Communications Consumer Panel and ACOD response to DCMS's Secure by Design policy and draft Code of Practice

The Communications Consumer Panel, established by the Communications Act 2003, is a group of independent experts with direct sectoral experience. We ensure the citizen and consumer voice is represented in communications policy development.

The Panel's job is to ensure that the sector works for consumers, citizens and micro businesses - and in particular people who may be in a more vulnerable position in society. We carry out research, provide advice and encourage Ofcom, governments, the EU, industry and others to look at issues through the eyes of consumers, citizens and micro businesses.

The Panel pays particular attention to the needs of older people and people with disabilities, the needs of people in rural areas and people on low incomes, and the needs of micro businesses, which have many of the same problems as individual consumers.

Four members of the Panel also represent the interests of consumers in England, Northern Ireland, Scotland and Wales respectively. They liaise with the key stakeholders in the Nations to understand the perspectives of consumers in all parts of the UK and input these perspectives to the Panel's consideration of issues. Following the alignment of ACOD (the Advisory Committee for Older and Disabled people) with the Panel, the Panel is more alert than ever to the interests of older and disabled consumers and citizens.

Response

The Panel welcomes the opportunity to comment on the latest draft Secure by Design policy and Code of Practice (CoP). We appreciate the inclusion of our points made during prior engagement with DCMS, while the policy and CoP were under development.

We believe that the principles underpinning the policy and CoP are solid, consumer and citizen-focused, and are expressed clearly in the policy paper. We are pleased to see that the CoP applies to all types of Internet of Things (IoT) devices.

We agree with all the principles outlined in the draft, and that the top three should be given immediate priority.

Our specific points on the latest draft are below:

- The 'no default passwords' principle is – we agree - a high priority. We would urge DCMS to consider ways in which this, and the other principles within the CoP, could – at least in part, where practicable – be extended to apply to existing IoT devices already in people's homes and businesses, for example, by way of software upgrades, information campaigns, etc.

- We appreciate the fact that a contact email address is provided for the disclosure of vulnerabilities and we hope that this will also be a point of contact where consumers can seek advice as well as reporting issues.
- Further to our previous advice, we are pleased to see that DCMS has taken into account our suggestion that an end-of-life policy is published which explicitly states the minimum length of time for which a device will receive software updates and the reasons why.
- We welcome the requirement for each update to be made clear to consumers and that an update should be easy to implement.
- Both in respect of the above principle and others we urge DCMS to take into account the access requirements of consumers with specific needs, so that the CoP explicitly requires that this information is accessible to all users – including those who are not able to read text or hear audio. It is important here to keep in mind the need to consider these requirements based on the effect of a particular condition or disability – rather than its cause.
- Consumers with hearing, vision, mobility or cognitive impairments, or with learning difficulties or mental health problems, and people whose first language is not English or who have low levels of literacy should be included in benefitting from the existence of the CoP. There is, we believe, a case for highlighting this within the CoP and any guidelines; and there should be no excuse for any of the four sets of stakeholders failing to consider them. This is not an exhaustive list of people and we would recommend some guidance for stakeholders on inclusive user testing.
- The term 'life-impacting' (principle 9/Guidance paragraph 4.14) should in our opinion be updated to reflect consumers' reliance on assistive technology where that is the case.
- We would also urge DCMS to give some thought to the safety and security of low income consumers, for example those who are unable to upgrade or buy a new device, but whose device reaches the end of the publicised term to receive updates.
- Whilst we do not wish to see undue burdens placed on industry and we want innovation to thrive, we welcome the exploration of regulatory options to ensure that manufacturers act ethically to ensure secure and accessible design by default. These may be a necessary backstop – particularly where:
    - the safety and protection of children and vulnerable adults is concerned;
    - there is a risk to national security.

- We believe that principle seven (ensuring software integrity) is an important consumer protection issue and could be further developed – for example, with some form of advice and support process for the consumer.
- We strongly support the aims relating to consumer information – in particular the need for clear information. We would urge this to extend to Terms and Conditions information, and information in respect of any consent required from consumers.

These should also be accessible to people with access needs, e.g., alternative formats.

In summary, we welcome this policy and CoP. We recognise that the IoT has the potential for untold benefits for consumers and citizens. At the same time there are significant risks for consumers (of which they may be unaware) and the pace of technological advances can outstrip the ability to eliminate or mitigate those risks. We therefore support moving the burden away from consumers having to secure their internet connected devices, by ensuring that strong cyber security is built into products by design. This is a preventative measure, which consumers should have every right to expect.