware of trademark requirements surrounding the use of generic icons and currently discussing this with trademark specialist lawyers.



How to qualify for a positive product label

- Retailers will need to ensure that the product's they are selling:
 - have **unique passwords** that are not resettable to any universal factory setting;
 - explicitly state the **minimum length of time** for which the device will receive security updates (Dec 2021 has been used as an example).
- Before the product can be sold, retailers need to ensure that the manufacturer of the product has a **point of contact** in place within the manufacturer's organisation to receive vulnerabilities reports from the public.

Positive



“Grace period” before legislation comes into force

- Important that industry has sufficient time to make required changes within their organisations and supply chains.
- Post-consultation, we will set out our confirmed regulatory next steps (including the **what** and the **how**)
- Later this year, we will separately launch the label as a voluntary scheme (and ensure consistency with whichever regulatory option we proceed with).
- Voluntary scheme will run for at least 2 years.



International Approach



- Want to ensure that there is a cohesive global approach to IoT security to encourage a level playing field.
- We are leading efforts and collaborating with international governments and industry partners in IoT security to ensure that guidelines from the Code drive global alignment across the global IoT supply chain (e.g. ETSI Technical Specification 103645).
- There are many international activities across HMG that also engage with on consumer IoT - e.g. BEIS Consumer and Competition Policy team represent the UK Government in working groups for various European Commission directives, such as the Sales & Goods Directive and Digital Content Directive.



What do consumers think of the regulatory plans?

Harris Interactive undertook a survey of 1,406 UK consumers following the launch of the consultation:

- 62% are concerned that their Smart devices are a target for cyber-attackers.
- 77% agree these plans are a step in the right direction.
- 65% would prefer mandated label option - ban retailers from selling devices without appropriate labels.
- 74% agree label will help them make more informed decisions.



How can you respond to the consultation?

- 5th June deadline (11.59pm)!
- Easiest way is to send formal responses to: securebydesign@culture.gov.uk



Consultation feedback: What happens with it?

- Not a tick box exercise.



- We will review and analyse every piece of feedback with technical experts, legal experts and relevant policy experts across HMG.
- Following this exercise - we will seek to follow up with specific respondents if necessary.
- Will publish consultation response later this year setting out our approach going forward.
- Will use feedback to inform voluntary labelling scheme.



Consultation questions set out in the document



Regulatory approach

- 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?
- 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?



Labelling scheme



- Do you agree with the use of the security label (positive and negative) to communicate these requirements to consumers?
- Do you agree with the wording of the labelling design?
- 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)?
- How best to approach issues associated with existing consumer IoT products on the market that, under these new proposals, will not have a label?



Impact of our proposals?

We welcome your views on these, Including:

- Direct costs
- Impact on competition
- Costs of cyber breaches to IoT consumers
- Number of manufacturers/retailers that sell these products in UK market
- Hours taken for companies to familiarise with legislation
- Costs of label (incl passing on costs to consumers)
- Cost to your business of implementing 3 v 13 guidelines of the DCMS Code of Practice
- Cost to businesses of implementing these regulatory approaches within the secondary market.
- How often do people upgrade their IoT devices?



Enforcement

- Do you have a view on how best to enforce the requirements set out in the regulatory options?
- Which UK agency is best placed to undertake enforcement?
- What additional penalties would need to be set out to ensure that companies correctly use the labels?



Questions for businesses (as users of IoT)

- How embedded are consumer IoT products in your businesses (securing IoT devices could impose further costs on business as they replace the products, but could also have benefits from reduced breaches)?
- What types of businesses use consumer IoT more? (Sector and size) Is it the more technical firms, or is it small businesses?
- How do businesses use consumer IoT in their day to day operations? E.g. in operations, production, communications etc.
- Do businesses consider the security of the consumer IoT products they use in their business as part of their risk management? Would they find a label beneficial to this process?
- Would they pay more for a secure IoT device as part of their equipment costs? To what extent would they pass on this cost to the consumer of their goods?

