Response of the Information Commissioner's Office to Ofcom's call for evidence on the first phase of online safety regulation.

About the Information Commissioner's Office

The Information Commissioner's Office (ICO) has responsibility for promoting and enforcing the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18), the Freedom of Information Act 2000 (FOIA), the Privacy and Electronic Regulations 2003 (PECR) and the Environmental Information Regulations 2004 (EIR).

The ICO is independent from government and upholds information rights in the public interest, promoting transparency and openness by public bodies and organisations and data privacy for individuals. It does this by providing guidance to individuals and organisations, solving problems where it can, and taking appropriate action where the law is broken.

Introduction

The ICO welcomes the opportunity to respond to questions in Ofcom's call for evidence on the first phase of online safety regulation. This response is limited to those questions where the ICO's experience of regulating online services is relevant.

We refer regularly to ICO public resources and guidance. These include the ICO's Guide to Data Protection and its Accountability Framework, which support organisations to comply with data protection law. Accountability is one of the data protection principles set out in the UK GDPR. This principle requires organisations to take responsibility for what they do with personal data and to have appropriate measures and records in place to demonstrate compliance with the legislation. Accountability enables organisations to minimise the risks arising from the use of personal data by putting in place appropriate and effective policies, procedures and measures.

In this response we also refer to the ICO's Children's Code (the Children's Code). The Children's Code is a statutory code of practice that applies to "Information Society Services likely to be accessed by children." It applies to many apps, programs, search engines, websites, streaming services and online games, including services likely to be captured by the scope of the online safety regime. It sets out standards that services should conform to in order to provide better privacy protections for children. If services do not conform to the code, they are likely to find it more difficult to demonstrate compliance with data protection law.

Responses

Q5 What can providers of online services do to enhance the clarity and accessibility of terms of service and public policy statements?

Drafting Effective Privacy Information

Under the UK GDPR, individuals have the right to be informed about the collection and use of their personal data. Services are required to provide individuals with privacy information about their personal data processing in a way that is easily accessible and easy to understand, using clear and plain language. The ICO's Guide to Data Protection provides practical guidance about how privacy information should be drafted. Among other measures, it recommends that user testing is carried out on privacy information to get feedback on how easy it is to access and understand. It also recommends that, when drafting privacy information, organisations should put themselves in the position of the user that they are collecting information about.

The above section of the Guide to Data Protection also refers to techniques that can be used to provide clear and accessible privacy information. These include using:

- A layered approach - short notices containing key privacy. information that have additional layers of more detailed information
- Dashboards - preference management tools that inform people how organisations use their data and allow them to manage what happens with it.
- Just-in-time notices - relevant and focused privacy information delivered at the time organisations collect individual pieces of information about people.
- Icons - small, meaningful symbols that indicate the existence of a particular type of personal data processing.
- Mobile and smart device functionalities - including pop-ups, voice alerts and mobile device gestures.

The ICO's Accountability Framework is an additional resource setting out how services can meet the ICO's expectations for transparency and clarity.

The Children's Code

Standard 4 of the Children's Code requires that the privacy information (and other published terms, policies and community standards) that services provide to child users must be concise, prominent, and in clear

language suited to the age of the child. Services should provide additional specific 'bite-sized' explanations about how they use personal data at the point that use is activated. Information should be tailored to the age of the child/user. The code provides some detail, including:

- Services should present all this information in a way that is likely to appeal to the age of the child who is accessing their online service. This may include using diagrams, cartoons, graphics, video and audio content, and gamified or interactive content that will attract and interest children, rather than relying solely on written communications.

- Services may use tools such as privacy dashboards, layered information, icons and symbols to aid children's understanding and to present the information in a child-friendly way.

- Organisations should take an evidence-based approach to what methods of presentation are most appropriate for their service. This could include consulting with children and parents, referring to best practice design methods or academic research, analysing user redress and feedback data, engaging with children's development and rights specialists or using external audits.

Best Practice in Service Design

The ICO has published recommendations for designing data transparency for children. This report celebrates current good practice and showcases the 'art of the possible' when it comes to creating data transparency for children.

The ICO's award winning Children's Code design guidance shows how to apply the Children's Code in practice and includes tools that organisations can use to create an open, transparent and safe place for children online.

Q7 What can providers of online services do to enhance the transparency, accessibility, ease of use and users' awareness of their reporting and complaints mechanisms?

The ICO's Accountability Framework sets out the ICO's expectations for online tools to support personal data transparency and user control. Services are encouraged to provide individuals with tools, such as secure self-service systems, dashboards and just-in-time notices so they can access, determine and manage how the organisation uses their personal data.

Under the framework services should give individuals clear and relevant information about their data protection rights and how to exercise them. Policies and procedures should set out the processes for dealing with requests from individuals about their rights. Staff should receive training and guidance about how to recognise a request and where to send it.

The UK GDPR itself requires services to provide users with information about their ability to exercise data protection rights (including the rights to rectification and erasure of data), as well as contact details for the organisation's data protection officer (where applicable) and the right of users to lodge complaints with the ICO.

The Children's Code

Standard 15 of the Children's Code states that services should provide prominent and accessible tools to help children exercise their data protection rights and report concerns. It also provides that online tools should include a mechanism to track the progress of any complaint or rights issues that are raised with the Information Society Service. The tools should be easy to find and the language should be age appropriate for users. The Children's Code sets out recommendations about how tools might be tailored to the age range of different child users to ensure they are clear and understood.

Q18 Are there any functionalities or design features which evidence suggests can effectively prevent harm and could or should be deployed more widely by industry?

a) The Children's Code places an emphasis on the use of **high privacy by default settings** for under 18's. These can contribute to child safety online. For example:

   Standard 7 requires services to set privacy settings to high privacy by default unless they can demonstrate a compelling reason for a different default setting taking into account the best interests of the child. High privacy by default settings can mean that children's personal data is only visible or accessible to other users of the service if the child (or a parent or guardian) actively amends their settings - this may help to reduce unwanted communications with people that children do not already know. High privacy by default settings may also means that, unless a setting is changed, a service's own use of the children's personal data is limited to use that is essential to the core provision of the service. Any optional or supplementary uses of personal data, potentially including any

processing to personalise the service, have to be individually selected and activated by the child.

Standard 10 requires services to switch geolocation options off by default unless they can demonstrate a compelling reason for geolocation to be switched on by default, taking into account the best interests of the child.

Standard 12 requires services to turn off profiling by default unless services can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child. The code notes that some profiling may be relatively benign but other profiling, such as personalised content feeds that gradually take a child away from their original area of interest into other less suitable content, raise more significant concerns.

- Standard 9 requires that services should not disclose the personal data of children to third parties unless they can demonstrate a compelling reason to do so, taking into account the best interests of the child. Any default settings relating to data sharing should specify the purpose of the sharing and who the data will be shared with.

The benefits of high privacy by default settings are also relevant to adults. The ICO's Guide to Data Protection recommends that organisations offer strong privacy defaults for all users, including adults, as part of a data protection by design and default approach.

b) Standard 13 of the Children's Code refers to **nudge techniques**. These are defined as design features which lead or encourage users to follow the designer's preferred paths in the user's decision making. The Children's Code envisages that nudge techniques can be used for pro-privacy reasons, for example nudging towards high privacy options where this is appropriate, taking into account the best interests of the child. The code also suggests that services should consider nudging to promote the health and wellbeing of child users. For example, nudging children towards supportive resources where necessary. The code sets out recommendations about how such tools might be tailored to the age range of different child users.

The use of nudge techniques in the design of online services can also have negative effects on privacy where they encourage users to provide more personal data than they would otherwise volunteer. Standard 13 requires that services should not use nudge techniques

to lead or encourage children to provide unnecessary personal data or turn off privacy protections. This requirement reflects data protection law generally as it applies to all users, including adults.

Best Practice in Service Design

The ICO's Children's Code design guidance contains design guidelines for protecting children's privacy by default and also references "things to avoid," such as nudge techniques that influence children towards sharing their personal data. One of the tools in the design guidance helps organisations identify the 'risky moments' in their service where supportive design features can help minimise the risk posed to children.

Q22 What age assurance and age verification techniques are available to platforms and what is the impact and cost of using them?

Age assurance measures are rapidly developing and can vary in the volume of personal data required to operate them effectively, as well as in their accuracy and cost.

There is a range of age assurance tools available to platforms, including age estimation techniques that use facial scans, iris scans, or voice scans. Age verification techniques can include the use of hard identifiers such as passports, driving licences or, another verifiable record of age. Other techniques include the use of self-declaration of age.

Standard 3 of the Children's Code requires organisations to: "Take a risk based approach to recognising the age of individual users and … effectively apply the standards in this code to child users. Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing or apply the standards in this code to all your users instead."

Platforms are therefore required to take a risk-based approach to using age assurance techniques to ensure the technique deployed is proportionate to the risks arising from their use of children's data. The ICO has published a Commissioner's Opinion on the use of age assurance to support online services in their risk-based approach to age assurance. The Opinion sets out how organisations should approach age assurance to conform to the Children's Code and comply with data protection law.

Annex 2 of the Opinion provides a summary of the ICO's assessment of current uses of age assurance (as at the date of publication of the Opinion in October 2021). Annex 3 of the Opinion contains an economic analysis of the impact of age assurance at the date of its publication.

Q23 Can you identify factors which might indicate that a service is likely to attract child users?

The Children's Code notes that, in practice, the likelihood of a service being accessed by children depends on:

- the nature and content of the service and whether there is a particular appeal for children; and
- the way in which the service is accessed and any measures in place to prevent children gaining access.

Services are encouraged to take a common sense approach to determining whether they are likely to be accessed by children. The conclusion that a service reaches about the likelihood of children accessing its service must be objective, documented, and supported with evidence. The code states that services may wish to refer to market research, current evidence on user behaviour, the user base of similar or existing services, and testing of access restriction measures.

Ofcom may also find the Irish Data Protection Commission's *The Fundamentals for a Child-Oriented Approach to Data Processing* publication to be of interest. Section 1.3 sets out a (non-exhaustive) list of factors that could assist in assessing whether a website, app or other online service is likely to be accessed by children.

Conclusion

The ICO is committed to continuing to work with Ofcom on the implementation of the online safety regime (including through the DRCF). We look forward to engaging further on the above issues and on other areas where the ICO's experience and expertise will be of value.

23 September 2022