



**Irish Heart
Foundation**

Irish Heart Foundation

Submission to the Data
Protection Consultation
Processing of Children's Personal Data
and the Rights of Children as Data
Subjects under the GDPR

April 2019



Introduction

The Irish Heart Foundation welcomes the opportunity to make a submission to the public consultation on issues relating to the processing of children's personal data and the rights of children as data subjects under the General Data Protection Regulation (GDPR). 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 Commission 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

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

The Irish Heart Foundation believes that the outcomes from this consultation must protect children from the effects of direct marketing and profiling. Neither parents nor law-makers could have anticipated how effectively children would be targeted as consumers by technologies that are evolving faster than our capacity to respond to them, and wherein oversight is minimal and barriers to oversight are systemic.

Background

Internet access

The growth of technology and the internet has transformed modern communications and the pace of technological development is impacting almost all areas of modern life. Internet access and frequency of use have continued to increase, with 89% of Irish households having access to the internet at home in 2018.³ Indeed, the activities carried out most by

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](https://www.unicef.org/csr/css/Children_and_Digital_Marketing_-_Rights_Risks_and_Responsibilities(2).pdf) p3

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>

³ CSO. (2018). Information Society Statistics - Households 2018. [Online]. Available from:

<https://www.cso.ie/en/releasesandpublications/er/isshh/information societystatistics-households2018/>

individuals on the internet were *finding information on goods and services* (88%), *E-mail* (84%) and *Social networking and Reading or downloading online news* (both at 73%).

Growth in Social Media

Digital transformation has also brought on an explosion in the use of social media. Social networking sites and apps are not only gaining large numbers of members and sign-ups, but there are steady numbers of people accessing these everyday. In Ireland, for example, 65% have Facebook accounts and of these 69% use it daily; 32% have Instagram accounts and 51% use it daily; and 29% have Twitter and 37% use it daily⁴. Social networking is the third most common internet activity in Ireland at 73%, and for individuals aged 16 to 29 this was the most common activity at 92%⁵.

Considering the utility of social networks in sharing and disseminating messages and creating relationships between people and organisations, and coupling this with the growth in usage and time spent on these networks, it is not hard to see why it is transforming the landscape for all organisations. Social media provides a perfect environment for businesses and for marketing, to recruit and maintain regular contact with customers, to spread key messages, to seek opportunities and to advocate for their products. However, it also comes with inherent risks and challenges that must be addressed.

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."⁶

This concern has been recently echoed in a complaint made to the 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

⁴ IPSOS MRBI (2017). Social Networking - Nov 17. [Online]. Available from: <https://www.ipsos.com/en-ie/social-networking-nov-17>

⁵ CSO. (2018). Information Society Statistics - Households 2018. [Online]. Available from: <https://www.cso.ie/en/releasesandpublications/er/isshh/information societystatistics-households2018/>

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> p765

the complaint to the Data Protection Commissioner, three causes for concern were identified⁷ 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:

- a) gathers a wide range of information on individuals going well beyond the information required to provide the relevant adverts; and
- b) 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.

The 2016 report *Tackling food marketing to children in a digital world: trans-disciplinary perspectives*⁸ from the WHO defines digital marketing as:

Promotional activity, delivered through a digital medium, that seeks to maximize impact through creative and/or analytical methods, including:

- creative methods to activate implicit emotional persuasion, such as building engagement in social networks (e-Word-of-Mouth); using immersive narratives or social-, entertainment- and humour-based approaches; using “influencers” popular with children, such as YouTube “vloggers” (video bloggers); using augmented reality, online games and virtual environments; or
- analysis of emotions, responses, preferences, behaviour and location to target specific groups, individuals and particular moments of vulnerability or to maximize the impact of creative methods.

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.⁹ Personalisation, profiling and behavioural targeting have quickly become the norm across digital and online platforms, creating opportunities for commercial use of children’s data.

⁷ 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

⁸ World Health Organisation. (2016). *Tackling food marketing to children in a digital world: trans-disciplinary perspectives*. Children’s rights, evidence of impact, methodological challenges, regulatory options and policy implications for the WHO European Region. [Online]. Available from: http://www.euro.who.int/__data/assets/pdf_file/0017/322226/Tackling-food-marketing-children-digital-world-trans-disciplinary-perspectives-en.pdf

⁹ 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>

As a general rule, it should be accepted that for any person to make a well-balanced commercial decision, they must be able to distinguish and recognise the commercial intent of a communication. This is not clear cut for many people, nevermind children. Recognising that a myriad of techniques and sophisticated algorithms are employed to engage and target advertisements, it is very difficult to expect an awareness of commercial communications to come naturally.

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.¹⁰

Social Media – A breeding ground for opportunism

While we have always experienced advertising and targeted marketing through traditional and out of home media, this activity has taken on new forms and has been hugely magnified by information technology and the ubiquity of social media. With the surge in social media and internet usage, its attractiveness to the advertising industry has also grown. Indeed, the dominant business model in the digital environment remains advertising-based (e.g. social media, search engines, video-sharing platforms).¹¹

Research suggests that social media users are more likely to consume information than to communicate information, with brands and advertisers using these social media platforms and networks to involve their brands in the social networks of individuals.¹² Unlike traditional media which is subject to regulation, social media has facilitated the advent of immediate advertiser-consumer interaction as advertisers create brand-related content that encourages consumers to engage and interact in the form of through comments, likes, shares, photos and videos.

Similarly, the WHO refer to the advent of the "attention economy" in the digital age, where "any product that is "free" – a website or social media product – is paid for with our attention and with our data"¹³. This has important implications for children as we see how the metrics employed by social media companies and websites allow for vast amounts of

¹⁰ 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>

¹¹ 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>

¹² 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>

¹³ 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 p4

data about users to be gathered, thus facilitating the targeting of users by sophisticated algorithms to retain attention and maximise ad views.

As a result, platforms are now seen as gatekeepers and, as such, there is exponential potential for the abuse of children's data. This is because platforms, contain large amounts of user-generated content, are heavily data-driven and are highly dependent on advertising revenues.¹⁴ Individual's choices and data management capacities are intrinsically shaped by the design and functionalities of these platforms, which are far from neutral and have been extensively shown to have been created to advance business interests, rather than to allow the user to exercise their autonomy and control over their data.¹⁵ UNICEF has noted that there exists a lack of transparency in the current digital marketing landscape, coupled with a greater intelligence about how individuals view, react to and engage with digital advertising, which has the effect of incentivising the expansion of data collection and discouraging the publication of such information.¹⁶ 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.”¹⁷

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.¹⁸ 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.

¹⁴ Lambrecht, I., Verdoort, 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>

¹⁵ 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>

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](https://www.unicef.org/csr/css/Children_and_Digital_Marketing_-_Rights_Risks_and_Responsibilities(2).pdf)

¹⁷ 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/cmcomeds/1791/1791.pdf> p5

¹⁸ 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>

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.¹⁹ 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.²⁰ 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.²¹

Of special importance, and of particular relevance to this consultation, 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.²² 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.²³

¹⁹ 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

²⁰ 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>

²¹ 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](https://www.unicef.org/csr/css/Children_and_Digital_Marketing_-_Rights_Risks_and_Responsibilities(2).pdf)

²² 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/>

²³ Ryan, J. (2018). *Behavioural advertising and personal data*. [Online]. Available from: <https://brave.com/Behavioural-advertising-and-personal-data.pdf> p4

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”²⁴

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.²⁵ 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.”²⁶

In its consideration of disinformation and fake news, the House of Commons Digital, Culture, Media and Sport Committee looked at both the use of personal and inferred data, noting that despite the assertion made by Facebook that users own all the content they upload, the advertising profile that Facebook builds up about users cannot be accessed, controlled or deleted by those users. Similarly, it notes that ‘inferred’ data is not protected under GDPR, which includes inferred characteristics about a user not based on specific information they have shared, but through analysis of their data profile.²⁷

Taking these techniques into account, it is likely that children and adolescents (and indeed most adults) are unaware that inferences can be made from their online disclosures and activities (e.g ‘likes’), which can then be used to generate profiles and produce targeted adverts.

Irish Heart Foundation Research & Concerns

In 2016, the IHF published a ground-breaking study - *Who’s Feeding the Kids Online?* - on digital food marketing to children in Ireland. The study revealed the sophisticated digital marketing techniques directed at children by the top food and beverage brands and how little parents know about the efforts being made to influence their children. Food companies magnify the known effects of broadcast advertising, by using the ‘3 Es’ –

²⁴ 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

²⁵ 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>

²⁶ 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](https://www.unicef.org/csr/css/Children_and_Digital_Marketing_-_Rights_Risks_and_Responsibilities(2).pdf) p8

²⁷ 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/cmcmds/1791/1791.pdf>

powerful engagement-, emotional- and entertainment-based tactics – in digital media. The report found many of the food and beverage brands are not now using websites to promote their products to children – with just one in ten top retail brands in Ireland having sites with child-directed content – although one in five still had content appealing to older children and teens, virtually all for items high in fat, salt or sugar. However, the picture changed dramatically on Facebook where all the food and beverage brand pages with the greatest reach among 13-14-year-old users in Ireland are for brands that feature unhealthy products.

The tactics exposed in *Who's Feeding the Kids Online?* - Europe's first ever research on the tactics used by junk food, which was endorsed by the World Health Organisation - exposed microtargeting and profiling methods similar to those that were subsequently shown to have been used by Cambridge Analytica. However, digital marketing is not subject to any statutory regulation, despite strong evidence that online marketing, particularly on social media, is far more personalised and effective than television advertisements and therefore potentially more dangerous. Instead it comes under a weak voluntary code governed by the Advertising Standards Authority of Ireland which only investigates complaints made about potential breaches after the advertisement in question has been seen by the public.

Clearly, digital platforms extract huge amounts of individual information from children: who they are, where they live, where they go, who their friends are, their hobbies, heroes, favourite foods etc. Furthermore, and more worryingly, these platforms also deliberately manipulate children's emotions or behaviour in order to increase the impact of advertising. The integrated, interactive and personalised nature of these platforms and communications makes it difficult for children to recognise the commercial, persuasive intent. As such, it should be questioned whether these methods are in line with children's fundamental rights.

Support for prohibiting the profiling of children for marketing purposes

The need to safeguard against the commercial use of children's data is dominant across children's rights organisations and advocates.

In the submission on the General Scheme of the Data Protection Bill, the Office of the Ombudsman for Children proposed the inclusion of specific protections in relation to "the use of personal data of children for the purposes of marketing and creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to the child".²⁸

The Children's Rights Alliance has argued that reliance on digital consent alone is an abdication of responsibility and takes the emphasis off data controllers. It notes that "if we are truly concerned about children's data, we should be imposing more restrictions on the use of their data by controllers."²⁹ Digital consent is not a panacea for protecting children's

²⁸ Ombudsman for Children. (2017). *Preliminary Observations of the Ombudsman for Children's Office on the General Scheme of the Data Protection Bill 2017*. Submission to the Oireachtas Joint Committee on Justice and Equality. 29 June 2017. [Online]. Available from:

https://www.oco.ie/app/uploads/2017/09/OCO_Submission_GSDDataProtectionBill2017_FINAL.pdf

²⁹ Children's Rights Alliance. (2018). *Real Solutions to Protect Children's Data*. [Online]. Available from:

https://www.childrensrights.ie/sites/default/files/submissions_reports/files/Real%20Solutions%20to%20Protect%20Children%27s%20Data_Briefing_February%202018.pdf p2

data online. Indeed, this overreliance on consent “can provide illusionary control and the agreement to the processing of personal data in situations of imbalance of powers is not delivered freely. A rich body of literature points to the characteristics of networked environments that predetermine power imbalances and limit individuals in asserting control over their personal data.”³⁰ The reliance on consent also ignores the lack of choice available to children and adolescents engrossed in the network effects of particular platforms, services or technologies.

In its discussion paper *Children and Digital Marketing: Rights, risks and responsibilities*³¹, UNICEF has explicitly highlighted the threats posed to children’s rights as a result of the economic exploitative practices posed by covert data collection for the purpose of profiling:

“When the commercial intent of advertising is obscured from children, either through the use of stealth or social means, or because children are not adequately equipped with the cognitive abilities or media literacy to identify advertising, the ramifications for children’s rights may be serious. Some innovative forms of advertising aim to subliminally influence children, including when they are engaged in games or learning, at a time when their critical faculties and decision-making processes are compromised.”

Council of Europe Committee of Ministers

Reflecting the fact that the Council of Europe included the rights of the child in the digital environment as one of five key priorities in its Strategy for the Rights of the Child 2016-2021, the rights of children in the digital environment have been given explicit consideration by the Council of Europe’s Committee of Ministers, and a set of recommendations for action have been provided to member states. In recommendations published in July 2018, European Governments have been recommended to review their legislation, policies and practices to ensure that these adequately address the full range of the rights of the child.³² The outcomes of the Data Protection Commission consultation should reflect these recommendations.

Of special importance in the area of direct marketing to, and profiling of, children, as well as complimenting the principle contained in Section 30 of the Data Protection Act 2018 discussed below, are those recommendations in section 3.4 on privacy and data protection where it is stated that:

“Profiling of children, which is any form of automated processing of personal data which consists of applying a “profile” to a child, particularly in order to take decisions concerning the child or to analyse or predict his or her personal preferences, behaviour and attitudes, should be prohibited by law. In exceptional

³⁰ 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> p185

³¹ 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](https://www.unicef.org/csr/css/Children_and_Digital_Marketing_-_Rights_Risks_and_Responsibilities(2).pdf) p18

³² Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment (Adopted by the Committee of Ministers on 4 July 2018 at the 1321st meeting of the Ministers' Deputies). Available from: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016808b79f7

circumstances, States may lift this restriction when it is in the best interests of the child or if there is an overriding public interest, on the condition that appropriate safeguards are provided for by law.”

It is clear from this that states must respect, protect and fulfil the right of the child to privacy and data protection, with explicit need to ensure that the profiling of children to analyse or predict their personal preferences should be prohibited by law.³³

Protecting Children – Amend & Commence Section 30 of the Data Protection Act

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.

³³ Council of Europe gives recommendations to member States on children’s rights in the digital environment. Available from: https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=09000016808c1a4f

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.³⁴ 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."³⁵

GDPR, Processing of Children's Personal Data and the Rights of Children as Data Subjects

While much is discussed across the Article 29 Working party opinions and recitals of the GDPR about the processing of children's personal data and the rights of children as data subjects under the GDPR, GDPR itself offers little clarity as to the actual implementation of a number of the provisions contained therein, leading to legal uncertainty for data controllers, parents and children.³⁶

The Irish Heart Foundation believes that the objective of the Data Protection Commission consultation on the process of children's personal data and the rights of children as data subjects under the GDPR should involve the curtailment of the deliberated and targeted profiling of children for advertising in view of their vulnerability and the sophistication of the messages crafted in the absence of any restrictions.

Why do children merit specific protection?

The need for particular protection for children is reflected in Recital 38, which says:

"Children require 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. Such specific protection

³⁴ Available at: <https://www.oireachtas.ie/en/bills/bill/2018/132/>

³⁵ 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

³⁶ Lievens, E., & Verdoodt, V. (2018). Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 34(2), 269–278. [Online] Available from: <https://doi.org/10.1016/j.clsr.2017.09.007>

should, in particular apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.”

Decisions based upon solely automated processing of personal data are often used with to influence a person’s future choices and behaviours. For example, in the context of behavioural advertising, a profile of past browsing habits may be used to automatically display certain products to particular individuals, with the aim of influencing them to buy those products. This is of particular concern where children are concerned because they may be more easily influenced, and less able to understand the motivation behind such processing.

What about the best interests of the child?

The concept of the best interests of the child comes from Article 3 of the United Nations Convention on the Rights of the Child. Although it is not specifically referenced in the GDPR it is something that must be taken into account when considering the processing of children’s personal data and the rights of children as data subjects. Indeed, in the observations on the General Scheme of the Data Protection Bill, the Ombudsman for Children noted that “while the UN Convention on the Rights of the Child pre-dates the current digital era, its principles and provisions are highly relevant to and resonate in the online environment”.³⁷

As mentioned previously, the rights of children in the digital environment, include participation rights must be balanced with protection and development. In the absence of such a balance, the well-being of children is seriously compromised. The WHO³⁸ have identified the risks to wellbeing of children in the digital world:

- Content risks: inaccurate, harmful or illegal content.
- Contact risks: inappropriate and unwanted contact between users.
- Conduct risks: inappropriate or otherwise harmful behaviour online.
- Commercial risks: short- and long-term harms resulting from data extraction, resale and targeting by commercial actors; users being encouraged to give out information that can be used to defraud or cause harm associated with exposure to inappropriate marketing.

This is especially important, given the information highlighted in the report *Behavioural advertising and personal data*, which notes that once personal data is released in a bid request to a large number of companies, they can freely trade these personal data with

³⁷ Ombudsman for Children. (2017). Preliminary Observations of the Ombudsman for Children’s Office on the General Scheme of the Data Protection Bill 2017. Submission to the Oireachtas Joint Committee on Justice and Equality 29 June 2017. [Online]. Available from:

https://www.oco.ie/app/uploads/2017/09/OCO_Submission_GSDataProtectionBill2017_FINAL.pdf p2

³⁸ 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 p2

business partners, however they wish. This is particularly grievous for children’s personal data since the data concerned is very likely to be “special categories” of personal data.³⁹

What does it say?

The GDPR aims at regulating the processing of personal data – creating parameters around its acquisition, use, storage and sharing. Profiling is an internal activity of many social media companies, where it uses personal data, incidentally collected, and creates a virtual identity of the user and uses that information for commercial gain by, for example, creating targeted ads. This technology is evolving all the time as is the detail of profiling – face recognition etc.

Article 22 of the GDPR governs automated decision-making and profiling and states that “the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her”. It differentiates processing from profiling and creates a legal regime around profiling and automated decision-making. It does not exclude children, however the interpretive tools of the GDPR, specifically Recital 71, views that where there is marketing aimed at children this should be prohibited as children are a vulnerable category (as recognised by GDPR, Recital 22).

Where children are concerned Recital 71 states in particular that children should not be subject to profiling that results in legal or similar significant effects (for example, influencing the child’s choices and behaviours in a potentially significant and harmful way). Although this wording is not reflected in the Articles of the GDPR itself, it does give a clear indication that such processing of children’s personal data should not be the norm.

The Working Party 29 Opinion 02/2013 on apps on smart devices (WP202), adopted on 27 February 2013, under the specific section 3.10 on Children, specifies at page 26 that “data controllers should not process children’s data for behavioural advertising purposes, neither directly nor indirectly, since this will be outside of the scope of the child’s understanding and therefore exceed the boundaries of lawful processing”.⁴⁰ The Working Party 29 bases this express protection for children on their view reflected in Recital 38.

Profiling endorses the online commercialisation of children, with no oversight. It is one of the most powerful tools used by tech corporations to collect and sell personal data, which is then used to create powerful personal ads that are uniquely targeted to children in the image of their personal digital footprint.

Is marketing a ‘legitimate interest’?

Personal data can only be processed to the extent that there is a ‘legitimate interest’ justifying the processing (Art. 6 GDPR). Therefore, it is noted that when processing is necessary to provide a service, providers can rely on the ground ‘necessity for the

³⁹ Ryan, J. (2018). *Behavioural advertising and personal data*. [Online]. Available from: <https://brave.com/Behavioural-advertising-and-personal-data.pdf> p6

⁴⁰ http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826 (footnote at page 29)

performance of a contract'.⁴¹ While 'legitimate interest' is one of the six legal bases for processing personal data, the text of Article 6(f) GDPR goes on to state 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." Similarly, it can be argued that processing personal data for online behavioural advertising purposes can be seen to go beyond the 'mere provision of the service' (e.g. provision of the platform).

From a children's rights perspective, a number of issues are highlighted with respect to the rules on the profiling of children namely that, notwithstanding the contents of recital 38, it is still feasible for companies to build profiles of children as long as they comply with GDPR principles and if no solely automated decisions are made that have legal or other significant effects for children. This then could be perceived as violating children's right to privacy, as well as their right to development.⁴²

While Recital 47 GDPR does explicitly state that "the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest" and therefore allows a legitimisation ground other than the consent of the data subject, the onus is still on the data controller to balance its legitimate interest with the interests or fundamental rights and freedoms of the data subject. Part of this consideration therefore entails scrutiny of the reasonable expectations of data subjects based on their relationship with the controller. This is especially important for children.

In a previous opinion on Online Behavioural Advertising, the Article 29 Working Party noted that "taking into account the vulnerability of children, the Article 29 Working Party is of the view that ad network providers should not offer interest categories intended to serve behavioural advertising or influence children"⁴³. This opinion was reiterated in a later opinion on apps on smart devices, where the Article 29 Working Group said that "children have little or no understanding of and knowledge about the extent and sensitivity of the data to which apps may gain access, or the extent of data sharing with third parties for advertising purposes."⁴⁴ Evidently the Working Party perceive that the processing of children's personal data requires extra care and, as such, this should be a fundamental facet of the interpretation and implementation of the GDPR.

Furthermore, in a complaint to the Data Protection Commissioner⁴⁵, the issue of behavioural advertising and the use of digital identifiers highlighted a broader concern

⁴¹ 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>

⁴² Lievens, E., & Verdoodt, V. (2018). Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 34(2), 269–278. [Online] Available from: <https://doi.org/10.1016/j.clsr.2017.09.007>

⁴³ ARTICLE 29 DATA PROTECTION WORKING PARTY. (2010). *Opinion 2/2010 on online behavioural advertising*. 00909/10/EN WP 171. Adopted on 22 June 2010. [Online] Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf p17

⁴⁴ ARTICLE 29 DATA PROTECTION WORKING PARTY. (2013). *Opinion 02/2013 on apps on smart devices*.00461/13/EN WP 202. Adopted on 27 February 2013. [Online]. Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf p26

⁴⁵ 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> p13

relating to the overarching principle of fairness in the GDPR, of relevance for this consultation:

“controllers have easy access to identifiers to single individuals out, whereas those same individuals have no real ability to use or control those identifiers. This creates concerns, in particular, under Article 25 GDPR, data protection by design and by default, which imposes a positive obligation on data controllers to build data protection provisions, such as access or objection, into their processing activities and systems.”

While some may argue that not every choice a child makes in response to data processing has a ‘similarly significant’ effect on them, the fact remains that children are more easily influenced, and less able to understand the motivation behind such processing. They may not be able to distinguish advertisements. In the context of the *Who’s Feeding the Kids Online?* research from the Irish Heart Foundation, it is clear that solely automated processing of a child’s personal data that influences a child to make poor food choices, to the detriment of their health, is equivalent in a way that is ‘similarly significant’ to a legal effect. Indeed, the Irish Heart Foundation notes the comments of the Article 29 Working Party in its opinion on Apps on Smart Devices⁴⁶ that “specifically, data controllers should not process children's data for behavioural advertising purposes, neither directly nor indirectly, as this will be outside the scope of a child's understanding and therefore exceed the boundaries of lawful processing.”

Closely related to this then are the findings of the House of Commons Digital, Culture, Media and Sport Committee final report on disinformation and fake news, which highlighted the malicious nature of micro-targeted political adverts. Of relevance for this consultation was the finding that “there is considerable obfuscation concerning the auditing of its adverts, which provide Facebook with its ever-increasing revenue. To make informed judgments about the adverts presented to them on Facebook, users need to see the source and purpose behind the content.”⁴⁷ Equally relevant for advertising and marketing to children, the ability of social media platforms to target content to children, and in private, without any scrutiny or detail of the techniques is deeply problematic and concerning for children’s privacy rights and, importantly, their health into the future.

It is clear that the drafters of the regulations anticipated the need for explicit protections for children. Therefore, action should be taken (legislatively and statutorily) to ensure that the personal data of children is not collected, retained or used for marketing or commercial purposes by data controllers. Where it is argued that there is a legitimate interest to process the data, the onus must fall to the data controllers to ensure that the interests and rights and freedoms of children is not undermined.

Conclusion

⁴⁶ ARTICLE 29 DATA PROTECTION WORKING PARTY. (2013). Opinion 02/2013 on apps on smart devices.00461/13/EN WP 202. Adopted on 27 February 2013. [Online]. Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf p26

⁴⁷ 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/cmcmums/1791/1791.pdf> p85

Concerns about 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.⁴⁸

For more Information Contact:



⁴⁸ 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>



Irish Heart Foundation
17-19 Rathmines Road Lower, Dublin 6.
Phone: +353 1 668 5001
Fax: +353 1 668 5896
Email: info@irishheart.ie
www.irishheart.ie

Follow us on  

Registered Charity CHY 5507