NCF Response to the Online Harms Consultation of April 2019

The National Consumer Federation welcomes the On-Line Harms consultation paper as an important step forward in consumer protection.

We have provided responses to the consultation questions in Section 2

Section 1 Summary

In summary the NCF sees the following aspects as key:-

(1) A focus on the products from suppliers is needed as specific products are the means by which harm is created.

(2) The new regulator should have a resourced and coherent market monitoring and enforcement strategy as too much bad practice will slip by if there are not the means to detect that bad practice in preventing harms and then enforce corrective action.

(3) A new On-Line Harms law needs to align with the UK implementation of the GDPR and so will require to distinguish between

- "O" for Organisational sources of harm from organisations and individuals communicating with or trying to organise and influence the whole public or groups of people

and

- "P" for Personal sources of harm between individuals in their private lives

See also Annex A with respect to "O" and "P" harms

This particularly relates to the proposed regulatory responsibility

- The regulator will have a legal duty to pay due regard to innovation, and to protect users' rights online, being particularly mindful to not infringe privacy and freedom of expression."

(4) The new law should make use of British Standards as for example the General Product Safety Regulation does where use of an appropriate standard carries with it a presumption of compliance (but also with clauses that state that none the less there is an over-riding responsibility to make products safe.)

This use of British Standards relates to the proposed regulatory responsibility

- "The regulator will take a proportionate approach, expecting companies to do what is reasonable, depending on the nature of the harm and the resources and technology available to them.

(5) A market monitoring strategy should enable consumers to help monitor the market place. The strategy should also engage with and reward professionals monitoring the digital market place for online harms. Company fines should be large enough to be a

real incentive to act and also to cover the costs of enforcement action and rewarding the responsible professionals mentioned above

A highly relevant standard under development

DCMS and the Home Department should note that when it comes to suitable standards that can cope with product digital diversity and innovation there is an International standard due in 2021 being developed by ISO committee PC 317. The standard is ISO 31700 for Consumer Protection: Privacy by Design of Consumer Goods and Services.

The ISO Privacy by Design standard ISO 31700 would help by requiring those who choose to comply with it to :

- For suppliers of consumer goods and services to be available in the UK using ISO 31700 would be required to reference the Online Harms law as relevant to design and then design to meet that law's requirements.

- The design process would be required to have as inputs known harms, consumer and technical vulnerabilities and known exploits causing those harms. These are then used in setting the product development and performance requirements.

- The design process would require the setting of Consumer Product Privacy Requirements (for example as derived from the joint BSI-CPIN, ANEC and ISO COPOLCO Privacy Guides like the domestic privacy guide which includes requirements with respect to :-

    - Governance
    - Parental overview of children's product use (especially for online services)
    - Provision of consumer information to avoid harms
    - Harmful content signalling online from the home or smartphone app to service providers to allow them to undertake analysis and action against sources of harm using the service
    - In market monitoring of product privacy performance the inclusion of online harms and corrective actions to remove or mitigate the harms

The ISO 31700 approach allows "good guys" to demonstrate due care.

The NCF has a good relationship with BSI and if required a view of the consumer value of ISO 31700 can be obtained via Sadie Homer BSI Consumer Policy Executive at Sadie.Homer@bsigroup.com

Section 2 - Consultation Questions and NCF responses:

Question 1: This government has committed to annual transparency reporting. Beyond the measures set out in this White Paper, should the government do more to build a culture of transparency, trust and accountability across industry and, if so, what?

HMG should let this law settle down first as it is a significant step forward and then review the situation with stakeholders.

Question 2: Should designated bodies be able to bring 'super complaints' to the regulator in specific and clearly evidenced circumstances?

YES

Question 2a: If your answer to question 2 is 'yes', in what circumstances should this happen?

As a backstop to good market monitoring and enforcement action by HMG and when the designated bodies have found, and can evidence, substantial harm to significant numbers of people especially when for one reason or another individual actions have not been effective.

Question 3: What, if any, other measures should the government consider for users who wish to raise concerns about specific pieces of harmful content or activity, and/or breaches of the duty of care?

Assign an Ombudsman

Question 4: What role should Parliament play in scrutinising the work of the regulator, including the development of codes of practice?

Parliament should review and scrutinise the new regulator against the *NCF proposed enhancement to the BEIS regulator code* to better reflect the consumer stakeholder perspective in regulation. This has been well received by the Consumer Minister.

Question 5: Are proposals for the online platforms and services in scope of the regulatory framework a suitable basis for an effective and proportionate approach?

The focus should be on the platform provider's services

Question 6 In developing a definition for private communications, what criteria should be considered?

Use as a similar basis the GDPR definition of private processing to distinguish that from processing of data for organisational purposes (like billing and product deliveries). Private processing in the GDPR is expressed as processing for personal or household purposes. A similarly phrased definition for private communications could then be "communications

between family and friends for personal purposes". That would cover one to one messages and content, and one to many known family and friends like invitations to parties.

There would be a need to distinguish between "domestic friends" who have been met and friendships formed directly in person from "online friends" where the ability of an individual to determine how genuine someone is, is very limited and deception easy.

Question 7: Which channels or forums that can be considered private should be in scope of the regulatory framework?

That would depend on the GDPR definition of personal and organisational processing where communications are an important sub set of such processing. Reference Annex A for proposed examples of "O" and "P" sources of harm

Question 7a: What specific requirements might be appropriate to apply to private channels and forums in order to tackle online harms?

The ability of the receiver of intrusive, offensive or abusive content to signal (digitally) within the service that the source of the content should be investigated as actually or potentially harmful. Allowance should be made for the role of responsible 3rd parties like parents or carers in overview of the cared for who might be experiencing online harm.

Question 8: What further steps could be taken to ensure the regulator will act in a targeted and proportionate manner?

A market monitoring strategy should enable consumers to help monitor the market place. The strategy should also engage with and reward professionals monitoring the digital market place for online harms. Company fines should be large enough to be a real incentive to act and also to cover the costs of enforcement action and rewarding the responsible professionals mentioned above.

Question 9: What, if any, advice or support could the regulator provide to businesses, particularly start-ups and SMEs, comply with the regulatory framework?

Provision of nationally available good practices to avoid or deal with online harms being experienced through their services. The acquisition of such knowledge from 'ground zero' without a reputable source of good practice would be a significant overhead and drag on SME abilities to innovate and grow.

Question 10: Should an online harms regulator be: (i) a new public body, or (ii) an existing public body?

Irrespective of whether the online harms regulator is new or an existing regulator it is only worthwhile putting the regulation in place if it 'has teeth".

Question 10a: If your answer to question 10 is (ii), which body or bodies should it be?

Both OFCOM and ICO, as the current main digital regulators, are heavily challenged at the moment.

OFCOM has many consumer issues on its plate with nuisance calls action only just starting to be effective in a limited way. Further OFCOM is in the process of reorganising its consumer engagement having recently ceased its Consumer Forum for Communications.

The ICO has much on its current plate settling down the UK implementation of the GDPR.

Question 11: A new or existing regulator is intended to be cost neutral: on what basis should any funding contributions from industry be determined?

Value of UK revenues

Question 12: Should the regulator be empowered to i) disrupt business activities, or ii) undertake ISP blocking, or iii) implement a regime for senior management liability? What, if any, further powers should be available to the regulator?

Instruct removal of content, where practical have powers to prosecute those whose material on a service causes harm, blocking content if the source cannot be removed, embed senior management accountability if due care has not been taken.

Question 13: Should the regulator have the power to require a company based outside the UK and EEA to appoint a nominated representative in the UK or EEA in certain circumstances?

No comment

Question 14: In addition to judicial review should there be a statutory mechanism for companies to appeal against a decision of the regulator, as exists in relation to Ofcom under sections 192-196 of the Communications Act 2003?

No comment

Question 14a: If your answer to question 14 is 'yes', in what circumstances should companies be able to use this statutory mechanism?

Question 14b: If your answer to question 14 is 'yes', should the appeal be decided on the basis of the principles that would be applied on an application for judicial review or on the merits of the case?

Question 15: What are the greatest opportunities and barriers for (i) innovation and (ii) adoption of safety technologies by UK organisations, and what role should government play in addressing these?

- See answer to question 9 to lower innovation barriers with respect to the creation of a National SME supporting knowledge base

- There are no such things as safety technologies. Technology can be used for good and bad purposes, as an example the technology of the dark web was introduced partly to enable oppressed citizenry to express their views without fear of retribution, however the same technology has led to dreadful use of the dark web for child abuse, drugs and more. The approach should be "Protection by Design" where design processes and product requirements are established to identify, remove or mitigate harms that can be caused by digital technologies.

Question 16: What, if any, are the most significant areas in which organisations need practical guidance to build products that are safe by design?

Start with a good quality privacy by design process for the whole product lifecycle that addresses online harms as one of the key exploits that invade consumer privacy.

Due in 2021 and being developed by ISO committee PC 317 is ISO 31700 for Consumer Protection: Privacy by Design of Consumer Goods and Services. This standard includes addressing harmful intrusive content over a product lifecycle.

A view of the consumer value of ISO 31700 can be obtained via Sadie Homer BSI Consumer Policy Executive at Sadie.Homer@bsigroup.com

Question 17: Should the government be doing more to help people manage their own and their children's online safety and, if so, what?

Start with an Industry knowledge base a good practice in product design for parental overview and dealing in practice effectively with the many difficult parent child situations. This would include practical design guidance as well as guidance on what information to provide to parents when signing up to / authorising the child's use of the service.

For example: At a BSI forum on AI and ethics on 26th June 2019 Lego described the challenges of balancing decisions where they were aware that the more restrictive parental controls were over their digital products, the more likely children were to avoid those by using much riskier services from other providers https://www.bsigroup.com/en-GB/our-services/events/2019/wednesday-26-june--cpin-summer-meeting/

More information about this meeting can be obtained via Sadie Homer BSI Consumer Policy Executive at Sadie.Homer@bsigroup.com

Question 18: What, if any, role should the regulator have in relation to education and awareness activity?

Start with the services and suppliers of those service, settle the new law and regulation down and then review the need for education and awareness. Meanwhile work with good practice suppliers, children's charities and consumer organisations to help them provide consumer awareness.

Annex A

For information Table 1 Online Harms Consultation list of harms and an initial "O" and "P" allocation.

Harms with a clear definition	
- Child sexual exploitation and abuse.	Both "O" and "P"
- Terrorist content and activity.	"O"
- Organised immigration crime.	"O"
- Modern slavery.	"O"
- Extreme pornography.	"O"
- Revenge pornography.	"P"
- Harassment and cyberstalking.	"P"
- Hate crime.	Both "O" and "P"
- Encouraging or assisting suicide.	Both "O" and "P"
- Incitement of violence.	Both "O" and "P"
- Sale of illegal goods/ services, such as drugs and weapons (on the open internet).	"O"
- Content illegally uploaded from prisons.	"O"
- Sexting of indecent images by under 18s (creating, possessing, copying or distributing indecent or sexual images of children and young people under the age of 18).	Both "O" and "P"
Harms with a less clear definition	
• Cyberbullying and trolling.	"P"
• Extremist content and activity.	"O"
• Coercive behaviour.	Both "O" and "P"
• Intimidation.	Both "O" and "P"
• Disinformation.	"O"
• Violent content.	"O"
• Advocacy of self-harm.	Both "O" and "P"
• Promotion of Female Genital Mutilation (FGM).	Both "O" and "P"
Underage exposure to legal content	
• Children accessing pornography.	"O"
• Children accessing inappropriate material (including under 13s using social media and under 18s using dating apps; excessive screen time).	Both "O" and "P"