horizon
DIGITAL ECONOMY RESEARCH

The University of Nottingham
UNITED KINGDOM · CHINA · MALAYSIA

Jiahong Chen
University of Nottingham
@jiahong_chen

Regulatory Considerations for Isolating End-of-Life Consumer IoT Products

Where's your cat… I mean your pop culture ref?

Most watched broadcasts by year [edit]

Year	Programme	Date	Viewers (millions)[4]	Network
2020	Take a wild guess!		18.16[53]	BBC One
2019	*Gavin & Stacey*	25 December 2019	17.92[52]	BBC One
2018	2018 FIFA World Cup: Croatia v England	11 July 2018	20.73[51]	ITV
2017	*Blue Planet II*	29 October 2017	14.01[50]	BBC One
2016	*The Great British Bake Off*	26 October 2016	15.90[49]	BBC One

Where’s your cat… I mean your pop culture ref?

Press release

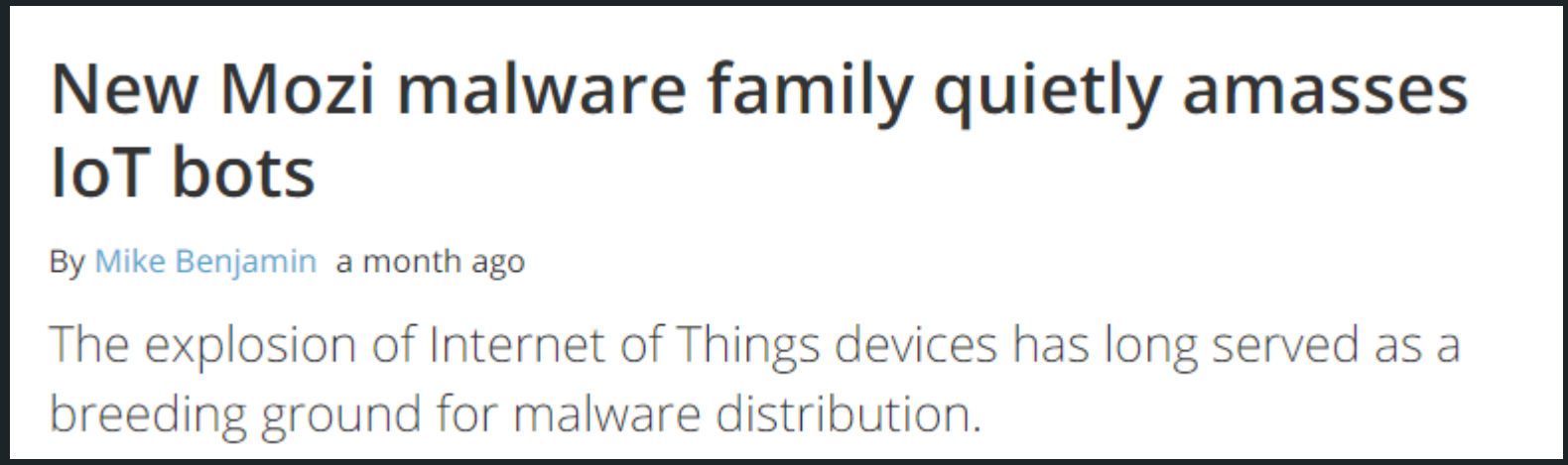
COVID-19 confirmed in pet cat in the UK

The virus responsible for COVID-19 has been detected in a pet cat in the UK.

Published 27 July 2020

From: Department for Environment, Food & Rural Affairs and Animal and Plant Health Agency

Saving lives by securing your IoT devices



New Mozi malware family quietly amasses IoT bots

By Mike Benjamin a month ago

The explosion of Internet of Things devices has long served as a breeding ground for malware distribution.

https://www.itproportal.com/features/new-mozi-malware-family-quietly-amasses-iot-bots/

Saving lives by securing your IoT devices

© Cineberg/Shutterstock.com

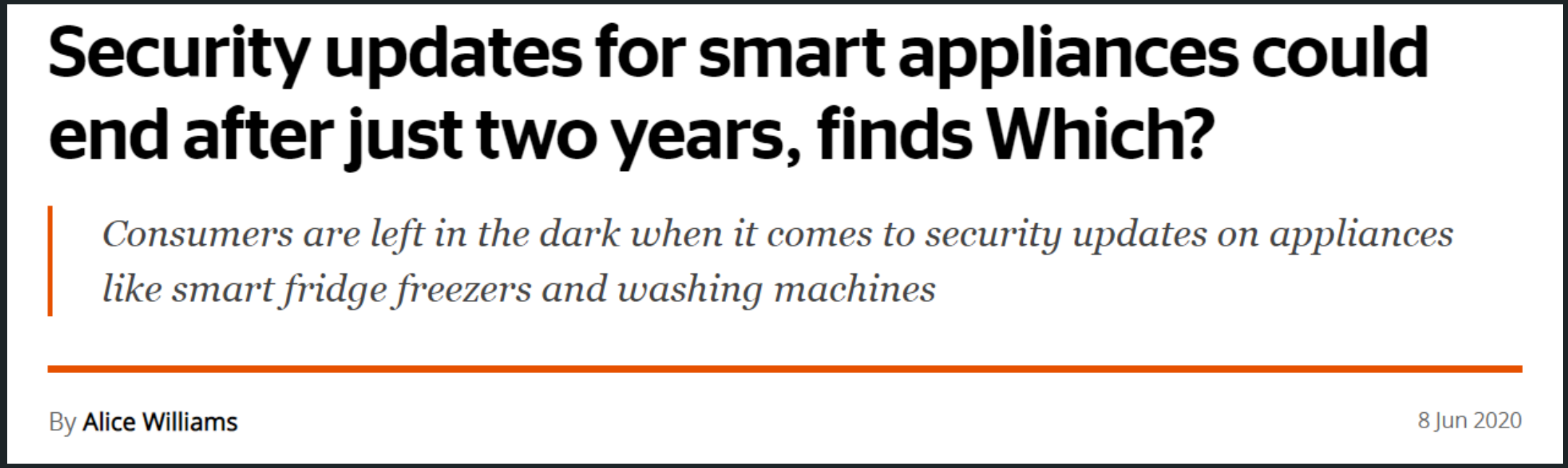
Parisian Hospitals hit by DDoS attack

Publication date: March 24, 2020 **Last edited:** March 24, 2020
Reading time: 1 minute, 19 seconds

Last Sunday the systems of a group of hospitals in Paris were hit by a DDoS attack. This temporarily prevented employees from accessing the home work programs and their email.

https://vpnoverview.com/news/parisian-hospitals-hit-by-ddos-attack/

What happens when your smart whatever is no longer supported?



Security updates for smart appliances could end after just two years, finds Which?

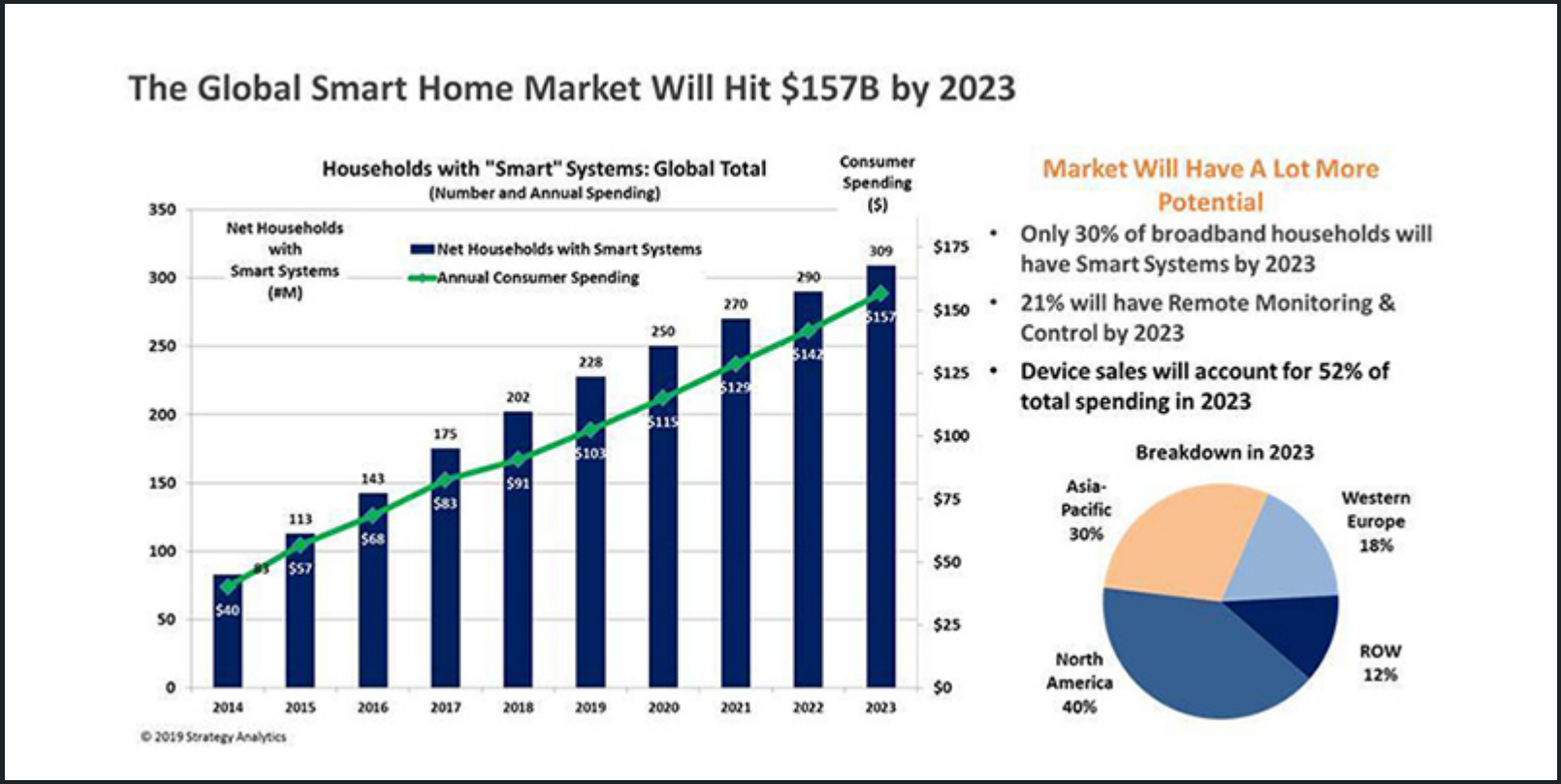
> *Consumers are left in the dark when it comes to security updates on appliances like smart fridge freezers and washing machines*

By **Alice Williams**

8 Jun 2020

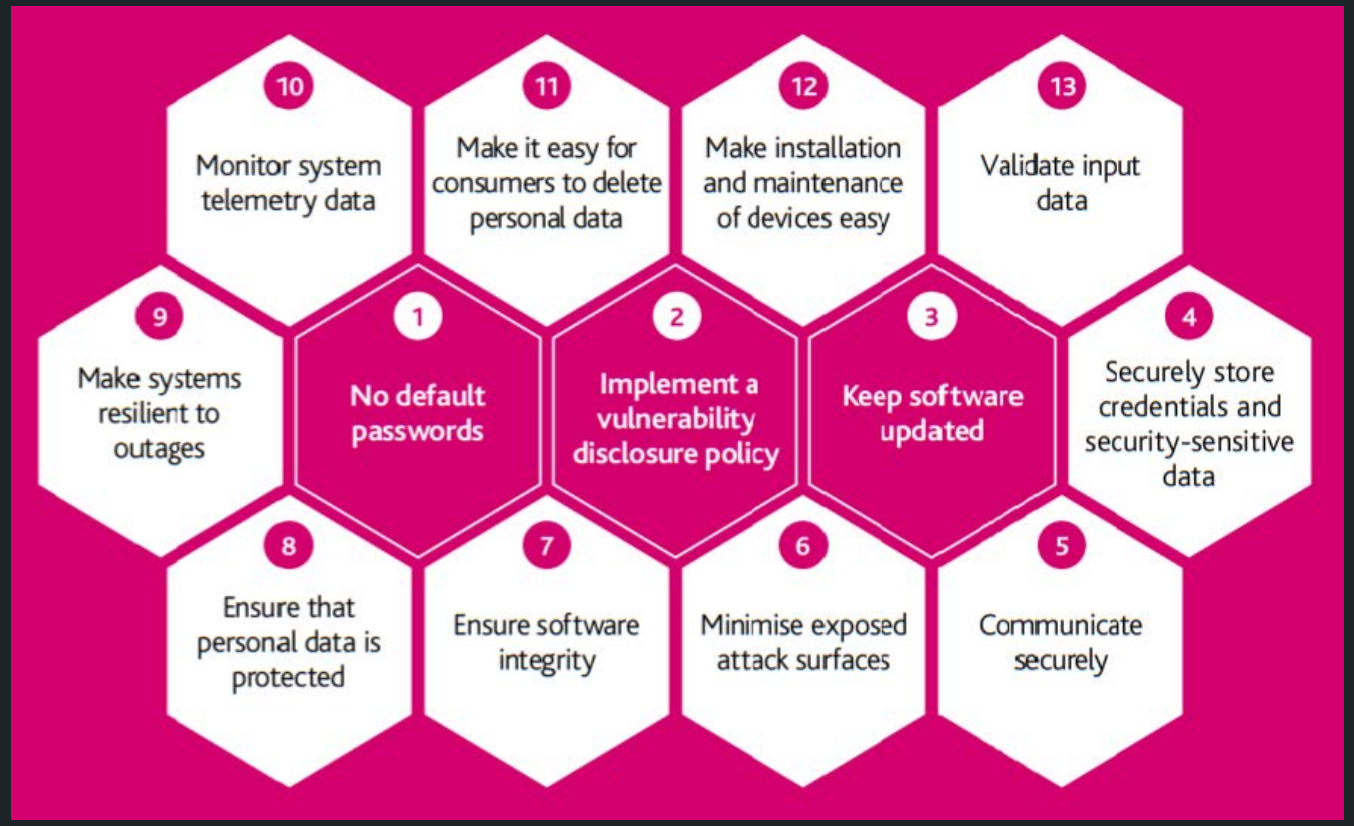
https://www.which.co.uk/news/2020/06/the-truth-behind-smart-appliance-security-updates/

What happens when your smart whatever is no longer supported?



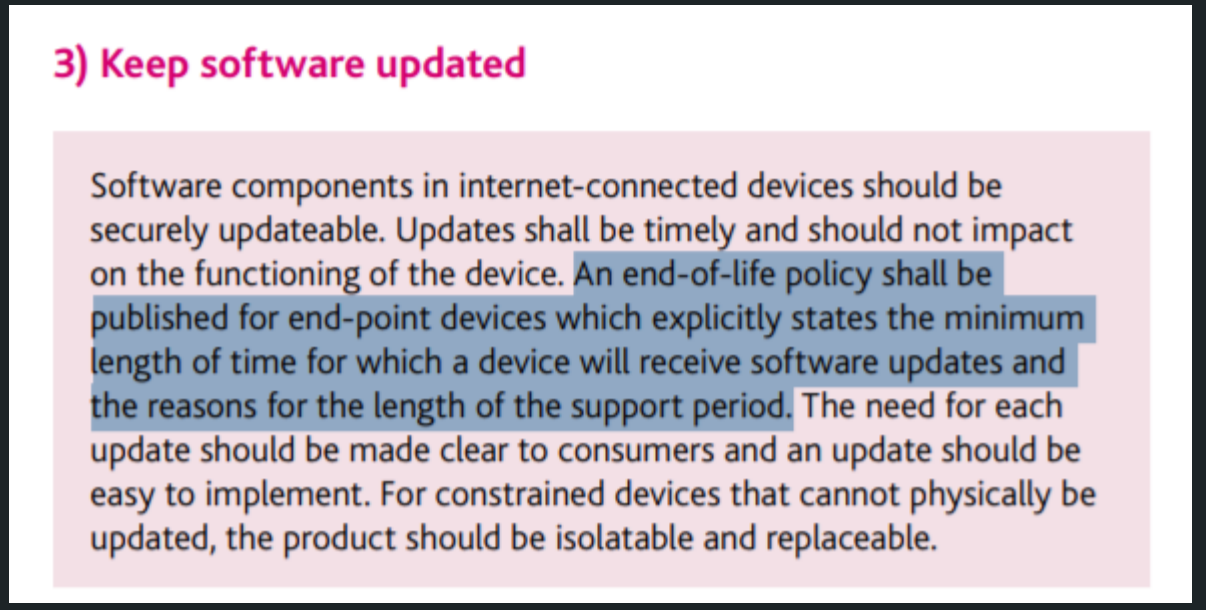
https://iotbusinessnews.com/2019/09/26/11853-global-smart-home-market-to-surpass-100-billion-in-2019/

Is this regulated yet?



https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

Is this regulated yet?



3) Keep software updated

Software components in internet-connected devices should be securely updateable. Updates shall be timely and should not impact on the functioning of the device. An end-of-life policy shall be published for end-point devices which explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period. The need for each update should be made clear to consumers and an update should be easy to implement. For constrained devices that cannot physically be updated, the product should be isolatable and replaceable.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

Is this regulated yet?

https://www.gov.uk/government/publications/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views

Is this regulated yet?

Requirement 3: Provide transparency on for how long, at a minimum, the product will receive security updates

Providing security updates in a timely manner is one of the most important mechanisms to protect consumers. Their purpose is to address security shortcomings that place consumer's privacy and security at risk and that typically are only identified once the product is on the market. They also enable consumers to make better informed purchasing decisions. When buying a product, consumers need to be able to find out the minimum period of time for which that product will be supported with security updates.

[...]

Setting the defined support period for software security updates can be challenging for long-life appliances that have an expected lifetime that is much longer than that of their digital components. There are a number ways to manage this, for example, creating the possibility to replace just those digital components, the automatic cessation of the product's internet-connectivity once the support period has ended or providing specific, and clearly understandable mitigation advice to users on possible actions to take if the support period has ended. It should also be noted that the defined support period can always be extended unilaterally by the producer or manufacturer.

https://www.gov.uk/government/publications/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views

Isolating the vulnerable - regulatory options

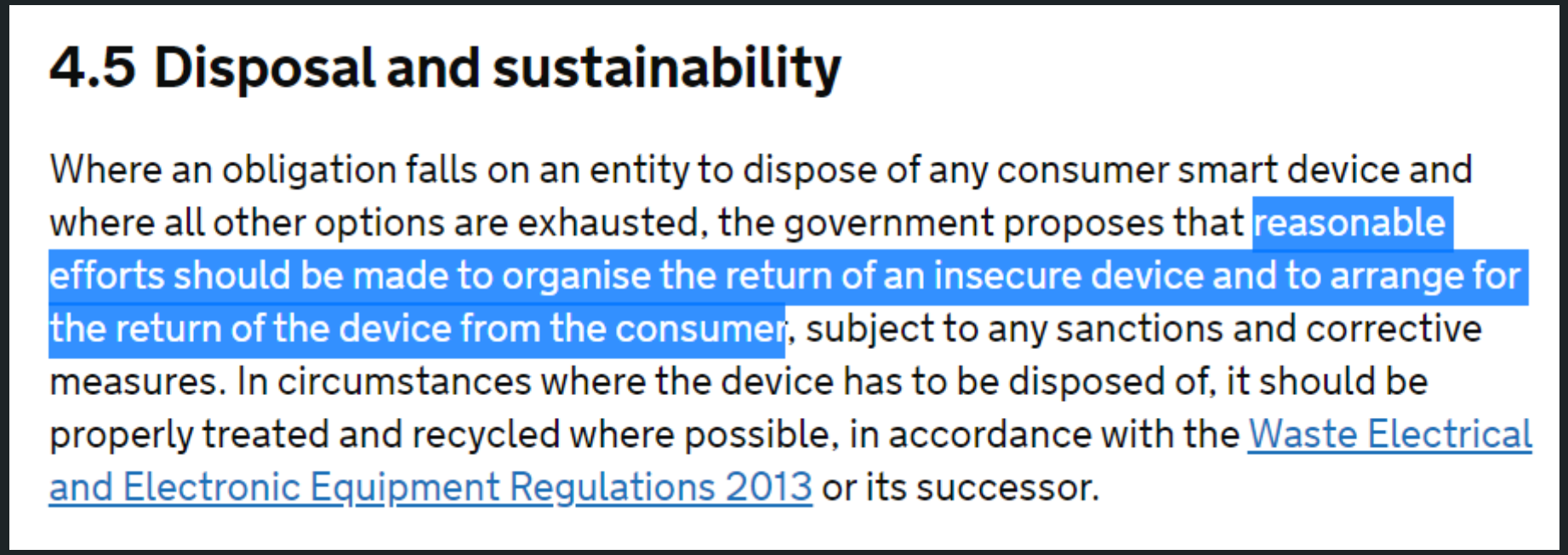
- "Avoid unnecessary contact" – minimise dependency on connection
- Also increases resilience

Isolating the vulnerable - regulatory options

- “Stay alert” – info on support period & warning on end of support
- Would users care?

Isolating the vulnerable - regulatory options

- "Shielding people at high risk" – mandatory recycling



4.5 Disposal and sustainability

Where an obligation falls on an entity to dispose of any consumer smart device and where all other options are exhausted, the government proposes that reasonable efforts should be made to organise the return of an insecure device and to arrange for the return of the device from the consumer, subject to any sanctions and corrective measures. In circumstances where the device has to be disposed of, it should be properly treated and recycled where possible, in accordance with the Waste Electrical and Electronic Equipment Regulations 2013 or its successor.

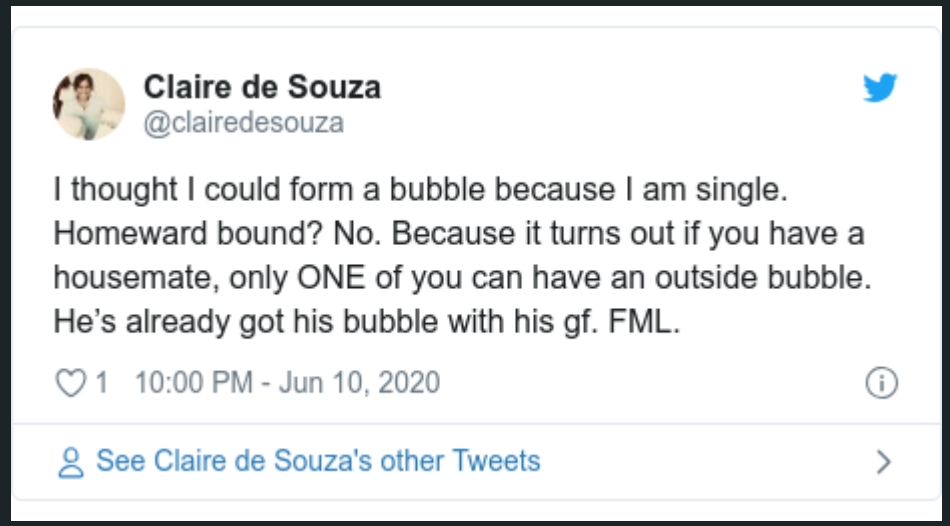
https://www.gov.uk/government/publications/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views

Isolating the vulnerable - regulatory options

- “Social distancing” – planned offlining of devices
- Optional / by default / compulsory

Isolating the vulnerable - regulatory options

- "Social bubbles" – localising connection
- Implemented on device / router / hub



Isolating the vulnerable - regulatory options

- "Immunity passport" – Selective connection permission
- Who is supposed to maintain the list?
- Have you heard of DADA?

Isolating the vulnerable - regulatory challenges

- "#scamdemic"
- Property rights vs security interests?
- Engagement with consumers and on-boarding of vendors

An anti-lockdown protester is detained by police officers during a demonstration in Hyde Park in London, on May 16, 2020. (Reuters)

Isolating the vulnerable - regulatory challenges

- "Ban on international travel"

Top Countries Hosting DDoS Weapons

DDoS weapons are globally distributed with higher concentrations found where internet-connected populations are most dense.

United States	1,591,719

China	1,388,531

Korea	776,327

Russia	696,186

India	283,960

Top Countries Hosting DDoS Botnet Agents

1. China	15%
2. Vietnam	12%
3. Taiwan	9%
4. Greece	4%
5. Other	60%

Top ASNS Hosting DDoS Botnet Agents

Chungwha Telecom (Taiwan)
China Telecom
China Unicom CN
VNPT Corp (Vietnam)
Telecom Egypt

https://www.a10networks.com/marketing-comms/reports/state-ddos-weapons/

Questions?

- jiahong.chen@nottingham.ac.uk
- Twitter: @jiahong_chen