Communications Consumer Panel and ACOD's response to DCMS' call for views on App Security and Privacy Interventions

About us

The Communications Consumer Panel, established by the Communications Act 2003, is a group of independent experts with direct sectoral experience. We ensure the voice of UK consumers, citizens and micro-businesses 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, 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.

Our response

We welcome the opportunity to response to DCMS' call for views. Our response confirms in writing the support we have given to DCMS in confirming our mutual belief that app users need more protection. We support the policy interventions set out and would welcome the development of regulation in this area, with input from consumer groups, digital regulators and international counterparts to DCMS.

We believe that in order to provide an accessible and affordable communications services, communications providers should enable consumers to contact them – or to engage with their services without direct contact - through as wide a variety of communications channels as possible. These channels may include telephone call, text message, text and video relay, email, webchat, online form – and some of these channels may be accessible to consumers through a provider's app.

For those who are able and willing to use them, apps can provide a shortcut to action, enabling them to note an additional access requirement due to a physical disability, or to check or pay a bill, raise a complaint, measure their data usage, and many other actions.

However, it should not be estimated that all communications service users are able to engage in an informed way with apps, from selecting the right one, to downloading it safely, to using it securely. We welcome DCMS' project to protect consumers from bad players in all sectors, 'piggy-backing' on communications networks to defraud or confuse consumers.

We note that the evidence from the NCSC report, highlighted in DCMS' document indicates that there are examples of malicious and insecure apps available on a range of app stores, thereby posing a risk to the security and privacy of users.

Having seen the positive impact of using apps like Zoom and Teams at keeping people connected during the pandemic, we believe it is vital that consumers who are less digitally skilled or confident are able to build confidence to go online and use apps safely. We believe this review and the proposed interventions are timely. A participant in our 2021 research said:

"I haven't got enough knowledge, it's not easy for old people. Downloading - I've got no idea what that means. I don't want to make mistakes, I'm frightened to because of the outcome. Banking online I don't trust as you hear all these stories about people being swindled."
(84-year-old female participant, first time internet user, clinically vulnerable and shielding at the time of the interview, lives in an urban area in the South of England)[1]

We have already provided a response to DCMS verbally at our hybrid meeting on 16 June 2022. In summary, we said that:

- alongside security, accessibility should be built into the process of selecting, purchasing, downloading and using apps. We believe in inclusivity by design and throughout, so consumers with additional access requirements do not face accessibility and usability issues. An inclusive by design approach would also avoid retrospective fitting, which can be costly, time consuming and disruptive. The Panel's 2021 think piece (written for the Panel by Graeme K Whippy MBE) sets out further details, including the POUR website accessibility model, as referred to in our meeting, which we believe should be adapted to become a requirement upon communications providers which serve customers through apps.[2]
- that consumer information about the security of apps should be accessible and available in a variety of formats, so that as many app users as possible can understand the risk of harm and how to protect themselves.
- the Panel's research had found that people's understanding of how their online data was handled and protected was limited, and the findings would be shared once published (emerging findings from the research had been that consumers felt they had very little control over the way organisations used their data and that bank details were the pieces of data that consumers were most reluctant to divulge online. Consumers were most suspicious of online shopping sites and in terms of the trustworthiness around keeping their data safe, they trusted healthcare providers the most and social media providers the least.)
- we asked for more detail on the potential consequences of non-compliance with the draft Code of Practice and were keen to see bad players held to account. We note that DCMS' comment that app store operators would need to consider the reputational damage they would face from not following the proposed Code should

[1] CCP-ACOD: Getting up to speed while staying at home: UK consumers digital connectivity challenges
[2] CCP-ACOD: Making communications services inclusive and accessible

it emerge, following a security incident, that they had not been adhering to its principles.

- we agreed with DCMS that looking into international standards would be a valuable exercise (please note the similarity in difficulty in tackling nuisance calls and texts that are from non-UK sources, faced by Ofcom).
- We said that we would share the call for views with other consumer bodies – having already shared it with participants of our Consumer Advocacy Hub, representing the main UK consumer advocacy bodies in England, Wales, Scotland and Northern Ireland, we would also raise awareness among participants of our National Consumer Stakeholder Hubs in each Nation of the UK.

Taking all of the above into account, including the views we regularly hear from consumer stakeholders that more needs to be done to ensure consumers can use digital communications services safely and securely.

We urge DCMS to investigate the potential for regulation to protect users of apps. In the interim, we support the Proposed Code of Practice for App Store Operators and App Developers, in particular:

- we support the criteria set out under 1 and 3 and would encourage the addition of a line to require app store operators and app developers to deliver accessibility and usability-tested apps and security updates that are not disruptive to assistive technology, as best practice.
- under 2, vulnerability disclosure processes should also be accessible to all – please note that the word 'vulnerability' is also used widely to convey consumers' difficulties in accessing regulated services when their circumstances make it difficult for them to access mainstream services without additional support. We believe that vulnerability is not a popular, widely used word by consumers, but would caution that care is taken not to confuse consumers.
- we agree with the considerations outlined under 4 regarding accessible access to information for potential users of an app – we particularly welcome the consideration that has been given to ensuring that an app works regardless of whether the user has chosen to accept certain permissions set out by the developer/app store, particularly where users have no other way of accessing a service effectively other than through an app.
- we welcome the considerations to app stores working collaboratively with developers to ensure the protection of users.
- we welcome DCMS' continued engagement with the ICO, consumer groups and international counterparts and would recommend that the Digital Regulation Cooperation Forum, or at least Ofcom features in this list.