Response to the Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security

Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. With over 3,000 active supporters, we are a grassroots organisation with local groups across the UK.

We are a project partner to Values and Ethics in Responsible Technology in Europe (VIRT-EU) – a European project funded by the Horizon 2020 program. VIRT-EU's mission is to foster ethical thinking in IoT development. The following comments stem predominantly from our experience accumulated in the course of that project.

We address the consultation questions in order below, omitting questions 7, 8 and 9 as these lie outside our remit.

1. 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?

We welcome the proposal to create primary legislation to introduce enhanced security for consumers using IoT devices. We also support the approach of making some requirements mandatory in the first instance with a longer strategy.

However, in addition to the 'top three', we would welcome other elements of the regulatory proposals being introduced now. The failure of self regulation and voluntary measures is thoroughly acknowledged in the consultation documents; in our view, mandatory requirements need to be implemented for industry as a matter of some urgency.

The development of EU Regulation 2017/0225 ('the Cyber Security Act') and the EU cyber security certification framework harmonising certification schemes across the EU, likely around ETSI Technical Specification 103 645 will remove the alleged negative impacts for the UK in creating a higher standard that would "stifle innovation". We fundamentally disagree with the view that regulation is the enemy of innovation, particularly in the long term.[1]

The Code and legislative proposal also does not solve another difficult problem for consumers: the lack of liability over software and services in relation to products. The status of software and particularly the protections in copyright law for digital rights management have led some authors to speak about the "end of ownership" - as digital

[1] Knut Blind, *The Impact of Regulation on Innovation*, January 2012 <http://www.innovation-policy.org.uk/share/02_The%20Impact%20of%20Regulation%20on%20Innovation.pdf>

products do not truly belong to the individuals who "purchase" them but are licensed as a service. A more fundamental review of digital goods in this regard is required.

2. 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?

We agree that the 'top three guidelines' form an appropriate baseline. However, we are also concerned that these should not detract from the wider Code and further steps towards the wider adoption of all the regulatory proposals should continue apace. We are concerned that without additional measures, the 'top-three' will become a ceiling for security rather than the minimum requirement. Legislation should set out measures to encourage industry adoption of the full Code. The example of data protection law could be followed: there, failing to follow codes of practice is an aggravating factor in enforcement cases.

There is one further aspect that could benefit from being included in the first-instance mandatory provisions. The PETRAS literature review of industry recommendations and international developments on IoT security often finds a requirement for cryptographic checks to allow updates only from an authorised source that is signed or verified from a trusted source. If consumers are led to expect and rely on security updates, the right security measures should be in place to avoid this provision becoming an even higher security risk.

3. Do you agree with the use of the security label (positive and negative) to communicate these requirements to consumers?

In her introduction to the Secure by Design report, Margot James, Minister for Digital and Creative Industries, stated the government's *"fundamental shift in approach to moving the burden away from consumers having to secure their internet connected devices and instead ensure strong cyber security is built into consumer IoT products and associated services by design."* The proposed labelling scheme clearly maintains the burden on consumers to ensure their privacy and security and as such is not the best option from the point of view of consumers.

We believe that the labelling scheme will likely not have the desired effect as it requires consumers to be informed and willing to take action to the point of having some impact on companies' profits, which is an uncertain eventuality. Whilst the presented research on price sensitivity is encouraging, our extensive experience in public advocacy has shown that it is difficult to change consumer behaviour on privacy and security grounds, and actual behaviour often differs from values expressed in surveys.

4. Do you agree with the wording of the labelling design?

We have no specific comments on the label wording. We however add that the inclusion of a negative label would be better than a simple absence, as many consumers would be otherwise unaware of the significance of no label.

The “expiry date” for security updates also needs to be written on the actual device, not merely on product packaging or a website.

5. 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)?

We agree that primary legislation should include the mandating of security requirements. The consultation impact assessment states that this policy option is not possible at this moment because several companies would be unable to comply. If this is the case, we need also to create a clear driver for these companies to change their systems. They have already had time to comply with the Code on a voluntary basis and have not done so. It is not certain that any labelling scheme alone will have the desired impact of driving up standards.

In addition, we believe that, at the very least, primary legislation must contain an automatic review and triggering of mandatory requirements by a certain date if the assessment is that the labelling scheme has not been successful to drive actual changes in security. That date should give sufficient time for companies to comply but be not so far into the future as to make them postpone immediate action. Failing to compel action at this stage would be a wasted opportunity, requiring a whole new policy cycle of several years of reports and consultation to bring new primary legislation in the future.

6. The consultation stage Impact Assessment published alongside the consultation document explores the costs and benefits of the options considered for this policy. Do you agree with our analysis?

… d) Data and research on the number of IoT manufacturers and retailers which sell their goods on the UK market.

The impact assessment states that there are only 59 IoT companies in the UK. We believe this figure could be undercounting. In our work, we have come across a large number of startups and suspect that not all of these have been accounted for. The analysis by our VIRT-EU project partners of social media conversations relating to IoT[2] shows that London is a major hub of IoT development. We recommend further data collection and research take place to accurately identify the number of companies involved.

10. Do you have a view on how best to enforce the requirements set out in both regulatory options? In particular, consider which UK agency is best placed to undertake enforcement and whether additional penalties would need to be set out to ensure that companies correctly use the labels.

The obvious agency to deal with cybersecurity would be the National Cyber-Security Centre, but we do not think this would be suitable as it mainly deals with businesses and not consumers. We think that it critical for an organisation with a strong

[2] VIRT-EU Project, Midterm Report, 30 June 2018 <https://blogit.itu.dk/inda/wp-content/uploads/sites/66/2018/11/Deliverable-1.3-.pdf>

consumer-facing capability to be in charge. The success of the labelling will depend on the demand of consumers.

The penalties involved need to be further clarified, as neither the consultation documents nor the impact assessment are very forthcoming. Penalties for large retailers need to be robust. The method in data protection law of making penalties proportionate to global turnover rather than fixing an upper limit has shown to be effective at modifying behaviour and we suggest that this could be a useful guide to follow.

The hardest element to enforce will be whether manufacturers maintain the security update schedule they promise on the label. There needs to be a penalty for non-compliance, a system for consumers to report failures to comply and an obligation on the regulator to review compliance levels through sampling.

The date for security updates can be problematic if implemented in isolation. There is a danger of simply supporting more unnecessary obsolescence and electronic waste if consumers are led to throw away serviceable devices. This needs careful consideration. Ultimately product companies need to make sure they support their devices for the full expected lifecycle. The EU is preparing a Sales & Goods Directive, which will require improved software support for goods with embedded digital components. The consultation impact assessment acknowledges this process and leaves it open depending on Brexit, but in our view the UK government should be making a clear commitment now to implementing these measures after Brexit.

The Code also needs more clarity over the level of "security updates", the severity of the risk required, whether it is linked to the CVE, etc.

There finally needs to be some mechanism to address the reality of companies going bust - a common occurrence with IoT startups - to ensure consumers are not left unsupported. Forcing companies to make available the required software code and documentation to produce third-party updates could be an option, although if servers are required and these are shutdown it may be impossible to keep the product supported.

<u>Further feedback</u>

In our view, the scope of applicability of the Code is fairly comprehensive, but it could be clearer in some edge cases. The provided list of examples show that most types of consumer goods can be made "smart" and therefore come in scope: toys, locks, fridges, TV sets, etc. We understand that motor vehicles would require separate legislation and possibly more stringent requirements, but suggest there should perhaps be more clarity over the Code's applicability to next generation vehicles such as smart bicycles and motorised scooters, which have security risks in e.g. their geolocation capabilities, remote locking etc.

There is also a need for more clarity over the role and status of crowdfunding platforms, such as Kickstarter. These have been the venue for the development of several highly popular smart devices, such as the Pebble Smartwatch; however, it is

unclear whether they would count as retailers under the proposal. Kickstarter in particular strongly denies being "a store"[3], but this is disputed, as many projects "sell" their devices there.[4] Kickstarter provides design guidelines that could incorporate the Code, but it is unclear how they are enforced. It is also unclear at what point in the Kickstarter (or similar) product development process the Code's requirements would need to be in place.

Components and electronics kits are currently out of scope for much regulation on electronics equipment. It is expected that they will be out of scope here, but lack of security updates for components could weaken the security of the sold devices. Mandatory requirements could be easier to cascade downstream towards suppliers. We would support their inclusion in the proposals.

The Code and overall process protect consumers from third-party attackers but not from the predatory business model of many technology companies and the negative effects that the harvesting of their data may have. This should be acknowledged more openly in next steps. Ultimately, a broader approach to responsible and ethical technology is required to ensure that security is taken into account.

[3] Kickstarter Blog, *Kickstarter is Not a Store*, 20 September 2012 <https://www.kickstarter.com/blog/kickstarter-is-not-a-store>

[4] Digital Trends, *Sorry, Kickstarter, You're a Store (Whether you admit it or not)*, 21 January 2014 <https://www.digitaltrends.com/opinion/yes-kickstarter-store-even-doesnt-want-admit/>