

Irish Heart Foundation

**Comment on the Concept Note for a General Comment on children’s rights in relation to the digital environment**

May 2019

**Who are we?**

The Irish Heart Foundation is the national charity dedicated to eliminating premature death and disability from heart disease and stroke through:

* campaigning and advocacy to change the public policy environment and improve services;
* primary prevention and health promotion to change health behaviours;
* building a nation of lifesavers through CPR training in schools, communities and workplace;
* supporting people living with the effects of stroke and heart disease.

**Introduction**

The Irish Heart Foundation welcomes the opportunity to comment on the concept note of the General Comment on children’s rights in relation to the digital environment. The Irish Heart Foundation (IHF) promotes policy changes that reduce premature death and disability from cardiovascular disease (CVD). A number of the risk factors for CVD have been shown to be influenced by developments in the digital world. The rapid evolution of online platform capabilities and the sophistication of new forms of commercial communication has sparked the need for concrete action to be taken to protect children from exploitation and harms.

The Irish Heart Foundation sees an important role for data protection law in protecting children from privacy risks, loss of reputation, commercial exploitation of personal data, profiling and cyber harassment. Indeed, there is significant scope for the Data Protection legislation to recognise and support the position that children hold in the advertising ecosystem, as articulated by UNICEF: “that of rights holders, entitled to be protected from violations of their privacy and deserving an Internet free from manipulative and exploitative practices.”[[1]](#footnote-1)

Due to the current complexity of the regulatory framework on commercial communications – which covers media law, consumer protection law, e-commerce law and data protection law – policy makers and legislators are being faced with increasing difficulties in how to provide accountability mechanisms, and regulate for, commercial communications that appear across various platforms (traditional media and internet content).[[2]](#footnote-2)

The comment of the Irish Heart Foundation will focus mainly on the protection of privacy, identity and data processing, using the example of the transposition of the GDPR in Ireland through the Data Protection Act 2018 as an example that can contribute to the drafting process for the General Comment.

**Digital Protection for Children**

While the online environment presents significant opportunities for children and young people to enjoy and exercise many of their rights, it also presents challenges with regard to safeguarding children and young people’s privacy rights and risk exposure. As a generation of digital natives, children and adolescents have been observed to be “either intentionally providing or unconsciously ‘bleeding’ increasing amounts of their personal data online.”[[3]](#footnote-3)

This concern has been recently echoed in a complaint made to the Irish Data Protection Commissioner, which highlights the need to protect individuals from wide-scale and systematic breaches of the data protection regime. The principal concern of the complaint, which the Irish Heart Foundation would support, is that the current frameworks and policies relating to the industry fail to provide adequate protections against unauthorised, and potentially unlimited, disclosure and processing of personal data. Particularly of concern would be the “Europe Transparency & Consent Framework” developed by the Interactive Advertising Bureau (IAB) trade association, as well as its “GDPR Transparency & Consent Framework” which, it is pointed out, recognise that once an individual’s data is broadcast, the data controller (and, therefore, the data subject) loses all control over how that data is used and that there are no technical measures in place to adequately protect the data. In the complaint to the Data Protection Commissioner, three causes for concern were identified[[4]](#footnote-4) which are equally applicable to this consultation:

“First, what started as an industry focused on assisting with personalised advertising has spawned a mass data broadcast mechanism that:

1. gathers a wide range of information on individuals going well beyond the information required to provide the relevant adverts; and
2. provides that information to a host of third parties for a range of uses that go well beyond the purposes which a data subject can understand, or consent or object to.

There is no legal justification for such pervasive and invasive profiling and processing of personal data for profit.

ii. Second, the mechanism does not allow the industry to control the dissemination of personal information once it has been broadcast (or at all). The sheer number of recipients of such data mean that those broadcasting it cannot protect against the unauthorised further processing of that data, nor properly notify data subjects of the recipients of the data.”

In light of this, the need for adequate safeguards to be in place to ensure the integrity of children’s personal data is critical.

A major trend in the area of commercial communication is the use of personalised advertisements, where the collection of personal data of users harvested from online behaviours and preferences is used to tailor specific messages and advertisements to consumers.[[5]](#footnote-5) Personalisation, profiling and behavioural targeting have quickly become the norm across digital and online platforms, creating opportunities for commercial use of children’s data.

Reliance on digital consent as a means to protect children’s data is not sufficient. Nor is the development of codes of conduct that are not legally enforceable or subject to sanctions for non-compliance. We know that children’s choices and data control possibilities are shaped by the design and functionalities of communication spaces, control of which rests neither with them, their parents or indeed national regulators.[[6]](#footnote-6)

As our online presence increases and we migrate much of our social, economic and functional activities into the digital space, we are becoming increasingly ‘datafied’, with a proliferation in commercial bodies seeking to capitalise on and profit from our personal data. Indeed, the use of social networks and these social media platforms by children and adolescents can be seen as means to satisfy the need for information, friendship, and connection.[[7]](#footnote-7) For children and adolescents, for whom online platforms are especially popular for social and peer engagement, online behavioural advertising is often accepted simply to avoid exclusion from the service and wider social networks. However, this cannot justify the increased commercialisation and commodification of children’s personal data. The advent of digital advertising, coupled with the increasing leakage of children’s data online, corresponds with a growth in the technical capability to send a different advertisement to each child, based on the individual characteristics of that individual customer or ad impression.[[8]](#footnote-8) Ultimately it enables the precise targeting of children, many of which may be more vulnerable and susceptible to the marketing and advertising that is being transmitted to them.

***Sophisticated techniques at play***

Rapid technological developments have made it possible for companies to collect, process and interlink data in previously unimagined ways and this data is used by companies for various purposes, such as personalised services and marketing.[[9]](#footnote-9) This has come increasingly to the fore in recent times as a result of the UK Parliamentary Committee Report into Disinformation and Fake News. In its report, the House of Commons Digital, Culture, Media and Sport Committee found that

“*what does need to change is the enforcement of greater transparency in the digital sphere, to ensure that we know the source of what we are reading, who has paid for it and why the information has been sent to us. We need to understand how the big tech companies work and what happens to our data. Facebook operates by monitoring both users and non-users, tracking their activity and retaining personal data. Facebook makes its money by selling access to users’ data through its advertising tools. It further increases its value by entering into comprehensive reciprocal data-sharing arrangements with major app developers who run their businesses through the Facebook platform.”[[10]](#footnote-10)*

Digitalisation has facilitated the pairing of data about customers’ online activities with data about their offline activities, allowing advertisers to more accurately target customers across a range of media.[[11]](#footnote-11)

Of special importance, is the fact that every time a person is shown a behavioural advertisement, intimate personal data that describes each visitor, and their online activities, is broadcast to tens or hundreds of companies. It has been pointed out that advertising technology companies broadcast these data widely in order to solicit potential advertisers’ bids for the attention of the specific individual visiting the website.[[12]](#footnote-12) This then has the effect of exposing children’s personal data as these bid requests often fail to protect these intimate data against unauthorised access. Some of the personal data broadcast during real-time bidding advertising include:

* What you are reading or watching
* Your location
* Description of your device
* Unique tracking IDs or a “cookie match” to allow advertising technology companies to try to identify you the next time you are seen, so that a long-term profile can be built or consolidated with offline data about you
* Your IP address
* Data broker segment ID, if available. This could denote things like your income bracket, age and gender, habits, social media influence, ethnicity, sexual orientation, religion, political leaning, etc.[[13]](#footnote-13)

Similarly, the increasingly invasive nature of data collection is evident in the methods and techniques employed. Indeed, information and data can be collected through a number of mechanisms, often unbeknown to us:

* Online browse and search habits
* Online tracking through use of cookies
* Mobile tracking & location services
* Transfers of personal information necessary to join social media apps and games
* “Dataveillance practices via wearable and mobile devices”[[14]](#footnote-14)

From this, it is possible for sophisticated profiles to be developed that not only facilitate the categorisation of individuals, but it is also possible to predict preferences or future behaviours based on clever statistical methods derived from the use of algorithms.[[15]](#footnote-15) In their research on children and digital marketing, UNICEF note that this process is referred to as ‘identity resolution’ – the creation of a single view of the customer across platforms and media in order to serve advertising that is far more personalised, targeted, relevant and effective than ever before.”[[16]](#footnote-16) In the paper *Keeping Consumers Safe Online Legislating for platform accountability for online content*, the damaging link between personalisation and harmful content is highlighted as the use of tools and algorithms allow intermediaries to ensure individuals get the particular content that maximises their value from the service, which has a dangerous potential as “the greater the degree of personalisation, the more opportunities exist for providers and consumers of harmful content to find each other, often largely unseen by other platform users”.[[17]](#footnote-17)

**Children’s Rights in the digital environment and Protecting Children – The example of Section 30 of the Irish Data Protection Act 2018[[18]](#footnote-18)**

The key purposes of the Data Protection Act 2018 include giving further effect to the GDPR in areas in which Member State flexibility is permitted and to transpose the Directive into national law. The GDPR aims at regulating the processing of personal data – creating parameters around its acquisition, use, storage and sharing.

The text of Article 6(f) of the GDPR states that the legitimate interest of the data controller may be “overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.” However, no clarification is currently provided as to how this protection should be envisaged or afforded. The newly inserted Section 30 aims to protect children from the effects of direct marketing and profiling. Indeed, it has the effect of placing an onus on industry to ensure that a child’s data is not used for marketing or commercial purposes.

As previously mentioned, it is not sufficient to rely upon parental consent to protect children’s data from exploitation and aggressive marketing techniques. Adults, nevermind children, experience difficulties in recognising commercial messages which undermines their ability to process their appeal in a critical manner. It is important to recognise the responsibility of social media platform providers given their increased use of profiling, complex recommender systems and automated content classification mechanisms. Indeed, given that online behavioural advertising is achieved through the use of persistent identifiers, such as IP addresses and cookies, there is a greater onus on these platforms to take responsibility.

The dangers presented to children in respect of the internet and online platforms must be expressly recognised in legislation, particularly in the context of personalised advertising campaigns, as companies know far more about them than they (or indeed their parents) know about the business models and the form and delivery of personalised marketing. The targeting of particular categories of people on the basis of personal profiles can arguably have a manipulative effect. This is especially true for children. For example, a cursory glance at the logic behind advergames- the gamification of commercial communications by integrating them with non-commercial content makes it nearly impossible for impressionable and young children to understand that they are being targeted with advertising.

Section 30 of the Data Protection Act 2018, once amended and commenced, will have important implications in the area of digital marketing, and social media companies will now have an onus placed upon them to ensure that profiling of a child for marketing purposes is prohibited. The section has not yet been commenced and will need minor amendment, but the principle is compatible with GDPR. An amending Bill has been tabled that will make the section both GDPR and constitutionally compliant.[[19]](#footnote-19) Indeed previously, the Minister for Justice and Equality, when asked if legislation could be introduced to put the onus on social media companies in the Oireachtas Committee on Children and Youth Affairs hearings on Cyber Security for Children and Young Adults noted: "Yes, I think we can do more in that area and I think we should explore it."

The prohibition of profiling in national and European law has the potential to abate the commercial exploitation of children’s data that is evidently happening through complex marketing, tracking and targeting systems used by many online platforms. Such systems have been widely reported on and are known to monitor and monetise people’s online behaviour and interactions. The Irish Heart Foundation believes that the restrictions on the collection of children’s data as contained in Section 30 “would be better suited to diminishing its commercial exploitation in complex marketing, tracking and targeting systems, than parental consent.”[[20]](#footnote-20)

**Conclusion**

Concerns about children’s privacy and the processing of children’s personal data should include their exposure to inappropriate content and the commercialisation of childhood. Children need special protection as their cognitive abilities are still developing and are less likely to understand how their data is being used nor recognise how this then translates into marketing communications that are being targeted at them.

Whereas traditionally, children had been reached by advertisers during specifically allocated time-slots between children’s programmes or family programming on television, online platform services now provide advertisers and companies with more opportunities, and indeed more insidious chances, to reach children directly.

Despite the promising opinions related to children from the Article 29 Working Party, as well as those rights observed in the Recitals to the GDPR, in reality, only their proper and effective implementation will empower and protect children.

The Irish Heart Foundation supports academic literature in the area of processing of children’s data which has called for more realistic possibilities to affect digital data collection practises that means shifting the responsibility from parents to data controllers i.e. prohibiting undesirable data collection practises through restrictions on the activities of data controllers.[[21]](#footnote-21)



1. UNICEF. (2018). Children and Digital Marketing: Rights, risks and responsibilities. Discussion Paper. Geneva, Switzerland: UNICEF Private Sector Engagement. [Online]. Available from: <https://www.unicef.org/csr/css/Children_and_Digital_Marketing_-_Rights_Risks_and_Responsibilities(2).pdf> p3 [↑](#footnote-ref-1)
2. Lambrecht, I., Verdoodt, V. and Bellon, J. (2018). *Platforms and commercial communications aimed at children: a playground under legislative reform?*, International Review of Law, Computers & Technology, 32:1, 58-79 [Online]. Available from: <https://doi.org/10.1080/13600869.2018.1443378> [↑](#footnote-ref-2)
3. Macenaite, M. (2017). From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. *New Media & Society*, *19*(5), 765–779. [Online] Available from: <https://doi.org/10.1177/1461444816686327> p765 [↑](#footnote-ref-3)
4. Irvine Natas Solicitors. (2018). *Grounds of Complaint to the Data Protection Commissioner.* [Online]. Available from: <https://brave.com/DPC-Complaint-Grounds-12-Sept-2018-RAN2018091217315865.pdf> p2 [↑](#footnote-ref-4)
5. Lambrecht, I., Verdoodt, V. and Bellon, J. (2018). *Platforms and commercial communications aimed at children: a playground under legislative reform?*, International Review of Law, Computers & Technology, 32:1, 58-79 [Online]. Available from: <https://doi.org/10.1080/13600869.2018.1443378> [↑](#footnote-ref-5)
6. Macenaite, M. (2017). From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. *New Media & Society*, *19*(5), 765–779. [Online] Available from: <https://doi.org/10.1177/1461444816686327> [↑](#footnote-ref-6)
7. Logan, K. (2014). Why Isn’t Everyone Doing It? A Comparison of Antecedents to Following Brands on Twitter and Facebook. *Journal of Interactive Advertising*, *14*(2), 60-72. [Online]. Available from: <https://doi.org/10.1080/15252019.2014.935536> [↑](#footnote-ref-7)
8. World Health Organisation. (2019). MONITORING AND RESTRICTING DIGITAL MARKETING OF UNHEALTHY PRODUCTS TO CHILDREN AND ADOLESCENTS. Report based on the expert meeting on monitoring of digital marketing of unhealthy products to children and adolescents. [Online]. Available from: <http://www.euro.who.int/__data/assets/pdf_file/0008/396764/Online-version_Digital-Mktg_March2019.pdf?ua=1> [↑](#footnote-ref-8)
9. Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, *34*(1), 134–153. [Online]. Available from: <https://doi.org/10.1016/j.clsr.2017.05.015> [↑](#footnote-ref-9)
10. House of Commons Digital, Culture, Media and Sport Committee. (2018). *Disinformation and ‘fake news’: Final Report* Eighth Report of Session 2017–19*.* HC 1791. 18 February 2019. [Online]. Available from: <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf> p5 [↑](#footnote-ref-10)
11. UNICEF. (2018). Children and Digital Marketing: Rights, risks and responsibilities. Discussion Paper. Geneva, Switzerland: UNICEF Private Sector Engagement. [Online]. Available from: <https://www.unicef.org/csr/css/Children_and_Digital_Marketing_-_Rights_Risks_and_Responsibilities(2).pdf> [↑](#footnote-ref-11)
12. Ryan, J. (2018). *Regulatory complaint concerning massive, web-wide data breach by Google and other “ad tech” companies under Europe’s GDPR.* 13th September 2018 Article [Online]. Available from: https://www.linkedin.com/pulse/regulatory-complaint-concerning-massive-web-wide-data-johnny-ryan/ [↑](#footnote-ref-12)
13. Ryan, J. (2018). *Behavioural advertising and personal data.* [Online]. Available from: <https://brave.com/Behavioural-advertising-and-personal-data.pdf> p4 [↑](#footnote-ref-13)
14. Macenaite, M., & Kosta, E. (2017). Consent for processing children’s personal data in the EU: following in US footsteps? *Information & Communications Technology Law*, *26*(2), 146–197. [Online]. Available from: <https://doi.org/10.1080/13600834.2017.1321096> p146 [↑](#footnote-ref-14)
15. Lambrecht, I., Verdoodt, V. and Bellon, J. (2018). *Platforms and commercial communications aimed at children: a playground under legislative reform?*, International Review of Law, Computers & Technology, 32:1, 58-79 [Online]. Available from: <https://doi.org/10.1080/13600869.2018.1443378> [↑](#footnote-ref-15)
16. UNICEF. (2018). Children and Digital Marketing: Rights, risks and responsibilities. Discussion Paper. Geneva, Switzerland: UNICEF Private Sector Engagement. [Online]. Available from: <https://www.unicef.org/csr/css/Children_and_Digital_Marketing_-_Rights_Risks_and_Responsibilities(2).pdf> p8 [↑](#footnote-ref-16)
17. Mark Bunting. (2018). *Keeping Consumers Safe Online Legislating for platform accountability for online content.* [Online]. Available from: <http://static1.1.sqspcdn.com/static/f/1321365/27941308/1530714958163/Sky+Platform+Accountability+FINAL+020718+2200.pdf?token=lIv5b6G14vIcGq8x%2BWRfKHhNTN4%3D> p13 [↑](#footnote-ref-17)
18. Available at: <http://www.irishstatutebook.ie/eli/2018/act/7/section/30/enacted/en/html#sec30> [↑](#footnote-ref-18)
19. Available at: https://www.oireachtas.ie/en/bills/bill/2018/132/ [↑](#footnote-ref-19)
20. Macenaite, M., & Kosta, E. (2017). Consent for processing children’s personal data in the EU: following in US footsteps? *Information & Communications Technology Law*, *26*(2), 146–197. [Online]. Available from: <https://doi.org/10.1080/13600834.2017.1321096> p188 [↑](#footnote-ref-20)
21. Ibid [↑](#footnote-ref-21)