Response to the Information Commissioner's Office public consultation on the age-appropriate design draft code of practice

Executive summary

Google fully supports the Information Commissioner's Office ("ICO")'s objective to help keep children safe online and welcomes the opportunity to comment on the draft age-appropriate design code (the "Draft Code").

In our response below, we aim to highlight what we think could be unintended consequences of the Draft Code, as requested by the consultation document, and make suggestions that we believe could help ensure that the final Code is as effective as possible while still allowing children and adults alike to have a positive experience of online services, and allowing service providers to consider a broader range of technical solutions to ensure this. We would like to respectfully recommend some clarifications to increase legal certainty, in particular to avoid overlap or contradiction with other legal instruments. We also add specific examples and potential solutions, such as an approach focused on empowering young users and their parents with transparency and privacy tools to experience the Internet in a safe, concerted way and in a manner that takes into account the individuality and rights of each child. Lastly, we make some specific suggestions based on our experience to date, aimed at avoiding "information fatigue" and ensuring the clarity of transparency notices for the broadest possible audience, and calling for a broader variety of age verification mechanisms to be recognised as effective.

Detailed response

Google fully supports the ICO's objective to help keep children safe online and believes that appropriate and effective regulation, in combination with a range of other initiatives, can help achieve this. This is an issue we take very seriously. We greatly appreciate the ICO's call for feedback and wish to offer the comments below to help ensure that the Code fulfils its goals and help prevent any unintended consequences.

In particular, we believe it is important that developers maintain a degree of flexibility in the way their services are developed, so as to ensure that children are adequately protected without unintentionally curtailing their online access and digital

development. The Internet offers important benefits for children and we must ensure that the Code protects their safety as well as their ability to access information, seize educational opportunities, communicate with friends or families, or gain access to culture and entertainment.

To date, Google has supported a number of existing frameworks that have been effective in helping drive innovation and safety for children online. For example:

- The Alliance to Better Protect Minors Online — an EU wide self-regulatory initiative aiming to improve the online environment for children and young people[1]. The framework of the Alliance is set in a Statement of Purpose, announced during Safer Internet Day 2017, in which companies agreed to curb harmful content, harmful conduct and harmful contact.
- The Safety framework of the ICT Coalition for Children Online, a European industry initiative aimed at making platforms safer for users[2].
- Google was also the first non-ISP member of Internet Matters — the online safety not-for-profit which provides tools and advice for parents on issues that could affect their children's mental health, from cyberbullying to sexting.

Internally, there are three main strands to our approach to online safety and our work with children and families:

- **Technological innovation** to ensure there are adequate protection mechanisms for children online. These include tools like:
    - Flagging and use of AI, for example to detect child sexual abuse imagery. Last year, we developed Content Safety API, which utilises AI technology to surface for review previously unseen violative content such as CSAI. We are already sharing this technology with industry partners and other NGOs.
    - The introduction of features that help users achieve a balance in their use of technology to improve their digital well-being.
    - Family-focused products, such as Family Link. Family Link gives parents tools to supervise their child's use of Google's services and enables them to help guide their child's online experience. For example, with Family Link a parent can check how much their child has been using a certain app, they can lock their child's device if it's time to take a break or set screen time limits on their child's Android or ChromeOS devices. Parents can also limit their child app

[1]European Commission, Safer Internet Day 2017: European Commission welcomes alliance of industry and NGOs for a better internet for minors, February 2017
[2] http://www.ictcoalition.eu/, Accessed May 2019

downloads and in-app purchases from the Play Store by requiring parental approval, and they can block apps on their child's device that have become too distracting.

- **Strong policies and community guidelines** that are clear to users and are routinely enforced. We are constantly improving our safety policies — introducing over 30 changes in 2018, hiring thousands of new people dedicated to safety policy, and investing in machine learning. This investment in technology is helping us make huge progress in detection and enforcement. On data sharing, we have implemented a number of safeguards. For example, children cannot post or share content on YouTube Kids.
- **Working in partnership** to develop programmes for young people so they are empowered to live positive lives online. Our PSHE-accredited programme includes Be Internet Legends, which teaches 8-11 year olds across the UK how to use the internet more safely and responsibly, and was developed in conjunction with the NSPCC, Childnet, ParentZone, Oxford Internet Institute and Internet Matters. Since its launch in March 2018, Be Internet Legends has already reached over 50% of UK primary schools, training +1.3m children via assemblies and/or teachers. For older teenagers, our Internet Citizens workshops, run in partnership with the Institute for Strategic Dialogue, tackle cyberbullying and hate speech, among other issues. In 2018, we trained over 1,600 secondary school students, as well as 300 youth workers and teachers.

As technology but also potential threats to users evolve, we remain committed to helping improve online safety and we are constantly working to understand the problems our users are facing through research and strategies to help protect our users with updates to our products.

In line with the work described above, we set out some suggestions below that we think would help encourage and strengthen such efforts while avoiding potential unintended consequences of the Draft Code.

Scope of the Draft Code — 'Services covered by this code'

In our view, the 'Services covered by this code' section seems, in its current draft, too broad to be effective, and the criterion set out for the interpretation of 'services likely to be accessed by children' seems unclear.

'Likely to be accessed by children'

The notion of 'services likely to be accessed by children' would cover services that are not directed at children. It could potentially cover the vast majority of all online services, including an online newspaper, for example. This would extend the scope of

this Code, and in effect expand the scope of Article 8 of GDPR, to potentially every service, even those that are not directed at children or that are agnostic towards the age of their audience or users.

Additionally, the Draft Code applies to all children under the age of 18. While the United Nations Convention on the Rights of the Child ("UNCRC") defines a child as anyone under the age of 18, applying this code to all children under 18 seems misaligned with important EU and UK instruments and with other provisions of the UNCRC itself.

The UK Data Protection Act 2018 establishes that, when preparing the Code, the ICO must have regard to the UK's obligations under the UNCRC. Given that the UNCRC is an international treaty, European policymakers also need to have regard to the UNCRC and yet the GDPR sets the age of consent in relation to information society services at 16, allowing Member States to set that age between 13 and 16.

Similarly, other pieces of legislation and codes that would also need to respect the UNCRC do not take 18 as the age threshold.

For instance, the CAP Code (enforced by the ASA) is the UK industry standard for advertising and marketing communications and defines "children" as "under 16".

To provide another concrete example, the UK allows teenagers to apply for a provisional driving licence from the age of 15 years and 9 months, and for a full license from the age of 17. Many young drivers use navigation apps such as Google Maps to guide them on commutes and forecast congestion on the road; in addition, most cars today are "connected", and their built-in GPS systems could themselves come under the definition of an "information society service likely to be accessed by a child". As currently drafted, the Code would require such useful, routinely used services to be modified for teenagers 15-17 years old, even as UK law grants them sufficient autonomy to drive a car.

We also note that the UNCRC recognises the need to respect the evolving capacities of the child. Extending the code to all young people below 18 seems to disregard the abilities and needs of teenagers, and would limit their autonomy, access to information, and digital development.

In light of the above:

- We would suggest clarifying the 'Services covered by this Code' section to increase legal certainty, ensure maximum effectiveness of the Code, and avoid the unintended consequences described.
- We suggest a risk-based approach that applies the Code to services that are directed to children under the UK age of consent, in order to focus requirements on situations where they are the most needed and impactful.

The determination of whether a service is directed to children could be made based on its marketing, intended or actual audience, and/or its features. The Code could additionally note that services must, upon acquiring actual knowledge of the use of the service by children, take action to ensure compliance with the Code's requirements.

- Access to online services should in our view not be viewed unilaterally as a risk to young users, but also as an opportunity and an important tool for their education (for example, using online services to do homework or for their teacher to communicate with the class) and their safety (for example, in finding the best route home or commuting easily to an extracurricular activity). We also think the Code could recognise the special needs of teenagers and the importance of enabling them to access sensitive information privately at this crucial time in their development.
- Lastly, we would suggest consideration of the fact that third party service providers, such as enterprise cloud services, may not have knowledge of the characteristics of the end-users, for either technical, contractual, or privacy reasons. As a result, they should not be within the scope of the Code.

Overlap with other instruments

The scope of the Draft Code could also potentially create overlap and friction with other instruments beyond the remit of data protection:

For example, the AudioVisual Media Services Directive (AVMS) will require video-sharing platforms to take appropriate measures to protect children from content that may 'impair their mental, physical or moral development'. There would appear to be considerable crossover, and potentially conflict, between the ICO's Draft Code and the AVMS Directive, at least with respect to video-sharing platforms.

Another example would be the Online Harms White Paper which will help set a new framework for online safety, covering some of the issues that are being regulated by the ICO's Draft Code. In particular, Part 8 of the White Paper entitled 'Technology as part of the solution' sets out for consultation a vast array of safety by design proposals and empowers the content regulator to issue codes of practice and duties that will inform companies on how to fulfill their duty of care. Together with the other codes that deal with specific types of content and harms, this overlaps with Section 5 of the Draft Code and its requirements around content guidelines and adequate mechanisms that enforce them, for example.

Unintended consequences of the draft standards

Age-appropriate application

This standard requires that service providers apply the provisions of the Code to all users, unless they have robust age-verification mechanisms in place to distinguish children from adults.

This approach could create significant friction with the data minimisation principle under the GDPR and UK Data Protection Act 2018. Indeed, this would require that potentially every online service collect additional user data to determine whether the service is in fact 'likely to be accessed by children'.

Article 5 of GDPR requires personal data to be '*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*'. Article 11 of GDPR foresees that '*if the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation*'. Yet the Draft Code states that service providers '*may need to carry out some market research, or refer to current evidence on user behaviour and the user base of existing services and service types [...] you must be able to point to specific documented evidence to demonstrate that children are not likely to access the service in practice*'.

As the Code is currently drafted, the requirement to determine whether a service is 'likely to be accessed by a child', along with the very high bar for a provider to prove that it is not, will encourage a very broad cross-section of service providers to verify the age of all their users. In practice, it could require all services to be offered in 'signed-in mode' only. This is not only in tension with data minimisation; it would also mean, for a company like Google, rolling back some of the privacy features and protections that we have implemented.

> *Example*: Google provides users within our Chrome browser and some of our mobile apps the ability to use the service in an "incognito" mode. What that means is that the user can use the relevant Google service such that no information is further retained or otherwise associated with that particular user, browser or device. If services including Google were required to verify the user's age and retain that information in order to tailor the experience to the age bands established by the Draft Code, then incognito mode could not be offered; or the service would need to ask the user for identification before every incognito session, which would degrade the user experience considerably. Storing a flag for the user's age within a cookie wouldn't work either, as using incognito mode would delete or otherwise restrict access to

the cookie that has the age flag. A user clearing their cookies (another privacy-protecting measure available to them) would have the same effect.

In addition, the requirement to ascertain a user's age to the level of certainty required in the Draft Code is also likely to incentivise the use of 'hard identifiers' like ID documents. Indeed, the Draft Code seems to indicate that self-declaration mechanisms will not be considered sufficient. The Draft Code does not provide guidance on how to balance the requirement for 'robust' age verification and the call to minimise the use of hard identifiers.

While the Draft Code envisages the destruction of identifiers as soon as the user's age has been verified, it also asks that service providers continue to offer bespoke tools and services to young users as they transition from one age bracket to another. This would, in effect, require the retention of age information to be able to adapt the services to young users as they grow up.

The Draft Code suggests that, in order to avoid large-scale age verification and limit the collection of hard identifiers, online service providers should make their services child-appropriate by default. This could mean restricting adults' legitimate access to information and services. Even if adults were able to submit credentials to prove their age, it would still remove their ability to access that information anonymously, which they may legitimately want or need to do (for example, in the case of adults anonymously seeking access to health resources, or support regarding domestic abuse).

- We would recommend an approach focused on empowering young users and their parents with the tools to experience the Internet in a safe, concerted way, while gradually building up the knowledge and critical abilities to navigate the web as a young adult.
- In line with the language of Article 8 of GDPR, we would suggest that the Code requires providers of services that are directed to children to make reasonable efforts to verify the age of their users, and to allow for the development of varied and creative age-verification mechanisms that do not consist solely in the collection of hard identifiers or the blocking of young users from services altogether.
- We would encourage the Code to recognise that self-declaration mechanisms, when thoughtfully designed, can provide a good solution for age verification. In our experience, in designing appropriate mechanisms to confirm the age of users, it is important to recognise that information about age can be reliably solicited if certain steps are taken to ensure the "neutrality" of the age screening:

    - For example, as we mentioned in our response to the Irish Data Protection Commission's Consultation on the Processing of Children's Personal Data and the Rights of Children as Data Subjects under the GDPR, organisations should provide users with choices which are not restricted to ages above the age of consent (e.g., users should either freely enter day/month/year of birth, or use a drop-down menu that includes ages that are both under and over the age of consent).
    - In addition, a technical mechanism can also be implemented to prevent a child from back-buttoning and entering a different date of birth on the form after they have confirmed their age the first time.

- These measures can be supplemented with additional steps that organisations could take to ensure that children interacting with services are being treated appropriately while also respecting data minimisation requirements.
- Furthermore, to cover the reasonable cases in which adults may use services or portions of services directed to children, organisations offering these services should be able to treat their adult users as adults if they take steps that are reasonably calculated to ensure that the individual interacting with that service or portion of the service is not a child.
    - For example, these steps could involve prompting a neutrally age-screened individual to make an active choice to enter a PIN or other device or account credential before using a product or service considered targeted to a child. This would enable adult users to continue to benefit from a full-fledged user experience, while also ensuring continued appropriate treatment of child users.

Age grading in transparency tools

The Code as currently drafted would require services to provide different tools, privacy notices, and terms of service to users in different age groups, defined in narrow bands of 6–9, 10–12, 13–15, and 16–17.

Yet the best interests of a child in each of these bands will vary greatly from one family to the other (depending on a child's stage of maturity or development, autonomy, cultural background, and more) and in the context of different services. Age alone is not necessarily an indicator of the cognitive abilities, experience, and maturity of a child. The same content might be clear to one child and hard to comprehend for another.

There are also other important interests to keep in mind — for example the need to provide services that are accessible to people with disabilities, regardless of their age. Forcing providers into a strict framework defined only by age brackets would dramatically limit their flexibility in providing the right tools for users with special needs.

In addition, multiple sets of notices, tools and other information could carry a significant risk of causing confusion and information fatigue among users, leading them to gloss over the multiple texts presented to them and inadvertently undermining the goals of transparency and clarity. There are a wide range of mechanisms to ensure that transparency information is conveyed to children and their guardians. For example, an email directed at the child may be more effective than having separate privacy notices for each of the age tranches. Implementing tools for the exercise of rights that work for a wider audience may be more effective than making stand-alone tools for each specific age band. The latter could create confusion among users as they age up and would disregard the fact that some children have different capacities even when they are within the same age bucket.

Similarly, how prominent the transparency information is will depend on the specific characteristics of each service and the assessment of any potential risks involved. For example, 'bite-sized' notices at specific points of interaction between users and platforms, while commonly and very usefully deployed in mobile phone applications, could simply not work for all services, and making them mandatory would not necessarily achieve optimal results for users at all times.

- We share the ICO's goal of ensuring transparency for children and their parents, and implementing tools that are easy to understand and access, and can be broadly used. We think this could be achieved by implementing a principles-based approach that incentives new innovative solutions.
- Rather than establishing a limited set of options, the Code could set out the need for organisations to provide parents and children with the necessary tools and controls so that they are empowered to define how they prefer to engage with the service concerned, by choosing the privacy settings that work best for them. This would help ensure that the interests, well-being, and privacy of each specific child are adequately guaranteed. We suggest clarifying that, in doing this, organisations should determine which methods are best suited to their specific products and services, including exploring innovative ways of enhancing transparency, clarity and wide access. This would provide more clarity as well as flexibility to ensure the Code is better fulfilled and enforced.
- The Draft Code could also be amended to require online services to provide transparency resources and tools that work for the broadest possible

audience. This would require service providers to ensure these texts are drafted in as clear and plain language as possible and other communication resources are used, rather than creating a confusing proliferation of versions. It would also require service providers to ensure their tools are easy to use and access.

Default settings

The Draft Code sets out that default settings should allow only for the data collection that is essential to the provision of the service, while 'optional' uses of personal data, including any designed to personalise a service to a child or that require the processing of location information, must be off by default.

However, personalisation can, in many cases, be used to make a service more suitable to a young user. For example, personalisation can help ensure that content recommendations are better suited to the user's age. Without a measure of personalisation, there is a potential incremental safety risk of surfacing content that is inappropriate for the specific user.

More broadly, many products and services depend on a measure of contextual awareness in order to offer the functionality expected by users.

> *Example:* A London user relying on Google search to search for "football" would expect results relevant to the Premier League, rather than the US National Football League. A user searching for "Parliament" is likely to want the UK Parliament if they are in the UK, but not if they are in Canada. Serving generic, location-unaware results instead is likely to provide an unfocused answer that frustrates that user's expectation of the quality of service provided by Google Search.

> *Example:* A user who wants to use Google Maps to find the best way to the public library would expect the route shown by Google Maps takes him from their current location to the library.

Location data and location-based services can also help protect users' safety.

> *Example:* Google uses location data to understand the risk to a user's account. If a user appears to teleport from the UK to the Ukraine, that could suggest that the user's account is under attack, and Google can take steps to re-authenticate the user.

While the Draft Code does provide for exceptions where a compelling reason is provided for the choice of different settings, overall the section on default settings is drafted in a very narrow manner that calls into question whether such important personalisation or location services, or even other types of features that would

require the processing of personal data, may still be offered to UK users. It seems unclear what will or will not be considered 'essential to the provision of the service', and what the threshold is for an exception to be deemed 'compelling'.

In addition, this section seems to go beyond the GDPR by imposing a requirement that all data use considered to be 'non-essential' be subject to user consent via an opt-in setting. Article 6 of GDPR offers six legal bases for data processing and requires organisations to determine which is the most appropriate to each processing purpose. Article 8 of GDPR also recognises that consent would not be the only legal basis for the processing of children's data. Yet the Code as currently drafted would seem to impose the use of consent as the sole available legal basis for all 'non-essential' data processing. In certain cases, other bases for processing, such as legitimate interests, whereby controllers can carry out the required balancing test and put in place the appropriate safeguards, may be appropriate for data processing.

In practice, asking individuals to opt-in for all uses of information could lead to fatigue that diverts attention from the most important choices, undermining the goal of clarity, transparency, and informed user choice. For example, some data processing is necessary to make products work and to ensure they are secure and reliable. Users expect their personal information to be used in this way, and asking them to separately consent presents the odd decision of "agree" or "don't use the service." This could have the effect of teaching users to simply click "agree" to everything without paying attention. Research has found that similar dialogs can lose their ability to attract the user's attention, and the user can have a decreasing ability to acquire information from the dialog over time.

- We would suggest, instead, recognising that data controllers can determine the most appropriate legal basis for a processing purpose provided that it meets the legal requirements, and leaving controllers flexibility to design default settings in the way that best fulfills user expectations of product quality and functionality, while adequately protecting their privacy. By focusing opt-ins and other consent requests on those operations that do require consent, the user is more likely to pay close attention to the request and that consent is more likely to be meaningful.

Data minimisation

We agree with the code's emphasis on the importance of the data minimisation principle in the GDPR. We would only suggest using slightly different practical examples to illustrate the requirements of this section.

The draft discusses a map service and says it is not acceptable to track a user's location after they have reached a specific destination or closed the map. However, in

some cases, processing a young user's location when they are not actively using a map service may provide a helpful functionality.

> *Example:* Users may want to use location information for safety purposes (e.g., if a young user is going to travel to a risky area or do a more autonomous activity without their parents).

We therefore believe that there should be an option for location information to be processed only while using an app, on a continuous basis, or not at all, provided that the relevant legal requirements are met.

The draft also says it is not acceptable to process data about the music a child downloads if they are not seeking content recommendations from the service provider. Yet there may be purposes for collecting such data other than providing the user with recommendations. For example, to be able to pay royalties to content providers or for financial reporting. In addition, even offering recommendations for personalisation purposes should be aligned with data protection principles if the necessary requirements are complied with and the relevant safeguards are put in place.

- We would suggest highlighting the importance of complying with data protection principles, while at the same time ensuring that users can have the flexibility to choose the services and settings that work for them.

User engagement

The Draft Code also addresses user engagement tools, such as "likes", and seems to categorise them as "nudge techniques".

In the digital era we are in, these user engagement tools are a relevant means for users to engage in civic life and express their views.

The UNCRC guarantees children's right to express their views freely (Article 12) and to freedom of information (Article 13), including the "*freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice*".

While the collection and processing of personal data must comply with the applicable requirements, and children and parents must be provided with the necessary educational resources to be able to use these tools wisely, taking them down could have an important impact on user's right to engage online and express their opinions and ideas. We would therefore encourage an evidence-based approach that would focus on where the harm is.

- In our view, the final version of the Code should recognise these other rights at stake and the value that these engagement tools could add, in so far as the necessary legal requirements are complied with and appropriate safeguards are put in place, including data minimisation.

Implementation

The UK Data Protection Act allows the ICO to establish a transitional period of up to 12 months beginning when the code comes into force.

Implementing measures that are protective of children and guarantee their own rights to privacy, digital development, and autonomy in accordance with their evolving capacities is complex, and it is crucial for organisations to get it right. Ensuring that all of children's different rights and interests are addressed and balanced, and designing and implementing any technical changes required to do so, requires time.

- In our view, a 12-month period would be needed to ensure that the right balance is struck and organisations can implement any technical solutions needed.