Information Commissioner's Office

ICO submission to the inquiry of the House of Lords Select Committee on Communications into Children and the Internet

1 September 2016

ico.
Information Commissioner's Office

Contents

Introduction

Specific questions

About the ICO

The ICO's mission is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The ICO is the UK's independent public authority set up to uphold information rights. The Information Commissioner does this by promoting good practice, ruling on complaints providing information to individuals and organisations and taking appropriate action where the law is broken.

The ICO enforces and oversees the Freedom of Information Act, the Environmental Information Regulations, the Data Protection Act and the

Privacy and Electronic Communication Regulations.

Introduction

Thank you for the opportunity to take part in this important consultation.
We agree that the protection of personal data can pose a problem for children using the internet, in that there is a risk that their data may be collected or shared without them being aware of this. We also share your concern that the online activity of children may remain visible to future employers or academic institutions.

In answering your specific questions we have confined ourselves to discussing matters that fall within our area of statutory responsibility, primarily as regulator for data protection law in the UK. These important challenges will not be addressed by the law alone, a broader strategy including the law, digital citizenship and education is required.

Specific questions

Risks and benefits

What risks and benefits does increased internet usage present to children with regard to data security?

The Data Protection Act 1998 (the DPA) requires organisations offering online services to children – and to other individuals - to put appropriate security measures in place. The law does not contain specific provisions relating to the security of children's data – security must be appropriate across all systems including front line and back office, online and offline, regardless of the age of the data subject. A system that keeps an adult's personal data appropriately secure, would also keep a child's personal data appropriately secure. The real difference lies in a child's ability and experience of identifying or recognising the systems of a poor performing or non-compliant data controller, prior to taking a decision to provide his or her personal data to a particular website. They may also be unduly incentivised or subjected to peer pressure to use a particular service, and may be more likely to spend more time online and therefore generate greater volumes of data to be stored and further processed "in the cloud".

Whilst there is no specific provision in the DPA specifying a higher standard of data security for a child's personal data in determining what is "appropriate" the ICO would expect a data controller to take into account the obligations associated with processing of a child's data imposed by society and thus should have a high level of security and privacy by default.

There is also a broader issue of the fate of personal data once a child has published it, for example on a social networking site. Although the rules of data protection may still apply to the further collection, use etc. of the data, in reality there may be little that can be done to prevent unscrupulous third parties from harvesting a child's data and using it for inappropriate purposes. The ICO is active in detecting and pursuing list-brokers and others who may engage in this sort of practice. However, our message to children, and their parents or guardians, is that once a child's personal data has posted – particularly publicly - it may be highly challenging to control what happens to it subsequently. The best protection for children is for their 'risky' personal data not to be put into the public domain in the first place. Therefore education also has a key role to play.

Risks are also present when data is intended to be shared privately, e.g. within a closed group or on a one-to-one basis, and where security settings are insufficient to prevent the wider sharing of material which was meant to remain private.

Many of the online services used by children are not specifically designed for children. What problems does this present?

This question touches on a major area of difficulty for the regulation of children's personal data online. A good example of the issue is contained in the General Data Protection Regulation (GDPR). The GDPR contains several provisions aimed at the protection of children's data. Essentially the GDPR seeks to introduce an age-based approach to protection, meaning that a child cannot consent to use an 'information age service' offered directly to him or her; there must be consent from the holder of parental responsibility.

Although the wording is not entirely clear, we take this provision as applying to commercial internet services specifically targeted at children. If such an approach is adopted in UK law, we think it could be difficult to apply in practice. There are services that are obviously aimed at children (e.g. Club Penguin or CBBC) and ones aimed at adults (gambling sites). However, in the middle of the spectrum there is a wide range of services – for example social networking, online video, marketplace and gaming sites - which are essentially age-neutral and are used by both children and adults. This leads us to be sceptical about seeing an approach that seeks to differentiate between children's and adults' sites as being in itself a solution to the problem of children's online protection.

Instead we would prefer a more flexible approach, meaning for example that social networking sites should explain their data collection practices in language that all users of their services are likely to understand and to invest in a high standard of security for all users. This should also include privacy settings by default (e.g. publication of data). Of course, where it is clear that a service is aimed at children then the way the service is offered and the way it is explained must be age-appropriate. A young child, for example, would be unlikely to understand the implications of their details being passed on to a third party data brokerage – however clearly that is explained. In our view services that are clearly aimed at children should not engage in data sharing of this sort, no matter how simply the relevant choices are explained. (Of course the inappropriate harvesting and use of children's data can lead to inappropriate contact with children, for example the sending of PII or vehicle accident lead generation messages.)

We advocate a risk-based approach to ensure that the potential privacy intrusion of different data collection and usage scenarios is assessed. Organisations are encouraged to use Privacy Impact Assessments (PIAs) to assess potential harms and solutions to mitigate. This should enable privacy protections to be considered when a service is being designed – an approach known as privacy by design. The ICO has developed a Code of Practice for Privacy Impact Assessments. Organisations processing significant amounts of personal data related to children should be regularly using PIAs. A requirement to conduct Data Protection Impact Assessments is part of the new GDPR.

Alongside the obligations organisations have to process personal data in accordance with Data Protection laws it is also very important to focus on education. This should include the creation of safe spaces for children to explore and develop online. Of course parents and guardians should play a role in the protection of children's data in contexts such as this.

What are the technical challenges for introducing greater controls on internet usage by children?

There are a number of challenges in this area including identification and authentication, but also ensuring that any controls that are considered necessary and proportionate are effective in delivering the benefits that they promise.

For example, introducing web-filtering software, either in the home router or within the Communications Service Provider's network can help with the creation of a safer online experience for children. However its effect may be weaker than billed because but it may fail to deal with the multitude of different ways that a child can access the internet (i.e. home, school and public Wi-Fi as well as personal mobile phones). Children can also have an extensive peer group and quickly share tips and techniques on how to circumvent such controls. This can result in a false sense of security for the parent or guardian.

Another problem surrounds age-verification which is often used by a data controller to prevent access to a group of individuals below a specific age. An age-verification system is possible – for example based on the provision of an individual's credit card or other 'adult' details but authentication is a complex problem for all online services without also processing excessive or disproportionate amounts of personal data. Simple age verification systems can suffer from similar problems as web-filtering software in that they can create a false sense of security for data controllers and parents alike. Basic systems requiring the user to input a date of birth can be easily circumvented. More advanced systems requiring a valid credit card (by definition only issued to over 18's) can also be obtained by a resourceful child.

From a privacy point of view, we are concerned that introducing an age-verification system could lead to service providers collecting 'hard' personal identifiers about all internet users, not just the children which they are attempting to prevent access certain services which they would not otherwise collect. Many services are accessed through the use of relatively low-risk identifiers – aliases for example – and service providers may only collect relatively low-risk identifiers such as users' IP addresses. The implications of moving more widely to an age-verification system based on the collection of names, addresses, credit card details and so forth need careful consideration.

Federated ID management should be considered a privacy friendly solution, for example the UK Government's Verify system. When you use this system to access a government service, you choose from a list of companies certified to verify your identity. Information is not stored centrally, and this reduces the amount of information shared. The company you choose doesn't know which service you're trying to access, and the government department doesn't know which company you choose.

Despite the above, we can see some advantages of imposing an age-limit for accessing certain online services. At least the approach would be simple – people under a certain age would not be able to use social networking sites without parental consent, for example. This would mirror the way the sale of age-restricted goods such as alcohol or cigarettes is regulated – where the mental competence of the prospective purchaser is not an issue. However, on balance we favour an approach where even quite young children can access appropriate online services without the consent of a parent or guardian, provided organisations have taken other safeguards. In our view a child should be able to take part in an online activity that presents little or no privacy risk and is of such a nature that the child in question is capable of understanding the implications for him or her. A good example might be accessing a pop-star's website and subscribing to a newsletter. (Of course children must be able to access confidential counselling services such as Childline without parental involvement.)

What are the potential future harms and benefits to children from emerging technology, such as Artificial Intelligence, Machine Learning and the Internet of Things?

The issues for children are much the same as those for adults, although as previously stated children may be likely to adopt online services earlier or spend longer periods of time using them. In short, we believe that more information about individuals is being collected. It is being shared more widely and is being analysed in more sophisticated ways. We do not necessarily see this as a negative phenomenon, provided that individuals are given an appropriate degree of transparency, choice and control at appropriate points in their online activity. However, providing this to children can be difficult or impossible, and of course it may be impossible to differentiate between an adult or a child user. As with our example of list brokerage above, we doubt whether a child – particularly a young one – could understand the implications of using an internet-connected smart device such as a TV or a fridge. This does not mean that children should be prevented from using such devices. It does mean though that there needs to be a suitable supervision, education or configuration by a parent or guardian and that when making privacy choices – for example whether to enable a particular connectivity feature of a device – the responsible adult takes the privacy implications (if any) for his or her children into account.

Education

What roles can schools play in educating and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?

The ICO has championed the raising of information rights awareness in our schools. We believe that it is important that children understand their online 'information safety' early on in their lives, given their early exposure to the internet.

This link: https://ico.org.uk/for-organisations/education/ leads to content aimed specifically at teachers and children. It includes an information rights video for schools and a series of lesson plans intended to help children understand the value and importance of their personal information, how to look after it, and the obligations organisations have. There is also a dedicated part of our website aimed at schools, universities and colleges.
We believe that the ICO's activity in this area will contribute to information rights becoming a mainstream part of every child's education. However, as we have seen in other areas such as sex and drugs education, we should not assume that all teachers are experts in this area. They may need ongoing support, and the training materials needed to provide effective e-safety to children. (Parents may also need similar support.)

Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed about risks?

In data protection terms, all organisations collecting children's personal data have a legal duty to ensure the data are processed in a way that is 'fair'. In our view, this can extend to organisations having to ensure that parents and guardians are aware of the risks and implications of data about children being collected – for example whether it will be made publicly available or whether it will be used for marketing purposes. This can be achieved through a combination of techniques for conveying privacy information, depending on the medium and the general circumstances.

The duties under the DPA are somewhat different to a duty to teach e-safety to parents. However, the DPA's transparency and fairness requirements can contribute to parents' education. As a general policy approach, the ICO has always championed the provision of clear, plain English, genuinely informative information to parents, children and other service users. Making sure that organisations adopt this approach will contribute to a better understanding of e-risk on the parts of adults and children.

We note that some commercial organisations are providing a degree of transparency and control, for example through ‘dashboard’ type mechanisms which may exceed the requirements of data protection law. We are keen to encourage the development of techniques such as this. To that end, we are in the process of revising our Privacy Notices Code of Practice, to give more prominence to these state-of-the-art transparency and control mechanisms.

Governance

What are the challenges for media companies in providing services that take account of children? How do content providers differentiate their services for children, for example in respect of design?

As we have explained above, providing transparency and consent mechanisms to children presents particular challenges, not least in the determination of whether a particular user is a child or not. However, generally simpler language and perhaps a more visual way of explaining information choices might help to protect and empower children. Again, our revised Privacy Notices Code of Practice very much promotes this approach. More specifically, when a child is offered an information choice – for example whether his or her data can be made available publicly or only within a limited group, then the choice mechanism should be both prominent and easy to understand. In addition, there should be a clear positive action by the child indicating that he or she has agreed to a particular proposition; in this context consent should not be inferred from inaction.

Legislation and Regulation

What are the regulatory frameworks in different media? Is current legislation adequate in the area of child protection online? Is the law routinely enforced across different media? What, if any, are the gaps? What impact does the legislation and regulation have on the way children and young people experience and use the internet? Should there be a more consistent approach?

We see one of the strengths of data protection law as being that it has a basic set of rights and principles that apply equally to all individuals, to all the situations where personal data are processed, regardless of the media used. We believe that the current law provides us with the powers needed to carry out effective enforcement and to promote good practice in relation to children’s personal data.

One problem area concerns the DPA’s personal, family and household exemption. This largely dis-applies the DPA in respect, for example, of information someone posts online for personal reasons. The ICO frequently receives complaints about matters such as false and derogatory social-media pages being set up, or hurtful or threatening posts appearing on chat sites. These are often the result of some form of personal animosity. The data processing by the individuals involved will often fall within the terms of the DPA’s ‘personal processing’ exemption so – in reality – there is often little the ICO can do to regulate this part of the internet in terms of the people who post the information. Criminal sanctions and a role for the Police will always be needed for the most serious cases. The ICO is not saying that there is a complete lack of regulation in this area or that it wants to become responsible for policing the content of social media and similar sites or to become the arbiter of personal disputes. However, we invite the Committee to consider this issue carefully, perhaps service providers should be encouraged – or required - to do more to clean-up problematic content from their networks. Most large social media companies do have some form of ‘take down service’ where individuals can comply but the volumes they have to handle are high and freedom of expression issues can be challenging to adjudicate on in some cases. We stress the need to work with other regulators and educators to provide a form of protection to children that is as comprehensive as possible.

It is important to consider the legal responsibility of publisher organisations that merely host content that others post or provide links to other publishers (i.e. a search engine), with no form of editorial control or moderation. Technically, if they process – i.e. host – personal data that are inaccurate, for example, then they will breach the DPA unless they have taken reasonable steps to ensure the accuracy of the data. However, how realistic is this for a social networking site that may host hundreds of millions of posts or even more? We believe that the responsibility of publisher organisations in this area needs further exploration, in terms of determining the most effective remedies for children who have been the victims of information posted about them by another private individual. Our experience of dealing with search engine ‘right to be forgotten’ delisting cases suggests that the taking-down of problematic search results can minimise the impact of, for example, damaging social media content on individuals. We think it important that children are aware of their deletion rights and have a simple means of exercising these.

The ICO recognises fully the need for a personal family and household exemption given the importance of ‘private informational space’. We also note that the interface between the DPA’s privacy protections and its provisions intended to protect freedom of expression add an additional level of complexity to this issue; one person’s hurtful posting may be another person’s freedom of expression.

What challenges face the development and application of effective legislation? In particular in relation to the use of

national laws in an international/cross-national context and the constantly changing nature and availability of internet sites and digital technologies? To what extent can legislation anticipate and manage future risks?

This could be a significant problem area. As it stands, most of the major providers of online services (search engines, social networks, gaming sites etc.) have some form of establishment in the UK (or EU). On the whole they seem committed to complying with local laws, including data protection law. So for the moment – within the EU at least – we are confident that we have a coherent set of laws that provide reasonable protection to children using online services.

However, there could clearly be problems where children use internet services provided by companies outside the EU and that are not required to meet EU-style data protection standards. It is questionable how much protection the ICO, or other EU data protection authorities, could deliver to individuals in respect of such companies. Although we can – and do – seek to resolve problems with overseas organisations, we must recognise the challenges we could face in carrying out any meaningful enforcement action should an organisation fail to cooperate voluntarily.

Given the methods individuals can use to register, operate and access online services we are aware of the problem of tracking down some organisations' physical location or those of the individuals who may misuse those services to cause harm to others. This might be a company making marketing calls to people registered with the Telephone Preference Service or an individual using an anonymisation service to post illegally obtained material on a social networking site.

However, the ICO is helping to develop more effective international co-operation mechanisms, for example our role in leading the Global Privacy Enforcement Network (GPEN). This is a global group of around 60 privacy enforcement authorities. Its objective is to develop better co-operation mechanisms and to learn how best to carry out effective enforcement when faced, for example, with a company that causes problems for individuals across the world. In 2015, 29 GPEN members conducted a 'privacy sweep' to look at websites and apps targeted at, or popular among, children. The project raised concerns about 41% of the 1,494 websites and apps considered, particularly around how much personal information was collected and how it was then shared with

Does the upcoming General Data Protection Regulation take sufficient account of the needs of children? As the UK leaves the EU, what provisions of the Regulation or other Directives should it seek to retain, or continue to

implement, with specific regard to children? Should any other legislation be introduced?

The extent to which future UK data protection law will replicate the GDPR is currently uncertain. However, the GDPR contains specific provisions intended to protect children's data online. As explained above, it does this by invalidating children's consent, and requiring parental or guardian consent, before information society services can be accessed by a child. (A child can be defined on a Member State basis as anyone below the age range of 13 – 16 years.).

During the passage of the GDPR the ICO expressed its reservations about a broad age-verification / parental consent model that did not take account of risk. This was in terms of workability and effectiveness as a protection. Whilst not ruling out such a system completely, we continue to favour an approach that takes into account the nature of the service being accessed and the child's ability to understand the implications of using it.

Data protection law can still provide protection for children without having specific provisions relating to them, just as it can offer protection to other groups who – for whatever reason – may have a relatively limited level of understanding. However, there could be advantages in including specific child-protection provisions in future data protection law provided they are drafted in a realistic, flexible way and offer genuine protection to those that need it.

What more could be done by the Government? Could there be a more joined-up approach involving the collaboration of the Government with research, civil society and commerce?

Generally, we think Government should continue to recognise that the online protection of children is a multi-faceted issue that needs a co-ordinated response from the various agencies, departments and groups with an interest in the area. Data protection provides specific but effective protection to children but – for some of the reasons we have set out above – it is only part of the answer. The ICO will continue to recognise the importance of children's privacy and to work with the Government to ensure a coherent and joined up approach that results in an effective and comprehensive privacy protection system for children using the internet.

House of Lords Select Committee on Communications inquiry into Children and the Internet

For further information on this submission, please contact Iain Bourne, Group Manager on 01625 545325 or email iain.bourne@ico.org.uk

If you would like to contact us please call 0303 123 1113.

www.ico.org.uk

Information Commissioner’s Office
Wycliffe House, Water Lane
Wilmslow, Cheshire, SK9 5AF

ico.
Information Commissioner’s Office