HOUSE OF COMMONS LIBRARY

DEBATE PACK

Number CDP 2019/0221, 2 October 2019

Regulating the Internet of Things

By Suzanna Hinson
Nikki Sutherland

This pack has been prepared ahead of the debate on regulating the Internet of Things to be held in Westminster Hall on Thursday 3 October 2019 at 3pm. The debate will be opened by Chi Onwurah MP.

Contents

1. Regulating the Internet of Things

1.1 Background

The Internet of Things (IoT) refers to a network of connected devices that talk directly to each other without needing to interact with human beings.

IoT devices (sometimes referred to as 'smart' devices) use software and hardware to process data, and typically include:

- **Sensors**, such as cameras, microphones or temperature sensors that enable data to be collected from the environment or user.
- **Actuators**, which control a mechanism in response to a signal, such as turning on a radiator or unlocking a door.
- **A network connection**, to a network like the internet, often via wireless technology such as Wi-Fi, 4G, Bluetooth, or Zigbee (a low-power radio wave network). This enables data to be communicated between devices, as well as to data centres and cloud platforms where data are often remotely processed or stored. 5G is likely to be the networking technology that supports the Internet of Things in the future, due to its low latency and capacity to support many devices at one time.

Many devices are controlled via software on another device, such as a smartphone. Some devices, such as smart home systems, can be used to control multiple other devices. This enables devices to operate together, for example lightbulbs may be switched on when a sensor detects movement

Examples of possible uses of IoT devices are numerous and encompass a vast range of sectors. Some of these technologies already exist or are in development, some are not. Examples suggested to date include smart energy meters, wearable health sensors, driverless cars, smart bins that send warnings when they are full, and smart fridges that can tell you how much food you have left or even order replacement items when you run out.

More information is available in the POSTnote on Cyber security for consumer devices. More information about 5G is available in the Library briefing paper on 5G.

1.2 Government policy

In May 2019, the Government released a consultation on regulatory proposals on consumer IoT security. The consultation said the Government wanted to better protect homes and the wider economy from the risks of a lack of cyber security provisions in consumer IoT devices:

> As the technological advances of the 21st century continue to accelerate, consumers are bringing more and more 'smart' devices

> (i.e. consumer IoT products) into their homes, such as smart TVs, internet connected toys, smart speakers and smart washing machines. The Internet of Things (IoT, also known as 'internet-connected' or 'smart' products) is already being used across a range of industries and it is delivering significant benefits to the lives of its users.
>
> In the future, we expect an ever increasing number of more developed consumer Internet of Things products and services. These devices will be able to anticipate and meet their users' needs and will be able to tailor information specifically to them across everything from home energy to security. This will offer users the opportunity to live more fulfilling lives; saving time, effort and money.
>
> As with all new technologies, there are risks. Right now, there are a large number of consumer IoT devices sold to consumers that lack even basic cyber security provisions. This situation is untenable. Often these vulnerable devices become the weakest point in an individual's network, and can undermine a user's privacy and personal safety. Compromised devices at scale can also pose a risk for the wider economy through distributed denial of service (DDOS) attacks such as Mirai Botnet in October 2016.

The consultation follows the government's voluntary Secure by Design Code of Practice for consumer IoT security launched in 2018. The Code advocates for stronger cyber security measures to be built into smart products from the design stage and has been adopted by numerous stakeholders. The proposals in the consultation focus on mandating the top three security requirements set out in this code, including:

1. IoT device passwords must be unique and not resettable to any universal factory setting.
2. Manufacturers of IoT products provide a public point of contact as part of a vulnerability disclosure policy.
3. Manufacturers explicitly state the minimum length of time for which the device will receive security updates through an end of life policy.

The consultation also proposed a new labelling scheme that would mean retailers could only sell products with a label that tells consumers how secure their IoT products are.

The consultation closed on 5 June 2019. In September 2019, in response to a parliamentary question on the proposals, the Government said they will publish a response in due course:

> We consulted on our core proposal to create a minimum cyber security baseline for consumer IoT products, and how best to implement this, mindful of the risk of dampening innovation and avoiding placing a sizeable burden on UK manufacturers and retailers.
>
> Following the conclusion of the consultation, we are now working through the feedback to refine our policy proposals and we will publish a formal public response in due course which will outline the Government's proposed next steps.

2. News items

BBC News Online

Plan to secure internet of things with new law

1 May 2019

https://www.bbc.co.uk/news/technology-48106582

Telegraph

Data now as important a commodity as oil, leading QC says

7 January 2019

https://www.telegraph.co.uk/news/2019/01/07/data-now-important-commodity-oil-leading-qc-says/

Independent

Children's toys and baby monitors can be taken over by hackers, security services warn

28 October 2018

https://www.independent.co.uk/news/uk/home-news/smart-toys-baby-monitors-internet-connected-hackers-cyber-attacks-guidance-ncsc-a8605346.html

FT

Manufacturers face tighter rules on devices

17 October 2018

https://www.ft.com/content/d21079b0-8a79-11e8-affd-da9960227309

Computer Weekly

IoT firms sign up to UK security code of practice

15 October 2018

https://www.computerweekly.com/news/252450588/IoT-firms-sign-up-to-UK-security-code-of-practice

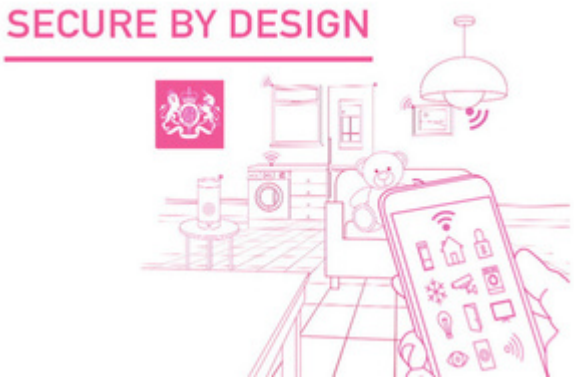
3. Press releases

Department for Digital, Culture, Media and Sport

Plans announced to introduce new laws for internet connected devices

1 May 2019

Plans to ensure that millions of household items that are connected to the internet are better protected from cyber attacks have been launched



- 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

Plans to ensure that millions of household items that are connected to the internet are better protected from cyber attacks have been launched by Digital Minister Margot James.

Options that the Government will be consulting on include a mandatory new labelling scheme. The label would tell consumers how secure their products such as 'smart' TVs, toys and appliances are. The move means that retailers will only be able to sell products with an Internet of Things (IoT) security label.

The consultation focuses on mandating the top three security requirements that are set out in the current 'Secure by Design' code of practice. These include that:

- IoT device passwords must be unique and not resettable to any universal factory setting.
- Manufacturers of IoT products provide a public point of contact as part of a vulnerability disclosure policy.
- Manufacturers explicitly state the minimum length of time for which the device will receive security updates through an end of life policy.

Following the consultation, the security label will initially be launched as a voluntary scheme to help consumers identify products that have basic security features and those that don't.

Digital Minister Margot James said:

> Many consumer products that are connected to the internet are often found to be insecure, putting consumers privacy and security at risk. Our Code of Practice was the first step towards making sure that products have security features built in from the design stage and not bolted on as an afterthought.
>
> These new proposals will help to improve the safety of Internet connected devices and is another milestone in our bid to be a global leader in online safety.
>
> National Cyber Security Centre (NCSC) Technical Director, Dr Ian Levy said:
>
> Serious security problems in consumer IoT devices, such as pre-set unchangeable passwords, continue to be discovered and it's unacceptable that these are not being fixed by manufacturers.
>
> This innovative labelling scheme is good news for consumers, empowering them to make informed decisions about the technology they are bringing into their homes.

CEO of techUK Julian David said:

> techUK welcomes the publication of the Government's consultation on regulatory next steps for consumer IoT. This follows the Government's voluntary Secure by Design Code of Practice for consumer IoT security launched last year, which techUK supported. The Code advocates for stronger cyber security measures to be built into smart products right from the design stage.
>
> We are pleased that the security requirements outlined in the consultation are consistent with the Secure by Design Code of Practice and key industry standards that already exist for consumer IoT devices. This is an important first step in creating flexible and purposeful regulation that stamps out poor security practices, which techUK's research shows can act as significant barriers on the take-up of consumer IoT devices.
>
> The proposals set out have the potential to positively impact the security of devices made across the world and it is good to see the Government is working with international partners to ensure a consistent approach to IoT security. techUK looks forward to responding to this consultation on behalf of our members.

The consultation follows the government's voluntary Secure by Design Code of Practice for consumer IoT security launched last year. The Code advocates for stronger cyber security measures to be built into smart products right from the design stage, and has already been backed by Centrica Hive, HP Inc Geo and more recently Panasonic.

The proposals come a day after Margot James held a roundtable on IoT security with global technology companies. As a result Amazon, Philips, Panasonic, Samsung, Miele, Yale and Legrand affirmed their commitment to taking steps to ensure that effective security solutions are being implemented across IoT products on the market.

The Government is working with international partners to ensure that the guidelines drive a consistent approach to IoT security. The proposals set out in the consultation have the potential to impact security of devices made across the world to meet the UK's future standards.

Alternative options to the label that Government are also consulting on would be to mandate retailers to not sell any products that do not adhere to the top three security requirements of the Code.

Notes to editors:

The consultation document will be available on the Government's Secure by Design pages and is open for 5 weeks. It has been published alongside a consumer survey report which tested various label designs with 6,482 UK consumers as part of helping to create a labelling scheme that was backed by evidence.

The public consultation is part of a wider evidence based approach, to create regulatory proposals for consumer IoT products.

In February, ETSI, the European Standards Organisation, launched Technical Specification 103 645, the first globally-applicable industry standard on the cybersecurity of internet-connected consumer devices. TS 103 645 builds on the Code of Practice for Consumer IoT Security, but has been developed for wider European and global needs. Cybersecurity Tech Accord signatories endorsed the ETSI TS 103 645 in March 2019.

Stakeholders can submit feedback to the consultation via securebydesign@culture.gov.uk

The UK Government has also updated its guidance for consumers ('Smart devices: using them safely in your home') - the guidance has been published on DCMS and NCSC's website.

The Industrial Strategy sets out a long term plan to boost the productivity and earning power of people throughout the UK. It sets out how we are building a Britain fit for the future – how we will help businesses create better, higher-paying jobs in every part of the UK with investment in skills, industries and infrastructure.

The Minister made the announcement at the PETRAS/IET Living in the Internet of Things Conference (1-2 May 2019), at the Institution of Engineering and Technology, Savoy Place.

Innovate UK and UK Research and Innovation

Improve cyber security in the Internet of Things: apply for funds

4 February 2019

Up to £6 million funding to support new ideas that can help keep connected devices and applications safe and secure.

The competition will develop new products and services that tackle cyber security in the Internet of Things.

Connected devices and sensors in our homes and workplaces – known as the Internet of Things (IoT) – offer huge potential for improving how we live and move around.

We can measure health data, travel habits and energy use, predict demand for public services and support planning and management of critical national infrastructure.

But as more devices become connected, the more vulnerable they are to sophisticated cyber security threats. This becomes even more important as critical applications for the IoT emerge.

Innovate UK has up to £6 million to invest in organisations with ideas that address industry-focused cyber security-related challenges.

The investment forms part of the UK Research and Innovation Strategic Priorities Fund, which supports the highest priorities identified by researchers and businesses.

Find out more about the Strategic Priorities Fund.

It is part of a set of measures by UK government to build increased security and protections into digital devices and online services. As well as this programme, this includes an up to £70 million investment through the Industrial Strategy Challenge Fund to tackle digital security by design.

Read the announcement.

More resilient, intelligent systems

The competition aims to join up the UK's research base with industry to transfer knowledge and develop new products and services that tackle cyber security in the IoT.

Projects should include artificial intelligence or machine learning and have a clear plan for commercialisation.

They should focus on at least 1 of the following:

- operational resilience technologies that can protect and recover data
- intelligent control systems for industry, commercial and public sector buildings
- protection of people living in digital homes and their smart systems

Projects could also look at complementary technologies, such as distributed ledger technologies that support the sharing of data across multiple locations, or 5G mobile networks.

Competition information

- the competition opens on 18 February 2019 and the deadline for applications is at midday on 1 May 2019
- UK-based businesses of any size can lead a project, working with other businesses, research organisations, public sector

organisations or charities. Collaborations should involve at least one academic partner and one small or medium-sized enterprise

- businesses could receive up to 70% of their project costs
- total eligible project costs can be between £2.5 million and £4 million
- projects must start by 1 December 2019 and can last between 18 and 24 months
- projects that pass the written application stage will be invited to an interview panel between 1 and 5 July 2019 to present their ideas

Find out more about this competition and apply.

4. Parliamentary material

Lords Committee report and debate

Lords debate: Regulating in a Digital World (Communications Committee Report)

HL Deb 12 June 2019 | Vol 798 c477-

http://bit.ly/2oWz2iT

House of Lords Communications Committee report Regulating in a digital world HL299 published 9 March 2019

Government response

POSTnote: Cyber Security of Consumer Devices

Parliamentary Office of Science and Technology: Cyber Security of Consumer Devices

PQs

Internet: Data Protection

Asked by: Onwurah, Chi

To ask the Secretary of State for Digital, Culture, Media and Sport, what steps she is taking to mitigate the risks of the internet of things surveillance raised by the Prime Minister in his speech to the UN General Assembly on 24 September 2019.

To ask the Secretary of State for Digital, Culture, Media and Sport, with reference to the Prime Minister's speech to the UN Assembly on 24 September 2019, what steps she is taking to develop a data framework for the internet of things to regulate the use of that data by companies.

Answering member: Nigel Adams | Department: Department for Digital, Culture, Media and Sport

The Government takes the protection of personal data extremely seriously. The Data Protection Act (DPA) 2018 and the GDPR are in place to ensure that organisations who collect and use data do so lawfully and transparently.

The rules included in the DPA 2018 and the GDPR impose strict obligations on organisations to process people's data fairly and lawfully and to ensure that any data collected is held securely. Organisations must also ensure they have a legal basis for processing data, are clear

and transparent about how personal data will be handled, and ensure that the data is processed in a way which individuals would expect. Organisations that fail to comply may be subject to enforcement action by the Information Commissioner's Office.

We have also issued a Code of Practice for organisations involved in the development, manufacturing and retail of products linked to the 'Internet of Things' to ensure that products are designed securely and keep consumers safe. In parallel, we have published consumer guidance to raise public awareness about setting-up, managing and improving the security of their consumer devices. The code of practice and guidance for consumers can be viewed at the following links:

https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security

https://www.gov.uk/government/publications/secure-by-design/consumer-guidance-for-smart-devices-in-the-home

The Government also set up the Centre for Data Ethics and Innovation last year to ensure that data and AI-driven innovations continue to deliver maximum benefits for society. The UK already benefits from a world-class regulatory regime, and the Centre will build on this by providing independent, expert advice on responding to the rapidly evolving way in which data is impacting our lives.

HC Deb 01 October 2019 | PQ 291016; PQ 291011

Internet: Safety

Asked by: Onwurah, Chi

To ask the Secretary of State for Digital, Culture, Media and Sport, pursuant to the Answer of 23 April 2019 to Question 242826, what the timescale is for the publication of the consultation on regulatory proposals regarding consumer Internet of Things security.

Answering member: Nigel Adams | Department: Department for Digital, Culture, Media and Sport

In May 2019 we launched a public consultation on our regulatory proposals which concluded on the 5th June 2019.

We consulted on our core proposal to create a minimum cyber security baseline for consumer IoT products, and how best to implement this, mindful of the risk of dampening innovation and avoiding placing a sizeable burden on UK manufacturers and retailers.

Following the conclusion of the consultation, we are now working through the feedback to refine our policy proposals and we will publish a formal public response in due course which will outline the Government's proposed next steps.

HC Deb 02 September 2019 | PQ 279001

Wearable Technology

Asked by: Lord Wasserman

To ask Her Majesty's Government whether the (1) sale, and (2) use, of wearable GPS tracking devices for (a) use in connection with the care of dementia patients, and (b) other purposes, is regulated; and if so, by whom.

Answering member: Baroness Barran | Department: Department for Digital, Culture, Media and Sport

The sale of wearable GPS tracking devices, including where they are sold to assist with the care of dementia patients, is subject to UK consumer protection legislation. This legislation includes the Consumer Rights Act 2015 under which all goods and services must be of satisfactory quality and fit for purpose.

In addition, all personal data collected by GPS devices is subject to the EU General Data Protection Regulation (GDPR) and the Data Protection Act 2018 which is regulated by the Information Commissioner's Office (ICO). This legislation provides that any data collected must be processed transparently, fairly and for legitimate purposes. Companies developing new technologies which are likely to result in a risk to the rights and freedoms of data subjects are also required to complete a Data Protection Impact Assessment before the processing begins. In these instances, the company will be required to consult the ICO if their assessment indicates the processing would result in a high risk in the absence of any mitigating actions.

As GPS tracking is used for a wide range of applications, there are also some cases where other regulations may apply. For example, Section B of the Bail Act 1997 includes provisions in respect of electronic monitoring of people on bail.

The Government is committed to supporting the responsible use of technology to improve people's lives, including supporting its use to help vulnerable people like dementia patients. The Medical Research Council, the Alzheimer's Society and Alzheimer's Research UK are jointly investing £290 million in the UK Dementia Research Institute at Imperial College London which looks at technology solutions that can assist people with dementia in their homes. Our Industrial Strategy also includes the Ageing Society Grand Challenge through which the Government will invest in the further development of technologies like Artificial Intelligence and the Internet of Things with the aim that people can enjoy at least five extra healthy independent years of life by 2035.

The Government also recognises the importance of ensuring that regulation is able to keep pace as technology advances. On 11th June, we published our White Paper on Regulation for the Fourth Industrial Revolution. The White Paper confirmed that the Government will establish a Regulatory Horizons Council to identify the implications of technological innovation and advise the government on regulatory reform needed to support its safe introduction.

HL Deb 01 August 2019 | PQ HL17327

Smart Devices: Children

Asked by: Lord Hunt of Kings Heath

To ask Her Majesty's Government whether they will take action to ban the sale of child-tracking smartwatches following research which has found that devices neither encrypt the data used nor secure each child's account.

To ask Her Majesty's Government what action they intend to take in regard to location-tracking smartwatches worn by children which are not secure and which are easy to hack.

Answering member: Lord Ashton of Hyde | Department: Department for Digital, Culture, Media and Sport

We take the protection of personal data very seriously, particularly when it relates to children and young people. Organisations that process personal data collected by smartwatches must comply with the the General Data Protection Regulation and the Data Protection Act 2018. The GDPR imposes strict obligations on organisations to process people's data fairly and lawfully and to ensure that any data collected is held securely. Organisations which fail to comply may be subject to enforcement action by the Information Commissioner's Office.

We do not intend to ban the sale of smartwatches, but we have issued a Code of Practice for organisations involved in the development, manufacturing and retail of products linked to the 'Internet of Things' to ensure that products are designed securely and keep consumers safe. In parallel, we have published consumer guidance to raise public awareness about setting-up, managing and improving the security of their consumer devices.

The code of practice and the guidance for consumers can be viewed at the following links:

https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security

https://www.gov.uk/government/publications/secure-by-design/consumer-guidance-for-smart-devices-in-the-home

HL Deb 30 November 2018 | PQ HL11615; PQ HL11614

5. Useful links and further reading

Institute of Electrical and Electronics Engineers Should the Government Regulate IoT Devices?

Department for Digital, Culture, Media and Sport Consultation on regulatory proposals on consumer IoT security published 1 May 2019

National Cyber Security Centre Smart devices: using them safely in your home February 2019

European Commission Digital Single Market Policy: The Internet of Things

Secure by Design The Government's Code of Practice for Consumer Internet of Things (IoT) Security for manufacturers, with guidance for consumers on smart devices at home, updated June 2019

The Royal Society (2017), The Internet of Things: opportunities and threats

Government Office for Science (2014), The internet of things: making the most of the second digital revolution.

Royal Academy of Engineering (2018), Internet of things: realising the potential of a trusted smart world.

DEBATE PACK
CDP 2019/0221
2 October 2019

About the Library

The House of Commons Library research service provides MPs and their staff with the impartial briefing and evidence base they need to do their work in scrutinising Government, proposing legislation, and supporting constituents.

As well as providing MPs with a confidential service we publish open briefing papers, which are available on the Parliament website.

Every effort is made to ensure that the information contained in these publicly available research briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated or otherwise amended to reflect subsequent changes.

If you have any comments on our briefings please email papers@parliament.uk. Authors are available to discuss the content of this briefing only with Members and their staff.

If you have any general questions about the work of the House of Commons you can email hcinfo@parliament.uk.

Disclaimer