Children’s data protection rights: a data protection casualty?
The UK’s Information Commissioner has identified children’s data as “a regulatory priority”. The Home Office has proposed a statutory duty of care between social media companies and children. The introduction of the General Data Protection Regulation (EU) 2016/679 (“GDPR”) last year caused a high volume of privacy policies to be updated, as companies rushed to provide certain “privacy” information to users.

GDPR mandates that data controllers provide certain information to individuals (“data subjects”) at the point at which personal data is collected from them. For those websites that target children - or those which do not, but are still likely to attract them as visitors - the bar is set higher: GDPR requires that the provision of privacy information must take into account that children have more limited awareness than adult visitors, and therefore will need a more accessible and clear framework. Despite GDPR and growing scrutiny surrounding the use of children's personal data, it appears that, in very many cases, websites and apps popular with children are ignoring this requirement. This puts those who operate those sites, or who use them to sell or promote their services, at considerable legal and regulatory risk.

Our review of a sample of privacy policies, for websites and apps popular with children, reveals that they collect a great deal of personal data from users and that they fail to communicate this in a clear and transparent way in their privacy policies. Such extensive data collection is unlikely to be appreciated and understood by children.
Children’s data protection rights: a data protection casualty?

GDPR Regulatory framework

GDPR sets out a general approach to the treatment of children’s data: “children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data” (Recital 38).

GDPR therefore identifies children as a particular group of data subjects requiring additional protection. Of course, concern about the online activities of children and their exposure to online risks is not new. In 2015, the Global Privacy Enforcement Network (an organisation of data protection authorities from around the world) carried out a sweep of websites and apps targeting, or popular with, children. It identified concerns with 41% of the websites and apps reviewed including the levels of personal information collected and how it was then shared with third parties.

Alongside enhanced obligations towards children in relation to privacy policies, data controllers should also be aware that children enjoy additional protection in other areas under GDPR, for example, where businesses intend to use children’s personal data for marketing or profiling purposes or where an individual asks for their personal data (provided when they were a child) to be erased. This report has a particular focus on the information requirements which apply to children, and so does not consider these additional protections further.

Children’s privacy – a fast moving area

More recently, press reports have suggested that children are being “datafied from birth” and tracked by thousands of apps. In February 2019, the UK Children’s Commissioner issued her proposal for a statutory duty of care between “Online Service Providers” and their young users, which was subsequently picked up by the Home Office in its White Paper on Online Harms. The White Paper recommends that a statutory duty of care be introduced, to be policed by an independent regulator who would be funded by industry. Companies will be required to demonstrate their compliance with this duty of care, including by designing products and services to make them safe for children.

The Council of Europe has issued recommended guidelines to Member States to respect, protect and fulfil the rights of the child in the digital environment. The first fundamental principle of these guidelines is that “in all actions concerning children in the digital environment, the best interests of the child shall be a primary consideration”. This has been seconded by the UK’s Information Commissioner in her proposed Age Appropriate Design Code.

Whilst not directly addressing privacy concerns, the House of Commons Science and Technology Select Committee held an inquiry on the impact of social media and screen-use on young people’s health. During her evidence, the Children’s Commissioner stated that not only are simplified terms and conditions needed, but “also the ability to report and know what to expect” from companies’ use of children’s data. There is therefore a clear and growing opinion that protecting children’s digital footprint and experience is of significant importance.

The UK’s Information Commissioner’s Office (the “ICO”) is working on its proposed “Age Appropriate Design Code”, currently in draft form (the “Draft Code”), and is consulting with parents, carers and children to finalise it. The Draft Code will provide practical guidance on the design standards it will expect providers of online “Information Society Services”, which process personal data and are likely to be accessed by children, to meet. An “Information Society Service” is defined as “any service normally provided for remuneration at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of the service” (Electronic Commerce (EC Directive) Regulations 2002). Examples include online shops, apps, social media platforms and streaming and content services. The ICO considers this definition covers most online services, even where the “remuneration” or funding of the service does not come directly from the end user. The Draft Code is applicable where children are likely to access a particular service, even if they represent only a small proportion of the overall user base.

The Draft Code contains 16 cumulative and interdependent standards of age appropriate design, including that settings should be “high privacy” by default and any parental monitoring controls should be made clear to the child. All standards must be implemented to demonstrate compliance with the Draft Code.
The first of the 16 standards is that the best interests of the child should be a primary consideration and that “it is unlikely…that the commercial interests of an organisation will outweigh a child’s right to privacy”. This is a bold and radical statement of which data controllers should be aware and is perhaps indicative of how seriously the ICO is looking to take children’s privacy. Failing to meet the data controller obligations towards children for fear of jeopardising commercial interests, or because it is too difficult to open up the black box of processing activities, is unlikely to be an acceptable justification.

Data controllers can meet this standard by taking into account the age of users, protecting and supporting their physical, psychological and emotional development and recognising the evolving capacity of the child to form their own view. The Draft Code also recommends that data controllers use evidence and advice from third party experts to understand better children’s needs and awareness. This evidence can also be helpful to data controllers when preparing their privacy policies, which may be read by children.

Baroness Beeban Kidron, a children’s rights campaigner and founder of the 5Rights Foundation (which seeks to articulate the rights of children in digital environmental), and the Council of Europe, have each noted that, as well as making clear to children how their personal data will be collected and used, data controllers must take into account that young people’s maturity and attitudes towards risk will change as they grow older. Some will embrace risk, some will avoid it and others will simply not yet appreciate it. In essence, what a data subject consents to at 13 may be different to that at 15 and 18, with young people perhaps no longer wanting to share the data they readily provided during their younger teenage years. Policies must be adaptable to respond to children’s changing needs and views in relation to the digital environment.

The ICO’s “Age Appropriate Design Code, expected to be published by the end of 2019, states: “it is unlikely…that the commercial interests of an organisation will outweigh a child’s right to privacy”
If we have children’s consent – are we ok?

The UK’s Data Protection Act 2018 provides that, if consent is being relied upon in relation to offering Information Society Services directly to a child, the child must be 13 or older for their consent to be valid. The age at which consent can be provided by a child may differ across European member states.

Where a child provides consent, the competence of the child (i.e. whether the child has the capacity to understand the scope of the data processing and the implications of the data collection and processing) must be considered. Arguably, consent is unlikely to be effective where there is complex information presented to children, or where they lack the ability to provide or withhold consent and still receive the requested services.

Companies must implement appropriate steps to verify the age of the child consenting. The exact age does not need to be confirmed, just that the child is old enough to provide his/her own consent. The Draft Code specifically states that asking a child to self-declare his/her age or age range will not constitute a robust age-verification mechanism, and companies must be able to demonstrate that children cannot easily circumvent age checks. Companies will therefore need to implement sophisticated technological solutions to identify sufficiently accurately children’s ages.

The ICO recommends that companies consider the degree of risk that the collection or use of the personal data poses to the child or others. Where the risk is low, and minimal information is being collected from the child - e.g. an email address to register for a newsletter - then asking the child to tick a box to confirm parental consent or his/her age may be sufficient. However, if more intrusive data processing activities are taking place - e.g. the child is posting personal data in an unmonitored chatroom - the ICO states that it will be necessary to verify that the child is old enough to provide his/her own consent or to check the identity of the person claiming parental responsibility and confirm the relationship between this person and the child.

Additionally, controllers must be able to show that consent to the specific processing operation taking place was “freely given, specific, informed and unambiguous”. The challenge for data controllers offering services to children is, therefore, to communicate clearly and simply the extent of their processing activities in a way that children can understand. Children can, where appropriate, consent to their data being collected and how it will be used, and understand the consequences of providing their consent, including any associated risks of the processing.

According to the UK’s Children’s Commissioner’s “Who knows what about me?” report, children between 11 and 16 years old post on social media, on average, 26 times a day.

Even where controllers do not rely on data subjects’ consent for their data processing activities, but rely on another lawful basis for processing, data controllers must still provide certain prescribed information to data subjects. This information must be in line with Article 12 GDPR, which requires controllers to provide information to users in a “concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.” Of course, this is not a wholly new requirement – the predecessor data protection regime also mandated it, although in less explicit terms. Recital 58 GDPR provides further guidance: “any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand”. The information provided should assist children or their parents to make properly informed decisions about whether to provide the information required to access the service and to continue to use it.

In all circumstances, regardless of whether data controllers are relying on children’s consent for the data processing activities, controllers must communicate their intended use of the children’s data in a clear and easily understandable manner and must not exploit any imbalance of power between them and the children. The Draft Code recommends that controllers carry out user testing to ensure that information is provided sufficiently clearly for the age range in question.

In addition, the Home Office’s White Paper on Online Harms recommends that the proposed independent regulator introduces a code of practice that sets out, amongst other things, guidance about how to ensure that terms of use are adequate and understood by users when signing up to the service. It is therefore clear that the transparency requirement will remain a key obligation with which data controllers must comply.
Privacy Policy sample analysis

Unfortunately, it appears that many websites and apps aimed at, and popular with, children do not appear to be meeting the clarity and simplicity standard. Our general review of five privacy policies for websites and apps popular with children found that the length of those policies ranged from 3,884 words to 6,016 words. All privacy policies were presented in full form, with only one providing complementary short summaries throughout the (long) length of the policy. Of course, children are not alone in being faced with impenetrable privacy policies; the majority of privacy policies aimed at adults are also incredibly dense and hard to understand.

In particular, our sample of privacy policies revealed that the websites and apps collect - or said in their policy that they collect - the following information from users, including children: substantial information on a user’s device, including signal strength and battery level; information about third party applications installed on a user’s device; information about a user’s online and offline actions and purchases from third party providers; communications with other individuals; facial recognition data; the estimated geolocation of users; photographs of users as provided to third party sites; and data in the user’s device phonebook and camera rolls.

Whilst the processing of these types of personal data is not expressly prohibited under data protection law, children may not expect this level of personal data collection, nor have a full appreciation of how organisations will use such data. With some of the policies reviewed, this extensive data collection was only explained later on within what was already a lengthy policy. It seems unlikely that young data subjects would be reading the relevant provisions. The Draft Code specifically requires data controllers to present all necessary information in a way that is likely to appeal to the age of the child who is accessing the service. This can include using diagrams, cartoons, graphics, video or interactive content that will attract and interest children. All of the policies we reviewed provide their information in text form only.

Similarly, particularly intrusive data processing activities with potentially wide-reaching consequences (for example making publicly available “shares”, “likes” and replies to posts made by child users) were generally not particularly prominent within the policies.

In relation to collecting information about children’s communications with other individuals, the Council of Europe has specifically highlighted in its Guidelines that children have a right to private life in the digital environment which includes “respect for the confidentiality of their correspondence and private communications”. We believe this particular form of data collection should be made more prominent to children.

Whilst not directly a transparency issue, the Draft Code notes geolocation data as being of particular concern. It states that geolocation options should be set off by default, with controllers considering the level of granularity of location data that is needed to provide their services, and providing an obvious sign for children when location tracking is enabled.

The privacy policies we reviewed also contained overly legalistic language, drawn of course from GDPR itself such as “withdrawal of consent”, “legitimate interests”, “Model Contractual Clauses” and “the EU-US Privacy Shield.” They also included statements that the company relies on “legitimate interest” where it believes that its use of personal data “doesn’t significantly impact your privacy” or there is a “compelling reason” for it to do so, and that the company may rely on consent “for a purpose that would otherwise be incompatible with this policy.” Use of these technical legal terms and long, vague statements is unlikely to meet the requirements of the GDPR or the Draft Code.

It has not gone unnoticed by the UK’s Children’s Commissioner who urged companies in its “Who knows what about me?” report to “put their terms and conditions in language that children understand.” The Draft Code provides guidelines for how controllers can present and tailor information according to the age of a child, warning that simplification of information should never be used with the aim of hiding how children’s personal data is being used.

It is clear from our general review of the privacy policy samples that some companies are not explaining their data processing activities in a way which is likely to meet the transparency requirements. Given the complexities surrounding current data processing activities, data controllers could be forgiven for struggling to explain their activities in a clear and transparent manner to children. Over the past few years, data processing activities have become increasingly complex, with data being collected from various sources including from data subjects themselves, websites and apps. However, given the heightened scrutiny surrounding children’s data, data controllers would be well advised to simplify their privacy notices in line with the GDPR and the Draft Code requirements.
Remember the virtual assistants

Children are not just interacting with websites and apps, but often also with “virtual assistants” being used in their homes. These virtual assistants may well be collecting children’s data, forming profiles of children and combining children’s data with adults’ data in increasingly complex ways. The Draft Code highlights connected toys and devices as requiring further consideration, as their scope for collecting and processing personal data is considerable. Children are also more likely, innocently, to give virtual assistants lots of information about themselves. They need a clear and simple explanation of what it means to provide virtual assistants, and similar technology, with their information. In 2017, Mattel cancelled its own virtual assistant for children amidst privacy concerns. There has recently also been growing debate over Amazon’s use of children’s data with the Amazon Dot Echo for Kids. Children and privacy activists have filed a complaint with the Federal Trade Commission, claiming that the Amazon Dot Echo for Kids is unlawfully recording children’s conversations without their consent, alongside two private claims against Amazon on similar grounds.

In the UK, the Draft Code suggests that, where a toy collects any video or audio material generated by a child, this should be made explicit on a prominent part of the packaging or accompanying information. Data controllers should provide clear information about the use of personal data at the point of purchase and on set up of the device. This would likely require a privacy notice to be provided on an online check out page, as well as on the physical packaging and instruction leaflets. The Draft Code recommends that any online information be provided without consumers having to purchase and set up the device, allowing them to make an informed decision in advance about whether to purchase. Data controllers should also anticipate that their connected devices may be used by multiple users of different ages, in particular that children may use the devices unsupervised, and are advised, in the Draft Code, to avoid any passive collection of personal data. These high profile concerns highlight the importance to data controllers of making the scope of their data processing activities clear to data subjects, particularly children and young people, and disclosing such activities as early as possible.

Again, given the complex way in which data controllers collect and use personal data, they could be forgiven for failing to provide this information clearly. However, complexity is unlikely to be a sufficient excuse for failing to comply with GDPR and the Draft Code.
Is a new regulatory regime inevitable?

Whilst there has been no formal investigation in the UK into an organisation that has failed to communicate its processing activities clearly to children, the Children’s Commissioner, in her “Who Knows What About Me” report, has issued calls for the UK government to monitor the situation and refine data protection laws, if required, to protect children. The Children’s Commissioner stresses that government, industry, regulators and other players will need to be able to respond quickly as we understand more about the impact of children’s data collection. This mirrors the Council of Europe’s suggestion that “each State should apply such measures as may be necessary to require that business enterprises meet their responsibility to respect the rights of the child in all their operations within the State’s jurisdiction”. Could these be the first signs to paving the way to legislative solutions?

The ICO, in its Draft Code, also alludes to a more active regulatory role in respect of children’s data protection. The ICO seeks to monitor compliance with the Draft Code through “a series of proactive audits”, as well as considering any complaints. Failure to comply with the Draft Code will render it difficult for controllers to demonstrate that their data processing is fair and in line with GDPR.

Parents take note - it’s not just companies that should be aware of children’s rights!

Alongside the concern around companies’ use of children’s personal data is a growing awareness around the dangers of “sharenting”. “Sharenting” is the trend of parents habitually using social media to share news, images and other personal information of their children. This is an increasingly complicated area, particularly where children are old enough to be able to consent (or not) to their information being uploaded by their parents and arguably should have a say over whether particular information is made public.

A survey by VotesforSchools found that children were concerned about being embarrassed or the period for which the content would remain online. This in addition to the increased risk of personal identity theft, which is made easier through the sharing of children’s online details; in fact, Barclays is predicting that “sharenting” will account for two-thirds of identity fraud facing young people by the end of the next decade and will cost £667m per year. Mishcon de Reya’s project on sharenting, which explored children’s views on the issue, similarly identified concerns from children around parents’ sharenting habits. Even celebrities are not immune to “sharenting” concerns, with Apple Martin publicly criticising her mother, Gwyneth Paltrow, for posting a photo of her online without her consent.

Parents should therefore consider the privacy risks to their children, when considering making public their children’s personal information.
Practical suggestions

As a general approach, data controllers should consider the perceptions, expectations and experiences of their young users, and acknowledge and respect that data controllers have the greater power. Specific tips for organisations targeting young people include:

— consider young people from the outset, when preparing privacy policies and undertaking data processing activities, and have the best interest of the child as a primary consideration when designing and developing online services; for example, where a child elects to share some information, include a child friendly explanation of the consequences and risks of sharing;

— use a data protection impact assessment to identify, assess and mitigate any risks to children and consider children’s views in relation to proposed data activities;

— include additional, specific “bite sized” explanations about how you use personal data at the point at which that use is activated;

— avoid age verification methods that can be easily bypassed by children e.g. asking users to select their birth year or to tick a box (the ICO has recognised that the ability to verify age may be dependent on the availability of suitable technologies and that verification will become easier over time as the technology becomes more available. Companies should regularly review available age verification mechanisms to ensure that they are using appropriate current technologies);

— appreciate that, just because young people can access the services, does not mean that they can understand the implications of the services;

— do not prevent young users from using the services if young people do not agree to particular uses of their data;

— have different versions of a privacy policy, where the intended audience covers a wide age range. Where there is only one version of the privacy policy, it should be understood by the youngest age range;

— have privacy settings set at the highest level by default, for example having the geolocation options off by default (unless a compelling reason can be shown for a different default setting, taking into account the interests of the child);

— offer young people an ability to agree or withdraw their consent to specific uses of their data over time (for example, through a data processing control dashboard);

— design processes so that, to the extent possible, it is easy for a child to request the deletion of their personal data and for companies to comply with these requests where possible (a recent report has found that children wanted their social media profiles to be wiped clean at 18); and

— provide information to young people in different and appealing ways, from short video clips to animations to icons (GDPR specifically suggests using icons).

Data controllers should appreciate that it will not be an easy task to communicate their data processing activities to children and young people, particularly as these activities are likely to be complicated. There are also bigger questions to consider: when is a child not a child anymore? How do we present risks to young people when they have different capabilities across their age bands? How should data controllers assess threats to young data subjects? Data controllers should expect the analysis to develop as these societal questions are debated. In the meantime, given the increasing awareness around data collection, sharing and usage, data controllers providing services aimed at or used by young people should consider the clear message of the 5Rights campaign that “a child is a child until they reach maturity, not only until they reach 18.”

Children’s data protection rights: a data protection casualty?
The information in this document is given without financial or other liability on the part of the writer or Mishcon de Reya LLP. This firm cannot be held responsible for any errors contained in this document. This document sets out findings following an analysis of open source, publicly available material. No reliance should be placed on this document in whole or in part by other parties.