Bloomsbury Professional

ISSN 1746-7616

www.bloomsburyprofessional.com

Communications Law

Volume 23 Number 1 2018 Pages 1-54

Volume 23 Number 1 2018

Communications Law

The Journal of Computer, Media and Telecommunications Law

Bloomsbury Professional

Manuscripts should be sent to the Editor in Chief, Dr Paul Wragg (P.M.Wragg@leeds.ac.uk) with a copy to the Managing Editor, Julian Harris (brandlingharris@dsl.pipex.com).

Other correspondence should be sent to:
Richard Cox
Production Editor
Bloomsbury Publishers
Kemp House
Chawley Park
Cumnor Hill
Oxford
OX2 9PH
Tel: 01865 596793
richard.cox@bloomsbury.com

N.B. Prospective contributors are advised to request a style sheet before commencing their article.

Subscription enquiries should be sent to customerservices@bloomsburyprofessional.com

Annual subscription (including postage): £450 (UK), £465 (overseas).

Published four times a year by:
Bloomsbury Professional Ltd
Maxwelton House
41–43 Boltro Road
Haywards Heath
West Sussex RH16 1BJ
Tel: 01444 416119
Fax: 01444 440426

Managing Editor: Julian Harris

Designed and typeset by Marcus Duck Design

Printed and bound in Great Britain by Hobbs the Printers Ltd, Totton, Hampshire.

Peer Review Policy

Where appropriate, academic submissions are sent to independent referees for comment. The peer review process is based on initial editor screening and refereeing by two anonymous referees.

Guidelines for Contributors

A. Articles submitted should be original contributions and should not be under consideration for publication in any other journal. Copyright of material published in the Journal rests with the Publishers, Bloomsbury Professional Limited. Contributors to the Journal will be asked ually be given (free of charge) to authors to publish their articles elsewhere, if they so request.

B. Contributors are entitled to two copies of the issue in which their article appears.

C. Articles must comply with the following specifications as the Editor will not undertake the re-typing of submissions which do not comply with Journal style.

1. Manuscripts should be supplied in a format compatible with standard word-processing packages, preferably MS Word. Manuscripts should be emailed to linda.murray@bloomsbury.com or sent to the address given on the inside front cover of this Journal. Please note that Bloomsbury Professional's Communications Law is a refereed journal. Contributors can obtain advice on any aspect of their contribution from the Editor at the above email address.

2. Authors should keep at least one copy of their article.

3. Book titles should be in italics or underlined; articles/essays contained within should appear in single quotes. Periodicals should be given their standard abbreviations and should not be italicised eg LQR not Law Quarterly Review.

4. Law reports should appear using the standard abbreviations of their titles and should not be in italics or underlined. Full stops should not be used in case names, or law report citations. Abbreviations should be preceded by year (in square brackets where the year is an essential element, otherwise use round brackets) and volume number; page number(s) should follow abbreviation: (1991) 88 LGR 737–750.

5. References to journals should appear as follows: (1987) 3 CL 193–97. Standard abbreviations of titles are: Communications Law CL
Professional Negligence PN
Trust Law International TLI
Immigration, Asylum IANL
and Nationality Law

   Subsequent references to sources already used should follow the ibid and supra system.

6. Italicise or underline words to appear in italics.

7. Spelling should comply with British, not American forms, eg -ise, not -ize, as in nationalise. Numbers one to twelve and per cent to be spelt out.

8. Quotation marks: use single quotes throughout, except for a quote within a quote – for this use double quotes.

D. Book reviews: full publication information should be given at the top of the review: title, author, edition, publisher, date, ISBN/ISSN, number of pages, price, pb (paperback)/hb (hardback). Eg:

European Data Protection Law:
Corporate Regulation and Compliance
Christopher Kuner
Oxford University Press
Second edition
ISBN 0 19 928385 0
xxvii + 460 pp
£125.00 (hb)

Communications Law Vol. 23, No. 1, 2018

Contents

Editorial

Children and digital rights

The internet provides children with more freedom to communicate, learn, create, share, and engage with society than ever before. Research by Ofcom in 2016 found that 72 per cent of young teenagers in the UK have social media accounts. Twenty per cent of the same group have made their own digital music and 30 per cent have used the internet for civic engagement by signing online petitions or by sharing and talking about the news.

Interacting within this connected digital world, however, also presents a number of challenges to ensuring the adequate protection of a child's rights to privacy, freedom of expression, and safety, both online and offline. These risks range from children being unable to identify advertisements on search engines to being subjects of bullying or grooming or other types of abuse in online chat groups. Children may also be targeted via social media platforms with methods (such as fake online identities or manipulated photos and images) specially designed to harm them or exploit their particular vulnerabilities and naivety.

These issues were the subject of 'Children and digital rights: regulating freedoms and safeguards', the 2017 Annual Conference of the Information Law & Policy Centre (ILPC) based at the Institute of Advanced Legal Studies, University of London. The ILPC produces, promotes, and facilitates research about the law and policy of information and data, and the ways in which law both restricts and enables the sharing and dissemination of different types of information. The conference – held on 17 November 2017 and one of a series of events celebrating the 70th anniversary of the founding of the Institute of Advanced Legal Studies – was sponsored by *Communications Law*, and some of the papers presented, discussed and debated during the day feature in this special issue of the journal.

Leading policymakers and regulators from government (including senior representatives from the Department of Digital (DCMS), the Information Commissioner's Office and the Deputy Data Protection Commissioner of Ireland), industry (Simon Milner, Facebook's Policy Director for the UK, Africa, and Middle East),

practitioners, and academic experts examined the opportunities and challenges posed by current and future legal frameworks and the policies being used and developed to safeguard these freedoms and rights.

These legal systems included the UN Convention on the Rights of the Child and the related provisions of the UK Digital Charter, and the UK Data Protection Bill, which will implement the major reforms of the EU General Data Protection Regulation (2016/678) which soon enter into force on 25 May 2018. Concerns expressed at the conference by delegates included the effectiveness in practice and lack of evidence-based policy for the controversial age of consent for children and their use of online information services provided for under the GDPR and the impact of the new transparency and accountability principles that must be implemented by data controllers when their data processing involves the personal data of children.

In 'Sharenting: balancing conflicting rights of parents and children', Claire Bessant, Associate Professor at Northumbria University, asks the important question of whether (and how) children might obtain a remedy when their parents share private photographs of them without their consent. As she recognises, 'sharenting' – the act of parents sharing information about their children – has become ubiquitous in the digital age. So much so, that there is little public consciousness of the privacy implications that (especially) cavalier attitudes towards social media privacy settings generate. In her view, the misuse of private information tort may provide for a meaningful remedy, but only if the court is prepared to place the interests of the children above parental decision-making.

Baroness Kidron OBE, one of the country's leading children's online rights campaigners, develops a different theme in the ILPC's 2017 Annual Lecture, 'Are children more than 'clickbait' in the 21st century?' She asks how children interact with digital technology, and argues strongly that there is insufficient recognition of a child's digital needs. As she puts it, a new deal is required, on terms that

must include their right to change their digital footprint and identity; to be safe and supported in online settings; to understand who, how and what their data is being used for; to be informed and creative participant digital citizens; and above all, to have 'agency' – meaningful choice in an environment that is responsive to, and respectful of, their full complement of rights and needs as minors.

Her powerful conclusion is that government needs to take a greater interest in the developmental needs of children on the internet – and so should Silicon Valley by re-engineering its metadata capturing policy to reflect those needs. She explains the amendments to the GDPR that she (and others) initiated, which would put children's development at the forefront of data protection rules, thus enabling the Information Commissioner to play an active role in this important area.

Continuing the theme of GDPR and its implication for children, Lisa Atkinson, (Group Manager in the Policy and Engagement Department of the Information Commissioner's Office), offers insights into this process. She is leading the ICO's work on interpreting the child-related provisions of the GDPR. Her article delivers a positive message: that the GDPR 'is an opportunity to reflect and recalibrate. This can only be a good thing, and we await further developments and debate with interest'. She explains the new measures arising from the GDPR, in practical terms and with great clarity.

Professors Simone van der Hof and Eva Lievens, from Leiden University and Ghent University respectively, in their joint paper, 'Protection of children under the GDPR: how to achieve meaningful control over personal data by parents and children' provide a thoughtful exploration of the underlying doctrine and philosophical implications of the new regulations. Their starting point recognises the protection of children provisions in the GDPR, 'although indeed…laudable, …raises many questions as to what said protection entails and how it can be effectively achieved.' For them, for example, it is 'highly questionable' whether parental consent will be a meaningful mechanism to protect children given the realities of 'consent overload, information overload, complexity of data processing, and lack of actual choice'. Further, it may jeopardise child development through exclusion from online services. The paper challenges this 'illusion of autonomy and control' by exploring alternative 'tools' to protect and empower children. Their conclusions are of both academic and practical value.

We finish with a paper from Anna Morgan, solicitor and Deputy Commissioner (Head of Legal) for the Data Protection Commissioner for Ireland. Drawing upon her experience as lead rapporteur for the Article 29 Working Party Guidelines on Transparency under the GDPR, she discusses the compliance issues surrounding the transparency provisions in a child context. As she notes, this will be challenging for data controllers:

No matter how accessibly or appealingly privacy information is presented on a website or an app used by children, if child users do not appreciate the significance of what that information is telling them, then the risk is that they will swipe right past it without taking any notice of it.

As she recognises, the 'biggest transparency challenge' will be to motivate children to '*want* to understand how and why their personal data is used and processed'. This, she argues, is a cultural issue and not simply a technical one: the challenge must be 'embraced… by data protection authorities, policy makers, educators, and parents who all have vital roles to play when it comes to educating children and young people about their rights and risks online'.

Dr Nóra Ni Loideain
Director, Information Law & Policy Centre, Institute of Advanced Legal Studies, University of London

Dr Paul Wragg
Associate Professor of Law, University of Leeds

In Brief

Government to give commercial radio more freedom on content

Commercial radio stations will have greater freedom to increase their choice of music genres and respond to the needs of listeners under new rules announced by Digital Minister Matt Hancock.

Under the current regulations, analogue radio stations have to play a particular genre of music as part of their licence agreement with Ofcom. This stipulation is being removed, and there will also be no requirement for Ofcom to approve changes to programme formats. However, with recent research showing that radio is the most trusted medium for news, strong requirements will remain on commercial radio stations to provide national and local news as well as travel information and weather.

A consultation was launched in February 2017 on commercial radio deregulation, and the Department for Digital, Culture, Media & Sport (DCMS) published the government response on 18 December 2017. Some changes to the original proposals have been made in the light of comments received:

- the government still intends to seek powers to enable Ofcom to license overseas services, but a more gradual approach is to be adopted starting with Republic of Ireland services;
- there was no consensus on whether obligations to provide news or core information in the event of a future digital radio switchover should fall to the existing stations or local multiplex operators (or some combination of the two), and further discussions will take place with the radio industry;
- a clear view was expressed that there was no need for Ofcom to have the power to set different news (national or local) or other local requirements in the nations, and the government has decided that a better approach is for Ofcom to have regards to the needs of all UK audiences in setting the requirements on a UK basis;
- while the government still believes that the localness requirements for non-news and local information content can be removed, there is a need for greater clarity in legislation defining what is meant by locally-sourced news, and Ofcom should produce guidance in this area.

The government intends to seek powers to enabtle Ofcom to license overseas services on UK DAB. This means that digital radio listeners will now be able to listen to stations based in the Republic of Ireland, and the government will gradually extend this to stations licensed in the European Union.

The proposals will require major changes to the Broadcasting Act 1990, the Broadcasting Act 1996, and the Communications Act 2013. DCMS will progress the arrangements and begin detailed work to develop the new legislative structure prior to analogue licences coming up for renewal in 2022.

High speed broadband to become a legal right

The government has confirmed that universal high speed broadband will be delivered by a regulatory Universal Service Obligation (USO), giving everyone in the UK access to speeds of at least 10 Mbps by 2020.

After careful consideration the government has decided that regulation is the best way of making sure everyone in the UK can get a decent broadband connection as soon as possible. Ofcom has said that a speed of least 10 Mbps is needed to meet the requirements of an average family.

The design for a legal right to high speed broadband will be set out in secondary legislation in the early part of this year. Ofcom's implementation is expected to take two years from when secondary legislation is laid.

In summer 2017 BT made a proposal to deliver universal broadband through a voluntary agreement, but the government believes that only a regulatory USO offers sufficient certainty and the legal enforceability that is required to ensure high speed broadband access for the whole of the UK by 2020.

The government considers that its regulatory approach also brings a number of other advantages for the consumer:

- the minimum speed of connection can be increased over time as consumers' connectivity requirements evolve;
- it provides for greater enforcement to help ensure households and businesses do get connected;
- the scheme will maximise the provision of fixed line connections in the hardest to reach areas;
- the scheme places a legal requirement for high speed broadband to be provided to anyone requesting it, subject to a cost threshold (in the same way the universal service right to a landline telephone works).

Children to be given extra protection online

A new statutory power to ensure greater protection for children online has been proposed by the government.

The new power has been added as an amendment to the Data Protection Bill, and has cross party support. The government's proposals will require the Information Commissioner's Office (ICO) to produce a statutory code of practice on age-appropriate website design.

Standards required of websites and app makers on privacy for children under the age of 16 will be set by the new code. It will also ensure that websites and apps must be designed to make clear what personal data of children is being collected, how it is being used, and how both children and parents can stay in control of this data.

The amendment has the support of Baroness Kidron and Baroness Harding, who have campaigned for many years to protect the rights and safety of children on the internet. The government has worked closely with campaigners on the new amendment, to secure these rights around the online processing of a child's personal data in the Bill.

The new code would have the same enforceability as the government's codes on direct marketing and data sharing. It also has a clear link to enforcement provisions already set out in the Bill.

It is expected that non-compliance with the code would play a relevant factor in any ICO decision to bring forward enforcement action against websites that do not comply with the Data Protection Bill – including in determining the level of fines of up to £18 million or 4 per cent of global turnover.

Changes to Electronic Communications Code come into effect

Reforms to the Electronic Communications Code (EEC) reflecting changes made by the Digital Economy Act 2017 have come into force.

The reformed Code, which took effect on 28 December 2017, will reduce the costs of housing phone masts and other communications infrastructure on private land. This opens the way for faster and more reliable broadband and mobile services, particularly in rural areas.

The government says changes to the EEC will:

- bring down the rents telecoms operators pay to landowners to install equipment to be more in line with utilities providers, such as gas and water;
- make it easier for operators to upgrade and share their equipment with other operators to help increase coverage;
- make it easier for telecoms operators and landowners to resolve legal disputes; and
- help to drive investment and stimulate the continued growth, rollout and maintenance of communication technology infrastructure, an increasingly significant area of the UK's economy.

Obligations have been placed on Ofcom to publish:

- a Code of Practice to accompany the changes to the Electronic Communications Code;

- a number of template notices which must or may (depending on the circumstances in question) be used by Code operators and landowners/occupiers; and

- standard terms which may (but need not) be used by Code operators and landowners or occupiers when negotiating agreements to confer Code rights.

Revisions made to Editors' Code of Practice

The Editors' Code of Practice, under which the vast majority of Britain's newspaper, magazine and news website journalists work, has been revised after a public consultation.

The revised Code, which came into effect on 1 January 2018, is applied by the Independent Press Standards Organisation (IPSO). One of the changes offers increased protection to children accused of crime (cl 9), and in a move that goes further than the law requires, the Code now states that editors should generally avoid naming children after arrest for a criminal offence but before they appear in court.

An amendment has also been made to clause 2 (Privacy), to clarify how the public domain is taken into account when complaints are considered, and to clause 11 (Victims of sexual assault), to align it more closely with the law. In a further development, the Editors' Code of Practice Committee has recommended that IPSO should consider how member publishers report on commercial transparency.

The Canary found to have breached IMPRESS standards

An IMPRESS Regulatory Committee has found The Canary to be in breach of its Standards Code over an article criticising the BBC journalist Laura Kuenssberg for speaking at the Conservative Party conference.

The Canary is a political blog supportive of Labour leader Jeremy Corbyn which describes itself as 'an independent, progressive news website.' In the headline of the article first published at noon on 27 September 2017, The Canary stated: 'We need to talk about Laura Kuenssberg. She's listed as a speaker at the Tory Party conference'.

In fact, as the remainder of the article made clear, Laura Kuenssberg had only been invited to speak at a fringe event. In misrepresenting those facts and in failing to take all reasonable steps to ensure accuracy prior to publication, The Canary breached the IMPRESS Standards Code.

An updated version of the article released at 16:50 on 27 September 2017 also breached the Code because it did not correct this significant inaccuracy with due prominence. The Canary was ordered by IMPRESS to publish a home page correction in the same-sized font as the original article and to release the correction on the same social media channels as the original article.

IMPRESS was contacted by 52 complainants who raised concerns about the article in question, and one complainant chose to escalate their complaint to IMPRESS following The Canary's initial response. The Canary cooperated fully with IMPRESS's investigation, which was mounted in response to the complaint and on issues identified by IMPRESS on its own initiative.

BBFC proposed as age-verification regulator for online pornography

The British Board of Film Classification (BBFC) has been proposed by the government as the regulator for the age of verification of online pornography in the UK.

Age verification will mean anyone who makes pornography available online on a commercial basis must ensure under 18s in the UK cannot access it. The government sees the BBFC as having unparalleled expertise in classifying content, and it can demonstrate a proven track record of interpreting and implementing legislation as the statutory authority for age rating videos under the Video Recordings Act.

These factors, along with BBFC's work with industry on the film classification system and more recently classifying material for mobile network operators, makes them the government's preferred choice. The government's proposal must be approved by Parliament before the BBFC is officially designated as the age-verification regulator.

The regulator will notify non-compliant pornographic providers, and be able to direct internet service providers to prevent customers accessing these sites. It will also notify payment-services providers and other ancillary service providers of these sites, with the intention that they can withdraw their services. Guidance on how the regulator should fulfil its duties will be published by the government.

Sharenting: balancing the conflicting rights of parents and children

Claire Bessant

Introduction

Many parents share information about their children online. It is reported that in the United States 92 per cent of children have an online presence due to their parents' disclosures by the age of two years old.[1] Although in the United Kingdom far fewer parents admit to sharing their children's information online,[2] many parents will post hundreds of photographs of their children before they reach their fifth birthday.[3] So many parents now share information about their children online that a new term, 'sharenting,' has emerged to describe the phenomenon. 'Sharenting' here means the 'habitual use of social media to share news, images, etc of one's children'.[4]

Parents are often considered the 'guardians,'[5] or 'gatekeepers'[6] of their children's personal information. Their role in providing consent to use their children's information is recognised in European Union legislation[7] and the jurisprudence of the European Court of Human Rights (ECtHR).[8] The English judiciary also seemingly acknowledge that parents are the best people to decide whether a child's information is shared.[9] In the sharenting context, however, a conflict of interests exists between parents and their children. This conflict was clearly highlighted in 2016 when media reports suggested an 18-year-old Austrian girl was suing her parents for posting embarrassing childhood photos on Facebook.[10] Whilst that story has since been denounced as untrue,[11] it nonetheless raises an interesting question: could a child successfully sue their parents for sharenting? In attempting to answer that question this article analyses the remedies in English law that a child might use to prevent sharenting and to secure the removal of sharented information.

The sharenting phenomenon

Many parents use online platforms, including Facebook, Flickr, Instagram, Snapchat, Pinterest, Twitter, and Mumsnet to share anecdotes, quotes and personal information about their children, including information about behaviour, development, appearance, and health.[12] Photographs are often shared.[13] Indeed, sharenting frequently begins before birth, with the uploading of foetal ultrasound photographs.[14] Significant numbers of parents blog.[15] Whilst some bloggers use pseudonyms or avoid posting their children's faces, others openly disclose their children's names, images and locations.[16] Some parents use websites such as YouTube to vlog.[17] Depending upon the privacy settings a parent uses and the extent of their social media following, children's information may be shared with family, with parents' friends, acquaintances and professional networks, or the world at large. Even where a parent believes they are sharing to a limited audience, information may be disseminated further if an image is tagged, or reposted.[18]

Sharenting: the positives

Parents sharent for many different reasons. Sharenting allows parents to broadcast their children's achievements.[19] Sharenting also helps parents to avoid isolation, to obtain emotional, practical and social support,[20] and to share parenting advice.[21] Sharenting enables parents to enact and receive validation of their parenting.[22] Through sharenting, parents can share their experiences as parents, whether good, bad or frustrating.[23] Certain parents (including 'mommy bloggers' and parents whose children have complex medical needs) report that sharenting affords a sense of solidarity or community, increased feelings of connectedness and a sense of greater wellbeing.[24] Parenting blogs also provide outlets for creativity, enable parents to advocate particular parenting practices or philosophies, and to earn income.[25] Sharenting may provide significant benefits to parents.

There appears to be less evidence that sharenting benefits children. Nonetheless, sharenting can help children develop positive networks of family and friends.[26] Some parents suggest that maintenance of an online record of the child's life enables the child to learn about themselves.[27] Others submit that sharenting allows parents to build a positive social media image for children, to counteract 'negative behaviours they might themselves engage in as teenagers.'[28]

Sharenting: the negatives

Parents have always shared stories and photos with friends and family. Sharenting, however, takes sharing to a different level. Sharented information has a reach and longevity unimagined 20 years ago.[29] Sharenting may cause children substantial embarrassment and anxiety.[30] Where third parties comment harshly upon sharented information this can impact upon the child's self-respect.[31]

Many parents express concern about 'oversharenting', when parents share too much, or share inappropriate, embarrassing information.[32] A 2017 Ofcom survey suggests most UK parents who sharent consider carefully who can view photos or videos and would not share information their child would be unhappy with.[33] Nonetheless, parents do not always portray their children favourably. The confessional blogs of 'bad' or 'slummy mummies,' tell stories of frustration, boredom, and parental deficiencies,[34] and disclose feelings parents might never reveal to their children's faces (seemingly forgetting those posts may be on the internet for years).[35] Some adults with chronic disabilities have expressed concern about parents discussing their children's disabilities, emphasising the embarrassment they would have suffered had their parents discussed their medical condition online.[36] There are parents who post information knowing it will, or might, embarrass their child.[37] At least one vlogger is believed to have lost custody of his children because of the harm he caused by 'pranking' and verbally abusing them on YouTube.[38] Other parents have been condemned for 'shaming' their children online, subjecting them to humiliation as a response or remedy for bad behaviour.[39]

Online photo sharing also raises concerns. Photographs and videos accompanied by information about a child's school, age, or location may expose children to online grooming.[40] Even if a child's photograph is not accompanied by such information the metadata behind photographs and technologies which facilitate user tagging, automated facial recognition and the compilation of disparate pieces of information, can provide third parties with significant amounts of personal information about children's identity, location and friends.[41] Photographs may be altered and re-used on illegal websites.[42] Even seemingly innocuous photos can affect a child's reputation, incite bullying or expose children to ridicule.[43]

Where private information is shared without a child's consent or knowledge, this may infringe their human rights, including the right to privacy,[44] the right to respect for private life,[45] the right to data protection, [46] and the right to preserve one's identity.[47] Online information sharing affects adults' privacy too, but where the victim is a child the need for protection is greater. Paragraph 38 of the preamble to the GDPR spells out clearly, '[c]hildren merit specific protection with regard to their personal data.'

Could a child sue their parents – the position in English law

One hopes that most children who object to sharenting will be able to ask their parent(s) to stop sharenting and to remove any objectionable information.[48] If a parent refuses to do so, however, several civil regimes provide the child with means to seek an injunction to prohibit ongoing dissemination.[49]

The first remedy which will be considered is the law of confidence. The law of confidence has long been used by private individuals to protect personal information, private images,[50] details of home and family life[51] and medical information.[52] In recent years

this action has developed, and 'branched off into two general forms.'[53] Now, where a child objects to parental sharenting, they could potentially seek an injunction using either the classic, 'old-fashioned' breach of confidence action, or the newer 'privacy-related variety,' the tort of misuse of private information (MOPI).[54] Both regimes are considered.

This article will also consider how a child might use data protection law to enforce their right to determine when and how their information is shared. Data protection, is 'broadly analogous to the concept "information privacy,"[55] which effectively describes "the claim of individuals, groups or institutions to determine for themselves, when, how and to what extent information about them is communicated to others"'.[56]

All these regimes are as relevant to adults as to children. In practice, however, the child is in a weaker position than an adult. Few children will have financial means to bring court proceedings. Additionally, before a child can bring court proceedings on their own behalf they must demonstrate they have the necessary capacity to instruct a solicitor and to bring proceedings.[57] This requirement will prove particularly challenging for younger children, who are generally assumed to lack capacity.[58] We will also see that where the child's privacy has been violated by their parents, their legal position is potentially inferior to that of a child whose privacy has been violated by a stranger.

The 'old-fashioned' duty of confidence

More than 50 years ago Megarry J detailed the three requirements which must be satisfied for a claim for breach of confidence to succeed.[59] The information must be of a confidential nature. The information must have been imparted in circumstances importing an obligation of confidence, or it must otherwise have been clear that the information was to be kept confidential. Finally, there must have been an unauthorised disclosure of their information. Whilst in Megarry J's original formulation disclosure needed to be 'to the claimant's detriment', subsequent case law refinements indicate that this is no longer necessary.[60] Indeed in the 2013 Supreme Court decision in *Vestergaard Frandsen* Lord Neuberger advised that the classic case of breach of confidence now:

> *involves the claimant's confidential information… being used inconsistently with its confidential nature by a defendant, who received it in circumstances where she had agreed, or ought to have appreciated, that it was confidential.*[61]

That detriment is no longer essential is perhaps fortunate. Although a child might argue that sharenting has caused embarrassment, distress, or bullying, or has negatively affected their mental wellbeing, sharenting does not necessarily result in concrete harm.

Confidential information

Where an injunction is sought the child must demonstrate either that their parents intend to publish confidential information or that they have already published confidential information which should be protected by an injunction prohibiting further disclosure.

Much of the information parents share details mundane aspects of everyday life. A child might not consider such information to be confidential, or that disclosure constitutes a significant intrusion into their privacy. In any event, they cannot expect the law of confidence to protect 'trivial information' about daily life.[62] Health-related information will, however, ordinarily be considered confidential.[63] Given Lord Buxton's comments in *McKennitt v Ash* that 'events in a person's home' cannot be lightly intruded upon,'[64] certain elements of a child's home life, particularly images taken in bathrooms or bedrooms, might also be deemed confidential. What is less clear is whether the courts would consider information about a child's activities outside the home to be confidential.

To bring a successful claim in confidence, the information disclosed must have 'the necessary quality of confidence about it; it must not be something which is public property and public knowledge.'[65] Where children's activities are undertaken outside the family home and viewed by or enjoyed alongside many other people, *Woodward v Hutchins*[66] suggests that such activities might be considered either to be 'in the public domain' and/or 'shared experiences.' Such activities would not then be 'confidential' but might then be considered to be 'public knowledge'. Whilst *McKennitt v Ash* suggests *Woodward* should be treated with caution,[67] where a child enjoys family, school or sporting activities 'in public', with many others, it could certainly be argued that sharing information about such activities does not breach any duty of confidence. However, an alternative argument can also be made.

In *Tchenguiz v Imerman* Lord Neuberger recognises concerns about 'conflating the developing law of privacy under article 8 and the traditional law of

confidence.'[68] He suggests, nonetheless, that:

> *the touchstone suggested by Lord Nicholls of Birkenhead and Lord Hope of Craighead in Campbell, paragraphs [21], [85], namely whether the claimant had a 'reasonable expectation of privacy'[69] in respect of the information in issue, is, … a good test to apply when considering whether a claim for confidence is well founded. (It chimes well with the test suggested in classic commercial confidence cases by Megarry J in Coco v A N Clark (Engineers) Ltd [1969] RPC 41, page 47, namely whether the information had the 'necessary quality of confidence' and had been 'imparted in circumstances importing an obligation of confidence.')* [70]

If one adopts Neuberger LJ's approach one could argue that the child will have a reasonable expectation of privacy, and might furthermore found a breach of confidence claim, where 'family activities' are conducted publicly. Whilst in *Campbell,* it was suggested that courts will not usually consider ordinary activities in public to be confidential or private,[71] in contrast, in *Weller* and in *Murray* the Court of Appeal were prepared to accept that where children were engaged in family activities,[72] and were subjected to clandestine paparazzi photography, those children had a reasonable expectation of privacy, even in public. The most recent case to consider a child's expectation of privacy in public is *Re JR 38,*[73] a case which saw the Supreme Court divided 3-2. Whilst in this case the majority were not prepared to accept that JR's activities (criminal rioting) fell within the 'protected zone of interaction between a person and others', or was 'the type of activity' which Article 8 protects, Lord Toulson's comments, recognising the importance of the 'circumstances' in which a photograph is taken, and the nature of the activity in which a child is involved,[74] leave the door open to the possibility that some family interactions in public might be considered subject to a reasonable expectation of privacy. This does not, of course guarantee that the courts will treat information about such activities as *confidential,* but, if not, as discussed below, the MOPI tort might alternatively be used to prevent publication of information relating to such activities.

When the duty arises

Assuming a child can prove that their information is confidential, they must then demonstrate why their parent was subject to a duty of confidence. There is no case law considering whether the parent-child relationship imports an obligation of confidence. It is clear, however, that a relationship of confidence is no longer essential to the establishment of a duty.[75] To establish whether a duty arises the court is more likely to consider the circumstances in which the parent obtained the objectionable information. Certainly, where a child blurts information out in public or on social media there will be no binding obligation of confidence in that information. [76] It seems equally clear that a parent could be expected to maintain confidence if a child, in private, asks their parent to keep information 'confidential' or 'secret'. Where a child expected confidences to be kept, but did not explicitly say so a duty of confidence might also be found to exist:

> *… [A] duty of confidence will arise whenever the party subject to the duty is in a situation where he knows or ought to know that the other person can reasonably expect his privacy to be protected.*[77]

The test is an objective one.

> *For a duty of confidentiality to be owed … the information in question must be of a nature and obtained in circumstances such that any reasonable person in the position of the recipient ought to recognise that it should be treated as confidential. … the law would defeat its own object if it seeks to enforce in this field standards which would be rejected by the ordinary person.*[78]

A key difficulty in the sharenting context is that parents enjoy many of the same experiences as their children. The information they share online will often tell a story not only of the child's life, but of the parent's life. This poses problems for the child claimant. How does one determine where a parent's identity ends and a child's begins, and whether the child or the parent is the owner of the sharented information?[79] Parents might well argue that when sharenting they are breaching no duty of confidentiality, but are merely exercising their Article 10 right to freedom of expression, disclosing *their experiences*. Whilst Ms Ash unsuccessfully raised similar arguments in *McKennitt v Ash,*[80] the reality was that in *McKennitt* the claimant was very much the focus of the disclosures.[81] Where a parent genuinely wishes to share information about their own experiences the position may be less clear. As Buxton reminds us in *McKennitt* 'all of these cases are fact sensitive.'[82]

Justifying disclosure

Even if the child establishes that their parent owes a duty of confidence, their claim for an injunction may still be unsuccessful if disclosure is justified.

Commonly defendants will justify disclosure on the basis that disclosure is in the public interest or that the information is in the public domain.[83]

To justify their sharenting a parent might argue, for example, that: disclosures were made in the exercise of their freedom of expression; information is shared with wider family for the benefit of the whole family (including the parent and child) or that disclosures are necessary to obtain support from family, friends or community (to benefit the child). They might also argue that talking about their parental experiences benefits the wider community and is thus in the public interest. Where a defendant raises a public interest defence they must, however, not only establish that disclosure is in the public interest, but that there is a greater public interest in disclosing the information than in keeping the information confidential; effectively that it 'is in the public interest that the duty of confidence should be breached'. [84] Although none of these potential arguments has been put to the courts, it seems unlikely that the parent could justify breach of confidentiality where sharenting is undertaken merely to update family and friends. A parent might, therefore, instead choose to raise the public domain defence.

Even if a child can establish that their parents have shared confidential information, where a parent has shared that information with the world at large or has a substantial social media following, they could argue that the information has become 'so generally accessible' that, it is 'in the public domain' and 'cannot be regarded as confidential.' [85] In such circumstances, the parent might argue that there is no purpose to be gained from an injunction. Certainly, in *Giggs (formerly CTB) v Newsgroup Newspapers Ltd and Thomas*[86] Eady J indicates that 'the court will not attempt to prevent publication or discussion of material that is genuinely in the public domain since, where that is so, there will no longer be any confidentiality or privacy to protect.'[87]

The problem is that where information has been viewed by a limited audience a court may not consider that confidentiality has gone for all purposes. Ultimately, it 'is not a black and white distinction between public and private'. The court will need to consider the particular facts and decide whether, 'notwithstanding some publication, there remains a reasonable expectation of some privacy.'[88] The difficulty is compounded by the fact that '[t]he legal principles determining the public domain proviso were formulated in a world predating social media.' [89] Whilst in *Stephens v Avery,* Sir Nicholas Browne-Wilkinson VC indicated, 'information only ceases to be capable of protection as confidential when it is in fact known to a substantial number of people,'[90] there is no clear agreement amongst the judiciary as to what constitutes 'a substantial number' or when publication on social media constitutes publication in the public domain.[91] Potentially, when a parent shares information with a small number of Facebook friends, that information might be considered to retain its confidential nature. If the information is shared with several hundred 'friends' or made publicly available, the child may struggle to establish that such information is not in the public domain. In such a case, whilst a child might succeed in a claim for damages for breach of confidence, they might struggle to obtain an injunction.

Moreham and Warby comment that '[t]he limitation of the breach of confidence action is … that it does not cover information which is private but not obviously confidential nor information which is already in the public domain.'[92] This comment is clearly supported by the analysis above. Fortunately, the MOPI action offers the child a possible alternative cause of action.

The MOPI tort emerged out of the breach of confidence action, and indeed the two regimes have become so entwined that it may not always seem clear how they differ one from the other.[93] The two actions nonetheless rest on different legal foundations and protect different interests, 'secret or confidential information on the one hand and privacy on the other.'[94] Whilst 'the duty of good faith' lies at the heart of the classic confidence action, the MOPI tort focuses upon 'protection of human autonomy and dignity – the right to control the dissemination of information about one's private life and the right to the esteem and respect of other people.'[95] Since the MOPI tort provides protection for information about individuals' private lives, including information which would not ordinarily be considered 'confidential',[96] individuals who have suffered intrusion into their private lives may find it easier to satisfy the requirements of the MOPI tort than breach of confidence. A child may be able to obtain a remedy under MOPI, even if their information has been and continues to be so widely sharented no injunction for breach of confidence would be available.[97] Indeed, *PJS* makes clear that repeated disclosures may constitute further invasions of privacy, even where disclosures are made to individuals to whom disclosure was previously made.[98]

The tort of misuse of private information

To succeed in their MOPI claim the child must satisfy both limbs of a two-stage test.[99] They must first establish that they had/have a reasonable expectation of privacy in the information which parents have shared or intend to share. They must then establish that their right to privacy prevails over their parents' rights. In the sharenting context the application of the MOPI tests is complicated by the fact that the privacy expectations of children and their parents appear often to be treated as one and the same.

A reasonable expectation of privacy

A child does not automatically have a reasonable expectation of privacy.[100] To determine whether any individual has a reasonable expectation of privacy the court will consider 'what a reasonable person of ordinary sensibilities would feel if she was placed in the same position as the claimant and faced with the same publicity.'[101] It will take account of all the circumstances, including:

> *the attributes of the claimant, the nature of the activity in which the claimant was engaged, the place at which it was happening, the nature and purpose of the intrusion, the absence of consent and whether it was known or could be inferred, the effect on the claimant and the circumstances in which and the purposes for which the information came into the hands of the publisher.*[102]

In *Weller*[103] Lord Dyson considered the application of these factors where a newspaper had taken and published photographs of three children. Concluding that the children did have a reasonable expectation of privacy, Lord Dyson emphasised that the claimants were children who, as children, were not in a position to have knowingly or accidentally laid themselves open to being photographed. He noted also that, for children, the publication of even anodyne images, and the resulting potential for their identification might cause harms, including embarrassment, bullying and threats to their safety and security.[104] Whilst *Weller* concerned proceedings brought by celebrity parents who had deliberately kept their children out of the public eye, many of Lord Dyson's comments might be applicable to a child who objects to parental sharenting. The case of *Weller,* however, is also significant for other reasons. First, it is one of several cases that recognise the special position of children, and the particular harms that publicity may cause them.[105] Most importantly, Lord Dyson confirms in *Weller* that although 'the broad approach that must be adopted to answering the question whether there is a reasonable expectation of privacy is the same for children and adults, there are several considerations which are relevant to children (but not to adults) which may mean that in a particular case a child has a reasonable expectation of privacy where an adult does not.'[106]

Ultimately, of course, the court will consider each case on its facts, taking account of factors such as the child's age, and whether the child themselves uses social media, or has objected to disclosure by third parties such as schools or sporting organisations. It is suggested, however, that in the sharenting context there is a fundamental question that the courts must also ask when considering whether a child has reasonable expectation of privacy; *is it reasonable for children to expect their parents not to sharent*?

Reasonable expectations of privacy in the digital age

Moreham and Warby suggest that:

> *The reasonable expectation of privacy test can be seen, at least in part, as shorthand for whether, in a given situation, the protection of privacy is consistent with prevailing social norms. … if applied appropriately, the reasonable expectation of privacy test allows courts to ask… whether the scenario was one in which there was or should be an objectively recognised social norm that privacy should be respected ...*[107]

Steijn explains that information sharing behaviours are regulated externally by four factors; law, the market, architecture and norms (the norms that determine what kind of information is appropriate for sharing in a given context being termed 'norms of appropriateness.')[108] He explains further that it takes time for norms to develop to accommodate new technologies.[109] This undoubtedly is the difficulty for the courts in the sharenting context. Whilst headlines suggest 'privacy is dead', that sharenting is the norm,[110] the 2017 Ofcom report suggests many parents still consider children can expect their information to remain private, and that parents are divided about the merits of sharenting.[111] A court may struggle, therefore, to determine what 'the norm' is, and thus to conclude either that children have a reasonable expectation of privacy in the information their parents hold, or that they must expect their information to be sharented.

Of course, the matter is complicated by the fact that children's privacy expectations may be very different

to adults. Indeed, Steijn identifies striking differences in the normative expectations of adults and children.[112] Even amongst children expectations may vary; the expectations of children born in the past five years may be very different to those of child born prior to the emergence of Facebook (who might validly argue that they did not expect their parents to share their information online).

The fact that a child may have different privacy expectations to their parents is a matter that itself also requires further consideration. In a number of cases, the ECtHR and the English courts have stressed the importance of obtaining parental consent to publication of children's information, acknowledging the role of parents as consent holders or privacy stewards for their children. The courts appear, in some cases, to also conflate the child's expectation of privacy with the parent's expectation of privacy for that child. This poses potential problems in the sharenting context.

Whose expectations?

In the cases of *Reklos and Davourlis v Greece*[113] and *Bogomolova v Russia,*[114] the ECtHR considered the failure of the Greek and Russian courts to protect the image rights of a young baby (*Reklos)* and a small boy (*Bogomolova)*. In both cases, the ECtHR stresses the importance of the parents not having given consent to photographs being taken or retained (*Reklos)* or published (*Bogomolova)*. Crucially, in *Reklos,* the fact that the *parents* had not given consent to the taking of the child's photographs led to a conclusion that the *child's* Article 8 right to private life had been breached.[115]

In *Reklos,* where the child was a baby, it is unsurprising that the ECtHR concluded both that the parents should oversee the exercise of the right to protection of their son's image and that their prior consent to photography was indispensable.[116] Concerns, have, however been raised about such an approach. Indeed, Hughes queries:

> *at what point are children able to consent for themselves; and what is the relationship between parental consent and the child's consent. These questions need exploring as the Court's blanket assertion that consent lies with the parents has the potential to undercut the very status of the child's Article 8 ECHR right as a 'right' held by the child.'*[117]

To date, the English courts have not articulated how *Reklos or Bogomolova* might apply in English law. Lord Dyson's judgment in *Weller* is, however, a striking example of the judiciary's acceptance that parents are entitled to decide what happens to their children's information (especially but not necessarily when they are young):

> *it is parents who usually exercise this decision-making for young children. Thus, if parents choose to bring a young child onto the red carpet at a premiere or awards night, it would be difficult to see how the child would have a reasonable expectation of privacy or article 8 would be engaged. In such circumstances, the parents have made a choice about the child's family life and the types of interactions that it will involve. A child's reasonable expectation of privacy must be seen in the light of the way in which his family life is conducted.*[118]

In *AAA,* Lord Dyson suggests further that in evaluating the strength of a child claimant's reasonable expectation of privacy, a judge would be entitled to take account of any relevant conduct of parents.[119] Similarly in *Murray* Sir Anthony Clarke suggests that 'if the parents of a child courted publicity by procuring the publication of photographs of the child in order to promote their own interests, the position would or might be quite different from a case like this, where the parents have taken care to keep their children out of the public gaze.'[120]

This line of reasoning is controversial[121]. It suggests that a parent's expectations and decisions on a child's behalf may trump the child's own expectations and that effectively, a child's right to privacy may be waived or curtailed by decisions taken by their parents.[122] Whilst in *Murray* and *Weller,* the Court of Appeal seemingly considers a claimant's status as a 'child' to be significant, a point in their favour, the court's reliance upon parents as privacy stewards at the same time potentially weakens the child's position as a claimant. The fact that the rights of children are in the hands of their parents may have not been problematic in *Reklos, Murray* or *Weller,* but it undoubtedly poses problems where older children have different privacy expectations to their parents, particularly when the child wishes to preserve their privacy but their parents do not.[123] In *Murray*, Sir Anthony Clarke acknowledges that a 'child has his own right to respect for his privacy distinct from that of his parents.'[124] Subsequent decisions do not, however, adequately recognise that children have an absolute right to privacy, independent from their parents, and that children should, as they mature, be entitled to enforce that right, irrespective of whether their parents value privacy.[125] A child should

not, however, be denied a right to privacy, see their privacy expectation weakened, or their sharenting claim fail, simply because their parents court publicity.[126]

The second stage – the ultimate balancing test

If the first stage of the MOPI test raises numerous issues, the second is no less problematic. The MOPI jurisprudence discusses at length the need to balance the claimant's Article 8 rights against the defendant's Article 10 rights. This is logical given that typically MOPI claims are brought by individuals against media defendants or against individuals who wish to exercise their Article 10 rights to freedom of expression. The argument usually raised by such defendants is that dissemination is required in the public interest, or will contribute to a debate of general interest. In a sharenting case, a parent certainly might justify sharenting on the basis that they are exercising their Article 10 rights. They might, however, additionally argue that the court should consider their Article 8 right to respect for family life. Article 8 offers parents protection from state interference in family life, and affords them autonomy rights, rights to determine matters relating to the family's upbringing. A parent might argue that Article 8 affords them *a right to decide what information about the family they share*.

Article 8 v Article 10

The Article 10 point is arguably more straightforward for the courts to determine given their long experience of balancing conflicting Article 8 and 10 rights. It is accepted practice that in such situations the court will resort to Lord Steyn's guidance in *Re S:*

> *Firstly, neither article has as such precedence over the other. Secondly, where the values under the two articles are in conflict, an intense focus on the comparative importance of the specific rights being claimed in the individual case is necessary. Thirdly, the justifications for interfering with or restricting each right must be taken into account. Finally, the proportionality test must be applied to each. For convenience I will call this the ultimate balancing test...*[127]

Whilst neither right has precedence, it is important that the claimant is a child. In proceedings under the Children Act 1989 the courts must treat the child's welfare as a paramount consideration.[128] Outside such proceedings no statute requires the courts, parents or the state to treat the child's welfare as paramount. Nonetheless, the court considering a child's MOPI claim cannot ignore that child's interests. As Lord Dyson made clear in *Weller*: 'the primacy of the best interests of a child means that, where a child's interests would be adversely affected, they must be given considerable weight.'[129] This is an approach which accords with the requirements of Article 3 of the United Nations Convention on the Rights of the Child (UNCRC), which stipulates that '[i]n all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration.'

The UNCRC recognises that children have particular vulnerabilities which justify additional protection. The domestic courts too are increasingly acknowledging the importance of children's rights, and the need to protect children from the harms caused by publicity or revelation of their identity.[130] In *Weller,* Lord Dyson explicitly considers the need for the child claimants to be protected from embarrassment, bullying and 'potentially more serious threats to their safety' which might be caused by publication of their images.[131] Even in cases brought by adult claimants, the courts have been willing to provide injunctive relief to prevent publication of information which might cause these claimants' children embarrassment or distress or result in bullying.[132] Whilst there are clearly differences between the facts in the decided MOPI cases and the sharenting case, the risks that may be posed to children in the sharenting context, risks of bullying, embarrassment and more serious threats (such as approaches from those seeking to groom children), are comparable. They are of significant importance when weighing the child's rights against the parents' Article 10 rights.

In relation to the Article 10 right to freedom of expression, the courts will undoubtedly consider the nature of the parent's disclosures and the contribution that they will make to debates of general interest. In most sharenting cases, parents will be making 'low value' communications, matters of personal rather than public importance, which offer no contribution to public debate.[133] It is arguable, again, that given the nature of the information shared by parents the courts might not consider sharenting to be in the public interest, or at least to not outweigh the child's right to privacy.

The family court's jurisprudence seems also to lend weight to the child's privacy claim.[134] *In Re J* a father, who objected to the removal of his fourth child into local authority care, used social media to share

information about J's removal from the family. Issuing an injunction to prohibit further disclosures Munby J makes clear that online discussion cannot

> *be allowed to go so far as to prejudice the rights of the individual children involved. There is a distinction to be drawn between, on the one hand, freedom to discuss the operation of the family justice system and the conduct of individual cases and, on the other hand, the freedom to disseminate identifying particulars of specific children which serves to cause, or risk causing, harm to them. … Article 10 cannot be allowed to justify conduct which interferes with a child's Article 8 rights to an extent that is harmful to him.*[135]

In *Re J* Munby refers to J discovering as he gets older that 'graphic and potentially embarrassing material … exists in a form accessible by the public, and which may be re-published at any time and for potentially nefarious purposes.' He highlights the potential for J to suffer bullying and other harms (including harm to J's emotions and his ability to develop relationships with others) because of revelations concerning his involvement in care proceedings. Where parents knowingly or unwittingly share intimate information about a child's family situation, where they disclose sensitive information about disabilities, play online 'pranks' on their children, or 'shame' then online, sharenting may cause significant harm. *Re J* suggests that such children would have a strong argument to support removal of such information from the online sphere.

Article 8 v Article 8

The English courts have not considered in the context of a MOPI claim how the parental right to respect for family life, which protects parents' rights to determine matters relating to the family's upbringing, should be balanced against the individual privacy rights of the children. Cases such as *Weller, Murray, AAA*, *Reklos* and *Bogomolova* seem to suggest that parents have rights to determine how information relating to the family is used and given the approach the courts have taken to date one must question whether any court would be willing to condemn a parent who sharents because they want to celebrate their children's achievements. Many children, however, might argue that they should be the ones to decide how their information is used, and not their parents. They might argue, further, of course that parental decisions to share family information are not always in the child's interests.[136]

The child's right to a private life and the parents' right to respect for family life are, of course, both qualified. Ultimately, therefore, even if a court accepts that a parent has a right to determine how their child's information is used, the court may nonetheless consider it appropriate to intervene where sharenting results in, or poses risks to mental or physical health, or impacts on children's privacy.

As Sedley LJ explained In *Re F (adult: court's jurisdiction)*:

> *The family life for which Article 8 requires respect is not a proprietary right vested in either parent or child; it is as much an interest of society as of individual family members and its principal purpose, at least where there are children, must be the safety and welfare of the child. … [Its] purpose, in my view, is to assure within proper limits the entitlement of individuals to the benefit of what is benign and positive in family life.* [137]

The jurisprudence of the ECtHR lends additional support to arguments that where the parent's right to family life conflicts with the child's best interests, it is the children's best interests that are the primary consideration[138] or paramount.[139] The question that is not clearly answered in any jurisprudence, however, is whether, the court would consider it in the child's best interests to order their parents to stop sharenting absent actual harm or a risk of harm, and where there is 'merely' interference with the child's ability to determine how their information is used.

Is harm essential?

Hughes has suggested:

> *that the only situations in which the courts have given serious consideration to the child's right to privacy are situations in which either a high degree of protection is afforded to that privacy-related interest in the adult context or where the child is vulnerable to a clearly identifiable harm. This is problematic because the right to privacy is not usually, and should not be, contingent upon the individual suffering harm.* [140]

Certainly, in *Weller* and in *Re J* it is the harms to which the children are potentially exposed (embarrassment, bullying, and other 'threats') which seemingly provide justification for the court's decision to favour the children's rights over the media defendant and J's father. In *Murray,* however, Sir Anthony Clarke suggests that harm is not essential, arguing that:

> *one needs … to differentiate between the case where the child has for medical or some other personal reasons come to the knowledge of the general public and for those very reasons may be particularly vulnerable to harm from intrusive press exposure and the much more ordinary case… Even in cases of this kind the Court is bound to have regard to any particular harm (actual or prospective) which the child may suffer from having his image publicly displayed. But in most such cases … the child will have suffered no upset or harm. The purpose of the claim will be to carve out for the child some private space in relation to his public appearances.*

It certainly seems wrong to expect the child to establish that they have suffered or are vulnerable to a clearly identifiable harm, because of parental sharenting. Not only are such harms not always easy to identify or quantify,[141] a focus on harm may prevent a child from obtaining a remedy under the MOPI tort if their only objection is to the dissemination of their private information.

Children value privacy, and the ability to control access to their information.[142] 'Privacy serves an important function in the development of individual autonomy, as the mechanism by which boundaries between ourselves and others are established and maintained.'[143] Privacy is important, particularly to older children for whom privacy is more central to their development and integrity, and for whom, therefore, the intrusion is experienced as a greater violation.[144] It is argued, therefore, that when a child brings a sharenting claim, whether the claim is brought because the child has suffered embarrassment, anxiety or hurt, or because the child simply wishes to maintain their privacy, the courts should be more willing to grant an injunction to prevent or limit disclosure than if the claimant were an adult objecting to online dissemination of their private information, and notwithstanding that the person who made those disclosures is that child's parent.

The difficulty, of course, as noted earlier, is that even if the courts would be minded to grant an injunction to prevent sharenting, few children will have the finances to be able to bring court proceedings. Whilst this is a major issue for children who wish to enforce their rights, this does not mean that such children are without remedy. One further regime exists which also potentially affords children with a remedy against ongoing sharenting.

Data protection

The rules governing processing of personal data within the UK, including the sharing of information relating to a child, are detailed in the Data Protection Act 1998 ('the DPA'). This gives effect to European Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('the Directive'). This details certain conditions under which personal data processing may be lawfully undertaken, the rights of individuals whose personal data is processed and certain standards to which those who process data must adhere. Where a child believes their data protection rights have been infringed, their remedy lies under the DPA, which should be interpreted in accordance with the Directive, to give full effect to the right to data protection detailed in the European Charter.[145]

Obligations imposed on data controllers by the DPA

The Directive and the DPA stipulate certain conditions that apply when an individual processes personal data. The leading European case of *Lindqvist*[146] confirms that where one person refers to another individual on an internet page, identifying then by name or some other means, they will be processing that individual's personal data by automatic means, within the meaning of Article 3(1) of the Directive. Accordingly, if a parent shares information online which relates to and identifies their child, they will be considered to fall within the remit of the Directive/the DPA and will be obliged to comply with the data protection principles detailed at Schedule 1 DPA, unless one of the exemptions in Part IV of the DPA applies.

In practice, this means that when a parent shares information about their child online they should act in accordance with the law and act 'fairly', letting the child know for what purposes their information is being used and using the information only for those purposes. Sharenting that results in a breach of confidence or the misuse of a child's private information is itself unlawful and therefore a breach of the DPA. If a parent has not told their child that they intend to share their information or photographs online, arguably, the fair processing requirement has not been satisfied. Parents should use appropriate technological means to avoid unauthorised or unlawful processing of that information. This is important given the evidence that unscrupulous individuals may use images of children to identify and groom children, or

may manipulate images and republish them on other websites. Parents should share no more information than is necessary, and ensure that information is relevant, accurate and, if necessary, kept up to date. Where hundreds of childhood photographs have been shared, a child might argue that parents have shared more information than is necessary. A teenager might also argue that photographs of their formative years, which no longer represent who they now are, are not up to date and are being made public for longer than is necessary.[147]Finally, parents must not share information unless one of the conditions in Schedule 2 DPA is met. If the data is sensitive personal data (information about racial or ethnic origin, political or religious beliefs, health or criminal behaviour) at least one Schedule 3 condition must also be met.[148]

Parents will be able to satisfy a Schedule 2 condition, if their child consents to the sharenting,[149] or where '[t]he processing is necessary for the purposes of their own legitimate interests or the legitimate interests of those to whom the data are disclosed. (This last condition is subject to a caveat that processing may be considered unwarranted where it is prejudicial to the rights and freedoms or legitimate interests of the child).[150] A parent might argue that they have a legitimate interest in sharing their children's information with friends and family, and/or that they are sharing information as permitted by their own right to freedom of expression. The issue then is whether sharenting is nonetheless unwarranted because of the prejudice caused to the child's privacy or wellbeing.

If a parent wishes to share sensitive personal data, meaning Schedule 3 applies, they must additionally have the child's explicit consent to sharenting,[151] unless the child has already deliberately made the sharented information public.[152] The child's consent is thus relevant both under Schedule 2 and under Schedule 3. One must question, however, how many parents seek their children's consent every time they share information online, particularly if the child is very young and lacks capacity to provide consent. (Whilst parents often consent to information sharing on behalf of young children there are obviously issues with parents providing consent to their own processing). Many parents may be unaware of the need to seek consent, or indeed to comply with any of the obligations imposed by the DPA. This does not, however, exempt a parent from compliance.

Remedies for non-compliance

The child may ask the Information Commissioner's Office ('the ICO') to undertake an assessment to determine whether their personal data is being processed in breach of the DPA. [153] This costs nothing. If the ICO is satisfied that there has been a serious breach of the data protection principles, the ICO may serve a legally binding enforcement notice requiring their parents to erase the objectionable information.[154]

Section 10 DPA additionally provides data subjects with a right to prevent processing likely to cause damage or distress. Under section 10, the child may ask their parents, in writing, to stop posting and/or to remove the information posted online within a specified period. The notice should state why the child believes continued online disclosure is causing or likely to cause them unwarranted and substantial damage or distress.[155] (Whilst sharenting is unlikely to cause a child financial damage, the case of *Google Inc v Vidal-Hall* suggested, albeit in the context of a compensation claim under s 13 rather than under s 10, that the term 'damage' should be widely interpreted to incorporate distress, or 'moral damage.'[156]) Assuming that the child has not consented to the sharenting, the parent must respond within twenty-one days to confirm either that they have complied with, or to what extent they will comply with the request, or stating why they consider the request unjustified.[157] If the parent ignores the notice, the child is entitled to seek court assistance. If the court is satisfied that the notice is justified and that the parent failed to comply with it, the court may then order the parent to comply with the notice, to the extent that the court thinks fit.

On the face of it, the DPA affords a child a real chance to secure removal of sharented information and to prevent ongoing sharenting. Unfortunately, however, success is not guaranteed: where the personal and household exemption applies, a parent may be exempted from compliance with the data protection principles and the requirement to satisfy the Schedule 2 and 3 conditions.

Article 3(2) of the Directive states that the Directive does not apply to the processing of personal data 'by a natural person in the course of a purely personal or household activity.'[158] The position in European Union law is that the personal and household exemption outlined in Article 3(2) should be interpreted narrowly. In *Lindqvist* the ECJ suggested the exemption would not apply where personal information was published online and made available to an indefinite

number of people.[159] The Article 29 Working Party[160] has since suggested that it might be appropriate to distinguish between those who restrict access to a small number of individuals (to whom the exemption applies) and those who have a high number of contacts or allow information to be made publicly available (who are unlikely to be able to rely upon the exemption).[161] Their approach would mean that parents who blog and vlog would be subject to the directive whilst parents who share only with limited, selected 'friends' would be covered by the exemption. Many data protection regulators have, however, adopted a stricter approach, akin to that in *Lindqvist*, considering all online publication to fall within the Directive.[162] In the UK, strikingly, the ICO has taken an entirely different approach.

Section 36 DPA is significantly broader than Article 3(2), stating that '[p]ersonal data processed by an individual only for the purposes of that individual's *personal, family or household affairs (including recreational purposes*) are exempt from the data protection principles and the provisions of Parts II and III' (author's emphasis). The ICO's interpretation broadens the exemption still further. Indeed, the ICO suggests that when an individual shares information online, in a personal capacity, purely for their own domestic or recreational purposes the exemption *will apply*, irrespective of the nature of the data being shared, what that data reveals, or the number of people to whom that information is revealed.[163] Most sharenting parents will accordingly be able to rely upon the exemption, although some parents who blog primarily to earn income might still be caught by the DPA.[164]

For a child, based in England, who objects to parental sharenting, the ICO's stance poses a significant problem. Since the ICO has made clear it 'will not consider complaints made against individuals who have posted personal data whilst acting in a personal capacity, no matter how unfair, derogatory or distressing the posts may be,'[165] the child can obtain no remedy for sharenting through the ICO. One small crumb of comfort for the child can be found in Tugendhat J's comments in *The Law Society v Kordowski,* which suggest that the courts accept that online dissemination of another person's information (particularly where dissemination breaches a duty of confidence) may breach the DPA.

Perhaps more importantly for the child, a new General Data Protection Regulation (GDPR) replaces the Directive in May 2018 introducing a new legal regime, which strengthens the right to data protection and provides individuals with greater control over their personal data.[166] Although the GDPR will only be directly enforceable within the UK for a short period prior to the UK's exit from the European Union, a new Data Protection Act (currently before parliament) will ensure that the UK affords the same protection to personal data as other European Union states post-Brexit.

The GDPR, the Data Protection Bill and the role of social media providers

The GDPR, in contrast to the Directive, acknowledges the importance of considering children's rights and vulnerabilities. Indeed, the preamble paragraph 38 states that '[c]hildren merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data….' The GDPR also, however, views parents as stewards of their children's privacy, as the people best placed to consent to use of children's information, at least until such time as the child has capacity to consent themselves.[167] Concerns have been raised that the GDPR does not appear to provide children (such as those whose information is sharented by their parents) with significantly increased protection.[168] Nonetheless, delving into the detail of the GDPR, it is possible that the GDPR could provide children with an improved means by which to secure removal of sharented information.

It should first be noted that the GDPR lays much greater emphasis on the importance of obtaining explicit consent to the processing of personal data. This is important. It has been suggested that parents should be seeking their children's consent before they sharent. Indeed Steinberg notes 'By age four, children have an awareness of their sense of self' and can build friendships, reason and compare themselves with others. She suggests further that:

> *Parents who post regularly can talk about the internet with their children and should ask young children if they want friends and family to know about the subject matter being shared. As is the case in many aspects of children's rights, the weight given to the child's choice should vary with respect to the age of the child and the information being disclosed. But parents should be mindful that even young children benefit from being heard and understood.*[169]

Of course, unless parents are aware of the new consent provisions they are unlikely to adopt a different approach, seeking consent from their children. To ensure that children's data protection rights are effectively protected parents and children need to be provided with better information about their rights and responsibilities. If parents do not seek their children's consent, however, or if children decide later in life that they wish to remove sharented information, the GDPR also affords a potential remedy for the child in the form of the 'right to erasure'.

A right to be forgotten was included in the Directive and the DPA. The scope of the revised right is, however, much wider.[170] Significantly, the law no longer requires proof that substantial damage or distress is likely to be caused. The right now applies whenever a data subject withdraws consent to processing, where processing is no longer necessary, where processing is unlawful, or where the individual objects to processing and there are no overriding legitimate grounds for processing.

Fully cognisant of its obligations to comply with the GDPR, in the Queen's speech the government stated that it would introduce legislation affording individuals new rights 'to require major social media platforms to delete information held about them at the age of 18.'[171] It was of some concern to read that an individual should have reached 18 years old before they could exercise the right to erasure, given that the DPA currently imposes no age requirements. The government has subsequently confirmed, however, that there is no requirement to have reached 18 years old before the right to erasure may be exercised.[172] Whilst the government has not explicitly considered how a child might use the right to erasure to remove sharented information (in its August 2017 statement of intent its suggestion was that the right would be used by 18-year-olds to remove information they had shared as children) [173] there is clearly scope to use the right for this purpose.

Of course, anyone can ask a social media provider such as Facebook to remove information posted online by a third party. Given that there is no charge or requirement to prove capacity, children could already be using such take down procedures. Unfortunately, however, there is no legal obligation for social media providers to remove the types of information that children might consider objectionable or embarrassing. Although the European Commission has made clear it expects online platforms to play a proactive role in removing online content, the European Commission's priority is the removal of 'illegal content', namely hate speech, speech which incites terrorism, child sexual abuse material and content which infringes intellectual property rights and consumer protection. [174] It does not expect providers to remove information such as a parent might share about their child. Unsurprisingly, therefore, Facebook's clear position is that it will not automatically remove information because someone finds it disagreeable. It will remove posts, which pose a genuine risk of physical harm, and posts that might result in self-injury, bullying and harassment, criminal activity or sexual violence and exploitation.[175] It will, however, only remove photos and videos that an individual reports as 'unauthorized' if removal is required by relevant privacy laws in the complainant's country.[176] As the above analysis shows, there is no legal provision that would explicitly require Facebook to remove sharented information. This is unfortunate. The transnational and rapidly evolving nature of internet services and providers pose significant challenges for the legal process. Whilst it has been suggested that intermediaries such as Facebook, YouTube, Twitter and Google should be taking greater 'responsibility for children's rights in the digital age,'[177] and some have even gone so far as to suggest that these organisations 'should have a duty of care to consider young children's privacy and best interests in their operations', with social media settings 'privacy respecting as default when images or information about young children are concerned,'[178] the child who objects to parental sharenting is unlikely to be able to secure removal of sharented information by contacting social media providers directly, at least not before the improved right to erasure comes into force.

Alternatives to the law

Whilst several legal remedies are available to children who object to sharenting, none are guaranteed success and the financial costs in bringing a court claim are likely to be high. The emotional costs and the potential damage to the family unit cannot be ignored.[179] It is perhaps for this reason that academics have suggested that more should be done to educate parents and children about the impact of 'sharenting' and the level of personal information parents are exposing by sharenting.[180]

There are alternatives to mainstream media which could be used by parents who wish to exercise their right to share information, whilst still providing some protection to their children's privacy. Messaging services such as Snapchat, where photos disappear, and WhatsApp which confines messages to a

group, have been suggested as a means to manage 'different levels of broadcasting'[181] (although of course screenshots of snapchat messages can be shared and photographs shared via WhatsApp are automatically downloaded to a recipient's phone and thus can potentially be disseminated further). There is a wealth of private online social networks for families (23 Snaps, Efamily, Family Wall, JustFamily, FamilyLeaf, MyFamily.com, Rootsy, Origami). Ammari et al also reported that a number of participants in their research used 'Dropbox, Google+, LiveJournal, Flickr, Shutterfly, Snapfish, Instagram and iCloud when they wanted to share to smaller or more private audiences than they had on Facebook.' Others used iOS photo (also perceived as more private).[182]

The use of private social networks for limited sharing may, of course, not offer a viable alternative to blogging, but Steinberg has suggested that it is possible for such parents to exercise their right to freedom of expression whilst protecting their children from harmful information sharing. She suggests, for example, that parents should: familiarise themselves with the privacy policies of the sites with which they share; set up notifications to alert them when their child's name appears in a google search result; consider sometimes sharing anonymously; be cautious about sharing their child's actual location; give their child 'veto power' over online disclosures; consider not sharing pictures revealing their children in any state of undress; and more generally consider the effect of sharenting on their child's current and future sense of self and well-being.[183]

Whilst there are likely to be few people who would disagree that an education campaign could help clarify the rights and responsibilities of parents and children, questions have been raised about who should undertake this crucial educative role.[184] In France and Germany the police have used social media to advise parents of the dangers inherent in sharenting and the need to protect the private life of minors.[185] Since sharenting is unlikely to result in commission of any criminal offence in the UK, education might perhaps better lie elsewhere, with government, with the ICO, who has a key role in upholding information rights and already provides guidance for the public on related matters, such as photography at school events,[186] or with a body such as the UK Council for Child Internet Safety, which already provides guidance for parents on children's use of social media. Since the Children's Commissioner is already working with government to implement a digital citizenship programme in schools, guidance for children sharenting could be included within that programme.[187]

Conclusion

Whilst parents have long shared information about their children, with friends, family and colleagues, online disclosures are of much longer lasting impact and significance. How the English courts will respond to the new phenomenon of sharenting, and the challenges it poses to children's privacy has yet to be seen. On the face of it a range of legal remedies are available to anyone who objects to the online dissemination of their personal, private or confidential information. In practice, however, where a child's privacy has been violated by their parents their ability to obtain a remedy is, in some regards, potentially more limited than that of an adult whose privacy has been violated by a stranger.

Children are afforded their own rights to privacy by international law. This includes a right to privacy against their parents. Unfortunately, it is clear that the ECtHR and the English judiciary view parents as guardians of their children's privacy rather than as privacy threats. In the sharenting context it is problematic that children's privacy expectations are inextricably bound up with their parent's expectations for the child's privacy. If children are to be able to effectively use existing remedies, such as the MOPI tort, to remove information which violates their privacy, English law may need to be reinterpreted to recognise that children have a right to privacy, 'independent from their parents' privacy expectations'.[188] In a similar vein, the law needs to recognise that children have a right to privacy *against* their parents, although this may perhaps need to be qualified according to the child's age and capacity.[189]

Undoubtedly, sharenting raises difficult issues for the courts for a host of reasons. The idea that the family should be left to govern itself, free from state interference, save where interference is necessary to protect vulnerable family members, is a principle that has long underpinned English law. It is a principle that is recognised both in the ECHR and the UNCRC. In the sharenting context, however, it is not clear when a parent's right to determine how their family's information is used gives way to the child's right to privacy. This is a particularly difficult issue when the information that a parent wishes to share relates to both their child's experiences and the parent's experiences as a parent and arguably belongs to both of them. When the information relates to activities that the child has enjoyed, with others, in public, one can perhaps understand why some parents might consider it legitimate to share that information, which will already be known to many. Parents do, however, seem to be

divided about whether and when sharenting is acceptable. For a court applying a 'reasonable expectation of privacy' test this is problematic.

Undoubtedly the advent of widespread use of the internet, and social media, poses challenges not just for the courts, but for data protection authorities also. The ICO has made clear that it will not consider complaints about posts made on social media. This is understandable – consider the number of complaints it might otherwise face. It means, however, that currently the DPA is largely ineffective at providing redress when anyone's information is published online without their consent, and in breach of the data protection principles, unless they have the money to go to court, and can demonstrate that processing has caused them substantial damage or distress.

Whilst the revised right to be forgotten offers some hope for the future, ultimately, the best way to ensure that parents rights and children's rights are both respected appears to be to promote wider debate about the issue, ensure that parents and children are fully informed of the rights that are afforded to them, and encourage dialogue between parents and children at an early stage.

Claire Bessant
Associate Professor, School of Law
Northumbria University

Notes

1 House of Lords Select Committee on Communications 2nd report of 2016-7 'Growing up with the internet' HL Paper 31 [206], Written evidence from Horizon Digital Economy Research, University of Nottingham.
2 42% of UK parents admit to regularly sharenting, 56% of UK parents never blog or post photos or videos of their children online, and they choose not to sharent because they consider their children's lives should remain private (OFCOM, The Communications Market Report 2017 https://www.ofcom.org.uk/research-and-data/multi-sector-research/cmr/cmr-2017, 35).
3 Megan Rose, 'The average parent shares almost 1,500 images of their child online before their 5th birthday'. http://parentzone.org.uk/article/average-parent-shares-almost-1500-images-their-child-online-their-5th-birthday
4 Top 10 Collins Words of the Year 2016 https://www.collinsdictionary.com/word-lovers-blog/new/top-10-collins-words-of-the-year-2016,323,HCB.html.
5 Tawfiq Ammari, Priya Kumar, Cliff Lampe and Sarita Schoenebeck, 'Managing Children's Online Identities: How Parents Decide What to Disclose About their Children Online' in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems,* April 18-23, 2015, 1895-1904, 1896.
6 Stacey Steinberg, 'Sharenting: Children's Privacy in the Age of Social Media' (2017) 66 Emory LJ 839, 842.
7 Article 8 General Data Protection Regulation (GDPR) authorises parents to provide consent to the use of information society services in cases where the child is deemed too young to do so themselves.
8 *Reklos and Davourlis v Greece* [2009] EMLR 16; *Bogomolova v Russia* (App No 13812/09) judgment 20 June 2017.
9 See *Weller v Associated Newspapers* [2015] EWCA Civ 1176; *AAA (by her litigation friend) v Associated Newspapers Limited* [2013] EWCA Civ 554; *Murray v Big Pictures (UK) Limited* [2008] EWCA Civ 446.
10 See Justin Huggler, 'Austrian teenager sues parents for 'violating privacy' with childhood Facebook pictures', *The Telegraph*, 14 September 2016 http://www.telegraph.co.uk/news/2016/09/14/austrian-teenager-sues-parents-for-violating-privacy-with-child/; Shehab Kahn 'Austrian teenager sues parents for posting embarrassing childhood pictures on Facebook,' The Independent, 14 September 2016 http://www.independent.co.uk/news/world/europe/teenager-sues-parents-over-embarrassing-childhood-pictures-on-facebook-austria-a7307561.html; Ashley May '18-year-old sues parents for posting baby pictures on Facebook,' USA Today, 16 September 2016; Unattributed 'Austrian teenager sues parents for putting her baby photos on Facebook,' 16 September 2016. http://www.itv.com/news/2016-09-15/austrian-teenager-sues-parents-for-putting-her-baby-photos-on-facebook/
11 Unattributed 'Story of Austrian teen suing parents over Facebook pictures debunked' 19 September 2016 http://www.dw.com/en/story-of-austrian-teen-suing-parents-over-facebook-pictures-debunked/a-19562265.
12 Ammari et al (n 5), 1895, 1897; Steinberg, (n 6), 852.
13 Priya Kumar and Sarita Schoenebeck, 'The Modern Day Baby Book: Enacting Good Mothering and Stewarding Privacy on Facebook' in *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (ACM, 2015), 1302-1312, 1302.
14 AVG Technologies (2010) 'AVG Digital Diaries – Digital Birth' http://www.avgdigitaldiaries.com/tagged/stage_one
15 More than 4 million parents in the United States read or write blogs, whilst in the UK Britmums maintains a network of more than 15,000 blogs: Alicia Blum-Ross and Sonia Livingstone, '"Sharenting," parent blogging and the boundaries of the digital self' (2017) *Popular Communication* 15(2) 110-125, 112).
16 Ibid.
17 Marion Oswald, Helen Ryan, Emma Nottingham, Rachael Hendry and Sophie Woodman, 'Have "Generation Tagged" Lost Their Privacy: A report on the consultation workshop to discuss the legislative, regulatory and ethical framework surrounding the depiction of young children on digital, online and broadcast media', (2017) 25.
18 Steinberg (n 6), 850; Nominet, 'Parents "oversharing" family photos online but lack basic privacy know-how' https://www.nominet.uk/parents-oversharing-family-photos-online-lack-basic-privacy-know/.
19 Steinberg (n 6), 846.
20 Maeve Duggan, Amanda Lenhart, Cliff Lampe and Nicole Ellison, 'Parents and Social Media' (Pew Research Center, 2015), 3; Kumar and Schoenebeck (n 13), 1302.
21 Duggan et al, ibid, 4; CS Mott Children's Hospital National Poll on Children's Health 'Parents on Social Media: Likes and Dislikes of Sharenting (2015) 23 (2); Kumar and Schoenebeck (n 13), 1302 and 1304.
22 Kumar and Schoenebeck (n 13), 1302.
23 Kate Orton-Johnson, 'Mummy blogs and Representations of Motherhood: "Bad mummies" and their Readers' (2017) *Social*

Media & Society 3(2) 1-10, 2
24 Steinberg (n 6), 852; Kumar and Schoenebeck (n 13), 1304; Orton-Johnson (n 23), 2.
25 Blum-Ross and Livingstone (n 15), 113.
26 Steinberg (n 6), 855.
27 Blum-Ross and Livingstone (n 15), 116.
28 Steinberg (n 6), 855 (Whilst this may be true, there is a potential problem with this viewpoint; the parent's portrayal of the child may not represent who the child is, or how they want to portray themselves).
29 Steinberg (n 6), 844.
30 CBBC Newsround, 'Sharenting: Are you ok with what your parents post?' http://www.bbc.co.uk/newsround/38841469.
31 Muge Marasli, Er Suhendan, Nergis Hazal Yilmazturk and Figen Cok, 'Parents' shares on Social Networking Sites About the Children: Sharenting' (2016) *Anthropologist* 24(2) 399, 400.
32 CS Mott, Children's Hospital National Poll on Children's Health 'Parents on Social Media: Likes and Dislikes of Sharenting (2015) 23 (2).
33 Ofcom, Communications Market Report 2017, 35.
34 Orton-Johnson (n 23) 2.
35 Ibid, 5 quoting Jessica Gottlieb, 'You're kind of a bitch of a mom blogger' http://jessicagottlieb.com/2015/03/bitch-mom-blogger/.
36 Steinberg (n 6), 852.
37 Family Online Safety Institute (2015) 'Parents, Privacy & Technology Use,' 22.
38 Clint Davis 'YouTube star DaddyOFive loses custody of kids after complaints over 'prank' videos' 2 May 2017 http://www.newschannel5.com/news/national/youtube-star-daddyofive-loses-custody-of-kids-after-complaints-over-prank-videos.
39 Steinberg (n 6), 853-4; Lisa Belkin 'Humiliating children in Public: A New Parenting Trend? https://www.huffingtonpost.com/lisa-belkin/humiliating-children-to-teach-them-_b_1435315.html accessed 11.10.17; Valentin and Blackstock Psychology 'The Dark Side of Public Shaming Parenting' 16.6.2015 http://www.vbpsychology.com/the-dark-side-of-public-shaming-parenting/.
40 Blum-Ross and Livingstone (n 15), 110.
41 Ammari et al, (n 5), 1896; Oswald et al (n 17), 13.
42 BlogHer, 'So I Posted Photos of My Kid Online and This is Where They Ended Up' 14 February 2013 (no longer accessible) cited by Steinberg (n 6), 847.
43 Kelli Bender, 'Mother of 2-year-old with rare disorder speaks out after internet memes make fun of her daughter' http://people.com/celebrity/mother-fights-cyberbullying-of-toddler-with-rare-disorder/; Terri Parker (2013), Mean moms bash 'ugly' toddlers in secret Facebook group http://www.wpbf.com/article/mean-moms-bash-ugly-toddlers-in-secret-facebook-group/1319522
44 Article 12, Universal Declaration of Human Rights (UDHR) and Article 16 United Nations Convention on the Rights of the Child (UNCRC).
45 Article 8, European Convention for the Protection of Human and Rights (ECHR); Article 7 Charter of Fundamental Rights of the European Union (EU Charter).
46 Article 8, EU Charter.
47 Article 8, UNCRC.
48 The focus of this article is the removal of images from the primary source, where it has been posted by the parent although it is recognised that third parties may subsequently share images shared by parents on social media and it may not be possible for a child to remove all information/images from the internet.
49 In addition to the three main remedies discussed below, where the publication of information has caused or is likely to cause serious harm to their reputation, a child might consider using the Defamation Act 2013. The Protection from Harassment Act 1997 also enables a child to seek an injunction restraining their parent from pursuing any conduct which amounts to harassment.
50 *Prince Albert v Strange* (1849) 1 Mac.& G 25.
51 *McKennitt v Ash and others* [2006] EWCA Civ 171.
52 *W v Egdell* (1990) 2 WLR 491.
53 Rebecca Moosavian, 'Charting the Journey from Confidence to the New Methodology'(2012) 34(5) EIPR 324-335, 326; *OBG v Allan; Douglas v Hello!; Mainstream Properties v Young* [2007] UKHL 21; [2007] 4 All ER 545 [255] (Lord Nicholls of Birkenhead).
54 Moosavian, Ibid; *Campbell v MGN* [2004] UKHL 22 [14]; *OBG v Allan; Douglas v Hello!; Mainstream Properties v Young* (n 69) [251].
55 Colin Bennett, *Regulating privacy: Data protection and public policy in Europe and the United States* (Cornell University Press, 1992), 14.
56 Alan Westin, *Privacy and Freedom* (Atheneum, 1967) 7.
57 Civil Procedure Rules 1998, r 21.2.
58 In the medical context s 8(1) Family Law Reform Act 1969 confirms the right of a 16-year-old to consent to medical treatment. Under-16s must prove they have 'sufficient understanding' (*Gillick v West Norfolk and Wisbech AHA* [1985] 3 WLR 830). In the data protection context, a child must demonstrate they are 'mature enough to understand their rights,' are able to broadly understand the process involved, and are able to interpret the information they receive. See ICO, 'Find out how to request your personal information' https://ico.org.uk/for-the-public/personal-information/ Note however that in Scotland a child of twelve years of age or more is *presumed* to be of sufficient age and maturity to have a general understanding of what it means to exercise the rights afforded by the DPA (s 66 DPA).
59 *Coco v A N Clark (Engineers) Limited* [1969] FSR 415, 419.
60 *Attorney General v Observer Ltd and others; Attorney General v Times Newspapers Ltd and anor (Spycatcher)* (1990) 1 AC 109, [281H-282A]); *Terry (previously referred to as LNS) v Persons Unknown* [2010] EWHC 119 (QB) [49] (Tugendhat J).
61 *Vestergaard Frandsen A/A (now MVF 3 ApS) v Bestnet Europe Ltd and others* [2013] UKSC 31 [23] (Lord Neuberger).
62 *Spycatcher* (n 60) 282C-F (Goff LJ).
63 *W v Egdell* [1990] Ch 359.
64 *McKennitt v Ash and ors* [2006] EWCA Civ 1714 [22] (Buxton LJ).
65 *Saltman Engineering Co Ltd v Campbell Engineering Co Ltd* (1948) 65 RPC 203, 215.
66 [1977] WLR 760, 763.
67 *McKennitt v Ash* (n 64) [33] and [36].
68 [2010] EWCA Civ 908, [66] Note in *Google v Vidal-Hall* [2015] EWCA Civ 311 [25] (referring to the comments of Lord Nicholls in *Campbell* (n 54)) it is similarly suggested that 'there are problems with an analysis which fails to distinguish between a breach of confidentiality and an infringement of privacy rights protected by article 8, not least because the concepts of confidence and privacy are not the same and protect different interests.'
69 This is the first test to be satisfied where a claim is brought under the MOPI tort, discussed further below.
70 [2010] EWCA Civ 908, [66].
71 *Campbell* (n 54), [154] (Lady Justice Hale).
72 In *Weller* (n 9) Lord Dyson emphasised that the children were enjoying a 'private family outing,' an activity distinctively different in nature to a mere trip to the shops or walk along the street.
73 [2015] UKSC 42.
74 *In Re JR 38* [2015] UKSC 42 [100].
75 *Spycatcher* (n 60)), 281D-F.
76 *Coco v A N Clark* (n 59), 420.
77 *Campbell* (n 54) [85] (Lord Hope), supported also by Lady Hale and Lord Carswell in *Campbell* at [134] and [165] respectively.
78 *Napier and Irwin Mitchell v Pressdram Ltd* [2009] EWCA Civ 443 (CA) [42] (Toulson LJ).
79 Blum-Ross and Livingstone (n 15), 111; Alicia Blum-Ross 'Sharenting: Parental Bloggers and managing children's digital footprints' http://blogs.lse.ac.uk/

parenting4digitalfuture/2015/06/17/managing-your-childs-digital-footprint-and-or-parent-bloggers-ahead-of-brit-mums-on-the-20th-of-june/.

80 *McKennitt v Ash* (n 64).
81 *McKennitt v Ash,* ibid [32, 36].
82 *McKennitt v Ash*, ibid [36].
83 *Terry (previously referred to as LNS)* (n 60), 50 (Tugendhat J).
84 *HRH Prince of Wales v Associated Newspapers Ltd* [2006] EWCA Civ 1776 [68] (Lord Phillips).
85 *Spycatcher* (n 60) 282C-F.
86 [2011] EWHC 1232.
87 *Ibid* [27].
88 *Giggs, Ibid* [28] See also *Douglas v Hello (No 6)* [2005] EWCA Civ 595; [2006] QB 125 [55]; *HRH Prince of Wales v Associated Newspapers Ltd* [2006] EWCA Civ 1776; *Browne v Associated Newspapers Ltd* [2008] QB 103 [61]
89 Max Mills 'Sharing Privately: the effect publication on social media has on expectations of privacy' (2017) JML 9(1) 45-71, 52 citing *Stephens v Avery* [1998] 1 Ch 454.
90 *Stephens v Avery* [1998] 1 Ch 454.
91 Mills (n 85), 53.
92 Nicole Moreham and Sir Mark Warby (eds), *Tugendhat and Christie: The Law of Privacy and the Media (* 3rd edn, 2016), 10.
93 See for example comments of Lord Neuberger in *Tchenguiz v Immerman* [2010] EWCA Civ 908, [66].
94 *Google Inc v Vidal Hall and ors* [2015] EWCA Civ 311 [25] referring to the comments of Lord Nicholls in *Campbell* (n 54).
95 *Google Inc v Vidal-Hall,* ibid [25] citing Lord Hoffman in *Campbell v MGN* [51].
96 *Campbell* (n 54) [14].
97 *PJS v NJN* [2016] UKSC 26 [32],[36[; see also *Contostavlos v (1) Michael Mendahun (2) any person in possession or control of material referred to in sch 2 of the order of Mr Justice Tugendhat dated 20 March 2012 (3) Justin Edwards* [2012] EWHC 850 (QB) [105].
98 *PJS* (n 114) [32].
99 *Campbell* (n 54).
100 *Weller* (n 9).
101 *Campbell*, (n 54) [99] Lord Hope.
102 *Murray* (n 9) [36] per Sir Anthony Clarke MR.
103 *Weller* (n 9).
104 *Weller* (n 9) [56-64].
105 Murray (n 9) [45] and [56], *Re JR 38* [2015] UKSC 42; and the cases of *K v News Group Newspapers Ltd [2011] EWCA Civ 439 and PJS v NJN* [2016] UKSC 26.
106 *Weller* (n 9) [29]; see also Murray (n 9) [57].
107 Moreham and Warby (n 109), 49.
108 Wouter Martinus Petrus Steijn, 'The role of Informational Norms on Social Network Sites' 117-37 in Walrave M, Ponnet K, Vanderhoven E, Haers J, Segaert B (eds) Youth 2.0: Social Media and Adolescence (Springer, 2016), 118-9.
109 Steijn, ibid, 119.
110 Alex Preston, 'The Death of Privacy,' *The Observer*, 3 August 2014 https://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston; Jo Glanville, 'Privacy is Dead! Long live privacy' (Sage Publications, 2011); Bobbie Johnson, 'Privacy no longer a social norm, says Facebook founder,' *The Guardian*, 11 January 2010. https://www.theguardian.com/technology/2010/jan/11/facebook-privacy ; Business Wire, 'Digital Birth: Welcome to the Online World' http://www.businesswire.com/news/home/20101006006722/en/Digital-Birth-Online-World.
111 Leo Kelion, 'Posting children's photos on social media divides nation' BBC, 3 August 2017 http://www.bbc.co.uk/news/technology-40804041.
112 Steijn (n 108), 130.
113 (App No 1234/05) [2009] EMLR 16 [40].
114 (App No 13812/09) judgment 20 June 2017 [52].
115 Reklos (n 8) [43].
116 Reklos (n 8) [41]
117 Kirsty Hughes, 'The Child's Right to Privacy and Article 8 European Convention on Human Rights' in Michael Freeman (ed) (2012) 14 *Law and Childhood Studies* (Oxford University Press, 2012) 456-86, 479.
118 *Weller* (n 9) [33].
119 *AAA* (n 9)*,* [21].
120 *Murray* (n 9)*,* [37-38].
121 Oswald et al (n 17), 10.
122 See Hughes (n 117), 480; also Kirsty Hughes, 'Publishing photographs without consent' (2014) 6(2) JML 180, 185.
123 Hughes (n 117), 480.
124 Murray (n 9) [16].
125 For further discussion see Oswald et al (n 17), 10.
126 Hughes (n 117), 480.
127 *In re S (A child)* [2004] UKHL 47; [2005] 1 AC 593 [17] per Lord Steyn.
128 Section 1(1) Children Act 1989.
129 *Weller* (n 9) [40-41].
130 Marion Oswald, Helen James & Emma Nottingham, 'The not-so secret life of five-year-olds: legal and ethical issues relating to disclosure of information and the depiction of children on broadcast and social media',(2016) JML 8(2) 198-228, 216 referring to *In Re S (a child) (Identification: Restrictions on Publication)* (n 118); *In Re W (Identification: Restrictions on Publication)* [2006] EWHC 2733 (Fam); *In Re M and N (Minors) (Wardship: Publication of Information)* [1990] Fam 211; *Re Steadman* [2009] EWHC 935 (Fam).
131 *Weller* (n 9) [64].
132 *ETK v Newsgroup Newspapers* [2011] EWCA Civ 439 [17]; *PJS v Newsgroup Newspapers Ltd* (n 92) [44] (Lord Mance); *Rocknroll v News Group Newspapers* [2013] EWHC 24 (Ch) [36-37], [39]. In *PJS* [72] LJ Hale makes clear that such an approach is justified as much by concern for the privacy interests of the children as for the family privacy and the privacy of the parents.
133 See Jacob Rowbottom, ''To rant, vent and converse: Protecting low level digital speech' (2012) *Cambridge Law Journal* 355, 356 for definitions of low and high value and low and high level speech.
134 See *Re J (a child) (contra mundum* injunction*)* [2013] EWHC 2694 (Fam); *In the matter of an application by Gloucestershire County Council for the committal to prison of Matthew John Newman* [2014] EWHC 3136 (Fam); also *Clayton v Clayton* [2006] EWCA Civ 878.
135 *Re J,* ibid, [76(v)].
136 In this regard consider the facts of *Re J,* ibid.
137 [2000] 2 FLR 512*,* 531.
138 *Maumousseau and Washington v France* (App No 39388/05) *(unreported) 6 December 2007, ECtHR* [68]; *Neulinger and Shuruk v Switzerland* (App No 41615/07) *[2011] 1 FLR 122* [134].
139 *Re R and H v United Kingdom* (Application No 35348/06) *[2011] 2 FLR 1236* [73].
140 Hughes (n 117), 456.
141 Oswald, James & Nottingham (n 130), 211.
142 Maxine Wolfe and Robert S Laufer, 'The Concept of Privacy in Childhood and Adolescence' in D H Carson (ed) *Man-Environment Interactions: Evaluations and Applications* (Dowden, Hutchinson & Ross, 1975).
143 Karyn D McKinney, 'Space Body and Mind: Parental Perceptions of Children's Privacy Needs' (1998) Journal Fam Iss 19(1) 75, 76.
144 Hughes (n 117), 458-9.
145 *Google v Vidal-Hall and others* [2014] EWHC 13 [78].
146 ECJ C101/01 [27].
147 This argument was made by a 16 year old in respect of photographs taken when she was 12 (Kaye Wiggins 'Should children ban their parents from social media?' http://www.bbc.co.uk/news/business-37834856).

148 Section 2, DPA.
149 Schedule 2, DPA, para 1.
150 Schedule 2, DPA, para 6(1).
151 Schedule 3, DPA, para 1.
152 Schedule 3, DPA, para 5.
153 Section 42, DPA.
154 Section 40, DPA.
155 Section 10(1), DPA.
156 [2015] EWCA Civ 311 [77-79].
157 Section 10(3), DPA.
158 Directive, Article 3(2).
159 ECJ C101/01 [27].
160 Composed of representatives from each of the data protection authorities across the European Union.
161 Article 29 Data Protection Working Party (2009), 'Opinion 5/2009 on online social networking' 00189/09/EN WP 163, adopted 12 June 2009.
162 David Erdos, 'Beyond 'Having a Domestic'? Regulatory Interpretation of European Data Protection Law and Individual Publication' University of Cambridge Faculty of Law Research Paper No. 54/2016 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2847628 3; Douwe Korff, (2010) 'Comparative Study on Different Approaches to new privacy challenges, in particular in the light of technological developments, Working paper no 2: Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments', 9
163 ICO (2014) 'Social networking and online forums – when does the DPA apply?' V1.1, 4.
164 Ibid, 9
165 Ibid, 15
166 European Commission 'Press Release: Agreement on Commission's EU Data Protection Reform will boost Single Digital Market, Brussels, December 2015 http://europa.eu/rapid/press-release_IP-15-6321_en.htm.
167 Article 8 GDPR specifies that consent to processing of children's data on 'information society services', will be lawful only if the child's parents consent or the child is of sufficient age to do so themselves. The GDPR sets a maximum age of 16 but permits states to authorise a child to consent at a lower age of 13, and the data protection bill currently before parliament confirms that in the UK a child may consent if aged 13 or over.
168 Oswald, James and Nottingham (n 130), 209.
169 Steinberg (n 6), 881.
170 Article 17 GDPR.
171 The Queen's Speech and Associated Background Briefing, on the Occasion of the Opening of Parliament on Wednesday 21 June 2017https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/620838/Queens_speech_2017_background_notes.pdf, 79.
172 Letter dated 19/10/2017 from Lord Ashton of Hyde and Baroness Williams of Trafford to Peers regarding issues raised during the Second Reading of the Data Protection Bill http://data.parliament.uk/DepositedPapers/Files/DEP2017-0603/Letter_on_Data_Protection_Bill_from_Lord_Ashton_and_Baroness_Williams.pdf.
173 Department for Digital, Culture, Media and Sport A New Data Protection Bill: Our Planned Reforms 7 August 2017 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/635900/2017-08-07_DP_Bill_-_Statement_of_Intent.pdf , 8.
174 Communication Tackling illegal content online https://ec.europa.eu/digital-single-market/en/illegal-content-online-platforms#Communication on tackling illegal content online.
175 https://www.facebook.com/communitystandards/ NB however that the article by Nick Hopkins 'Revealed: Facebook's internal rulebook on sex, terrorism and violence' The Guardian 21 May 2017 https://www.theguardian.com/news/2017/may/21/revealed-facebook-internal-rulebook-sex-terrorism-violence suggests removal of such hateful, hurtful or violent content is by no means guaranteed.
176 https://www.facebook.com/help/428478523862899 accessed 9.10.17.
177 Sonia Livingston, John Carr and Jasmina Byrne, 'One in Three: Internet Governance and Children's Rights' Global Commission on Internet Governance' (2015), 13-14.
178 Oswald et al (n 17), 6-7.
179 Benjamin Shmueli and Ayelet Blecher-Prigat, 'Privacy for Children' (2011) 42 Colum Hum Rts L Rev 759, 793-5.
180 Oswald et al (n 17), 30.
181 Geraldine Bedell, 'The Digital Family', Parentzone (2015) 16 https://parentzone.org.uk/system/files/attachments/DF%20Report_FINAL2016_0.pdf.
182 Ammari et al (n 5), 1900.
183 Steinberg (n 6), 877-82.
184 Oswald et al (n 17), 30.
185 'Gendarmerie nationale '[PREVENTION: Preserver vos enfants!' (Prevention: Protect your Children!) 23 February 2015 https://www.facebook.com/gendarmerienationale/posts/1046288785435316; Polizei Nordrhein-Westfalen (NRW) Hagen 13 October 2015 https://www.facebook.com/Polizei.NRW.HA/posts/474114729427503:0.
186 Information Commissioner's Office, 'Taking photographs in schools' (2014).
187 Children's Commissioner, 'Our Work: Digital' https://www.childrenscommissioner.gov.uk/our-work/digital/.
188 Oswald et al (n 17), 5.
189 Shmueli and Blecher-Prigat (n 169), 763.

Are children more than 'clickbait' in the 21st century?

Baroness Beeban Kidron

This article considers the rights and privileges of childhood, and about how we might start to redress the imbalance of power between tech and children in the digital environment. It begins with the concept of childhood.

Childhood is the word we use to describe the journey from dependence to autonomy, from infancy to maturity. Whilst different individual children – and different personal, social and economic circumstances – impact hugely on that journey, we have, over time, established an understanding of this transition in terms of childhood norms and childhood needs, that academics call 'childhood development milestones'.

A development milestone is an age, or more commonly, an age range, by which certain maturities and understandings are likely to be achieved – and conversely, an age or age range when certain maturities and understandings are 'unlikely' or 'not supposed to be' in place. So, whilst a child at 3-5 years is beginning to understand that others feel and experience life differently to them, they are not yet able critically to evaluate that information and will take what they are told at face value. It is not until between their 13th and 15th birthday that a child will develop a heightened sensitivity to risk; at that age some will embrace risk and others will shrink from it, but until then they are unlikely to anticipate or see it. Our understanding of the physical, neurological and emotional changes that take place during childhood has shaped society's response.

Although we take the view that parents and those with parental responsibility for children offer the first line of both care for and defence of children, we have also concluded that children by virtue of their age, and the vulnerabilities associated with that age, require a broader set of inputs, privileges and protections beyond that offered by their immediate families. These inputs include a complex but widely understood – and respected – set of social norms, educational frameworks, advisory bodies, regulatory interventions, and national and international laws.

Perhaps the most recognised expression of our common understanding of the rights and privileges of childhood is the UN Charter on the Rights of the Child (UNCRC). It is the most ratified treaty in the world, with 196 signatories. A glaring exception is the country host to the major tech companies, but nonetheless the UNCRC serves as a codified description of what we collectively believe is necessary to ensure a safe and secure environment for childhood.

In addition to the UNCRC, we design and mitigate for childhood in multiple ways across all aspects of our society. We educate, we consider paediatric medicine to be a distinct specialism and require doctors to obtain additional skills and expertise; we don't criminalise young children, and impose a public interest test on the Crown Prosecution Service when

considering prosecuting older children; we don't allow adults to hold children to contractual obligations; we put pedestrian crossings near schools; we rate films according to the developmental stages of childhood; children have special protections around sexual activity; and we make it illegal for children to smoke, drink and gamble and even take steps to protect them in environments where adults smoke, drink and gamble.

In short, the overriding understanding is that society must, above any other consideration, act in the 'best interests' of a child. This reflects a global consensus that the capacity of a child to understand and act is necessarily limited by vulnerabilities and immaturities associated with their age.

The digital environment

Yet the digital environment does not reflect this consensus. Several years ago, I interviewed a number of people credited with inventing the World Wide Web for a film project. Repeatedly they described the original vision as a democratising technology where gatekeepers would be banished and all users would be treated equally.

In the middle of an interview with Nick Negroponte, founder of the MIT Media Lab, I had one of those 'moments' that change how you see things. I realised there was a category error, because however good it first sounds, if you treat everyone equally then *de facto* you treat a child as if they are an adult. And a child is a child until they reach maturity – not until they reach for their smartphone**.**

Perhaps even more important than the category error that I identified was that other promise – to get rid of the gatekeepers. The founders' utopian vision – a network of open-source small holders with a chain of active participant users – had been rapidly replaced by a handful of powerful platforms that quickly made the digital environment more powerful, less responsive, more autocratic and less accountable than the gatekeepers they had promised to replace. It made a handful of young, privileged men (mainly young, mainly privileged, and mainly men) insanely rich and insanely powerful on a global scale, with no balancing oversight or societal responsibilities. This is something that governments, international institutions, and several increasingly unhappy 'inventors and founders' are only now beginning to understand.

It is in the DNA of Silicon Valley, as famously articulated by Mark Zuckerberg, to 'move fast and break things' – but in this breathless journey to innovate, communicate, and of course make money, the young, privileged men I refer to have not properly considered that some of the things they might break are our children. In creating an environment that does not consider the needs of child users they have rejected hugely precious cultural, social and legal norms of childhood.

Perhaps at first unconsciously, but for the last 10 years at least wittingly, they have allowed a denigration of the hard-won privileges and protections that a century and a half of careful consideration, research and law-making across the globe has afforded our children. In doing so the status of children, and childhood, has been changed in the plain sight of parents, media, civil society and governments.

I would like to kill the myth of children as 'digital natives' – a term which implies that they have grown up in some exotic land which they alone understand and embrace in a manner that we adults never will. If we accept that analysis we become foot soldiers for Silicon Valley's army of lobbyists who would have us believe that the 'kids are ahead of the game'. They most definitely are not.

As the longitudinal study, EU Kids Online, consistently shows, children remain on the lowest ladder of digital opportunity because they spend the most time on a few highly commercial sites and have the least critical understanding and facility to understand, organise or use the information they are presented with online. As an eminent child psychologist wrote: 'Using technology with two fast thumbs cannot, in itself, be taken as evidence that a child is a creative participant in the digital environment with full literacy, citizenship and agency.' In plain language this means that just because you can access technology, it doesn't mean that you understand or control it!

I would particularly like to draw attention to the concept of 'agency' to which the psychologist refers. A child that has 'agency' has the ability to make choices based on information that has been provided in a way they can understand, and in conditions in which that choice is meaningful.

With that in mind I would like to repeat a conversation I had recently with the Managing Director of IT at a major technology company, who described the 'bundle' of technological methods currently used to capture and hold our attention on the tubing, gaming and social media platforms where children

spend so much of their time. This bundle is referred to as *captology*. It is its own science; the science of capturing a person's attention and keeping them in 'rapture', which can include:

- soft rhythmic sounds or music to block out real life;
- sharp, narrative sounds to pull user attention to what is happening on screen;
- bright, intense light that vibrates intermittently at high speed;
- cycles of intense activity followed by a slow end – like changing an avatar, or responding to a message, or being congratulated – only to be interrupted by something fast and even more intense to drag the user back just as they are ready to quit (this, she explained, is because if you think you are getting off, but come back at the last minute, you will stay longer than if you are attached for a single exhausting session at the same pace);
- vibrating devices;
- confirmation signals from peers – the heart/like/share buttons;
- random confirmations – from algorithms that feel your waning activity;
- personal streaks – not breaking a 'run' irrespective of any intrinsic value in the exchange;
- community streaks – not breaking a 'run' with someone else so that you are not guilty or embarrassed, irrespective of your desire to be in contact with that person;
- attracting your attention with a key word or image that you have just used in another setting;
- attracting your attention with an extreme word or powerful image;
- attracting your attention by showing you that others in your circle are online, getting more attention, posting more, etc;
- the colour blue.

And this list, though exhausting, is not exhaustive!

Children's developmental capacity

A child, not yet fully-formed, does not have the developmental capacity to resist one or another or a combination of these pulls. The algorithms follow their behaviour on such tight loops that they can, in real time, provide the 'exact' personalised mix to keep them clicking. So, if one child is more responsive to image and confirmation from peers but another responds to sharp sounds and being set challenges, each will get the loop of events that will most entice them to their own 'personalised' state of rapture.

These techniques are digital norms that I'm sure we all recognise from our own experience, but they are especially potent when deployed against children whose brains are still being moulded, and whose critical thinking has yet to mature. Most importantly, they *deliberately* orchestrate a context in which a child cannot make a meaningful choice whether or not to engage with their digital environment – ie to exercise their right to agency. They are in the digital sweetshop, which most certainly has its pleasures and positive outcomes, but it does not provide a balanced diet. Being stuck there in a state of 'rapture' is not in the 'best interests' of the child.

Research carried out in the US by Common Sense Media in 2016 found that 70 per cent of teenagers argued with their parents about their devices, with 32 per cent saying devices caused arguments on a daily basis.[1] Research conducted across different childhood age groups and multiple locations reflected a similar pattern, and in 2017 tech-related conflict was widely reported as the top cause of familial discord in the UK.

I have spent my whole life working in media, and have set up organisations that encourage young people to watch films online. I regularly co-create technology with children, and I am a strong advocate for the rights of children to access the digital environment. But I see an increasing tension between a technology that has a singular power to redress some of the world's greatest challenges and inequities, and a corporate culture that aggressively rejects its societal responsibilities to the communities in which it operates and to the people which it so successfully commoditises.

I am not alone. Jaron Lanier, inventor of virtual reality; Sean Parker, the co-founder of Facebook; Sir Tim Berners-Lee, inventor of the web; and Justin Rosenstein, the designer of Facebook's 'Like' button, have in various recent public pronouncements

decried the problematic use of technology against its users. Jaron Lanier accused tech of having gone over a threshold into behaviourist scientific experiments in which behaviour is provoked by stimuli that can guarantee changed human behaviours, and that the wellbeing of the nation (by which he meant America) depends on stopping it. He called for a new culture, in which users have 'dignity and autonomy'.

I believe that not just the wellbeing of America is at stake, but the wellbeing of children the world over. Whether a child loves cartoons, football, fashion, music or comedy, or whether they are a gamer, a tuber or a social media junkie or simply interested in the news, online services will deploy the full power of their data-churning algorithms to ensure that a child is perpetually bombarded with a bespoke recipe of emotional and technological pulls. Designed by engineers, delivered by robots, in an environment where neither the engineers nor the robots have any responsibility for the consequences, these 'bespoke', or should I say 'personalised', recipes are designed to keep a child clicking for as long as possible.

The consequences of this were highlighted recently when it was revealed that machine-learning algorithms that generate content for YouTube Kids, which are based on popular trends and key word searches, resulted in thousands of deeply creepy, sometimes violent, videos being watched by hundreds of thousands of very young children. These videos do not reflect the social norms of childhood, yet no one stepped in to temper the consequences of algorithms deciding what our children watch. When YouTube finally responded, they announced they would restrict these videos once reported. This is a solution that relies on pre-schoolers policing content. Where children are the end user, surely we need better oversight than that?

Children year on year spend more and more time online – for a 12-15 year old in the UK it was 20 plus hours a week in 2016. But I share the opinion of Professor Sonia Livingstone that it is inadequate to look at how long children are online. What we should be looking at is *what they are doing online and what being online is doing to them*. Being online is not in, and of itself, bad, risky, unhealthy or negative in any other way.

However, commercial environments that are largely designed for adults, and demand significant levels of interaction and normalise the spread of personal information, are not great environments for children to spend the bulk of their time. These young people are entering contracts and giving away vast swathes of personal information, using services that do not take account of their age. They are emerging from the experience sleepless, anxious, and overexposed. It cannot be a good use of technology to allow its brightest and finest to ignore the needs of most vulnerable demographic in our society, and it is a failure for any government, international institution or legislative body not to do what it can to tackle these norms.

I want to make it clear that the answer is not to kick children out of the digital environment – on the contrary, every child should be allowed to access the digital environment creatively, knowledgeably and fearlessly. But the digital environment is a network of businesses that provides services to children, and those businesses need to be responsive to their presence. It was that simple principle that led me to found 5Rights to, in effect, deliver the rights of the UN Charter in online settings.

The rights and needs of minors

Over the last several years 5Rights has made many interventions and worked with many organisations, nationally and internationally. Our mission is to take every opportunity on all platforms supporting research, policy and the building of tech in order to make the case that although 21st century children always need access to the digital world, they need it on new and improved terms. Those terms must include their right to change their digital footprint and identity; to be safe and supported in online settings; to understand who, how and what their data is being used for; to be informed and creative participant digital citizens; and above all, to have 'agency' – meaningful choice in an environment that is responsive to, and respectful of, their full complement of rights and needs as minors.

I hope I have made my case that we have a problem. So, what is to be done about it? Self-regulation is a whole topic in itself, so here is my brief ABC:

A. *Silicon Valley is not very interested in children.* The real interest is in drones and driverless cars, conquering space and cryogenics, and operational leverage – specifically how robots can replace humans to provide a high gross margin, and naturally share price. The one third of all users that are children are an inconvenient truth for big tech, beautifully illustrated by the fact that they consistently refuse to collect and publish data on children's complaints or monitor under-age use of their services.

B. *There is both an explicit and implicit message from industry that we have to make children 'resilient' and inform them of risk*. Some businesses are doing excellent work in both these areas, but there is a great deal less appetite to design their services to make them fit for children. I see no world order in which the duty should rest on a child to adapt to the needs of tech, rather than on tech to adapt to the needs of childhood.

C. *Whenever we talk codes or conditions there is a unified response – that any form of conditionality would mean tech have to turn its back on young people, thereby throwing them off their platforms and services*. The response is based on the premise that the natural choice is between children using adult services or nothing. This is, at best, diversionary; nearly a billion current users are children, so should they be cast out then undoubtedly someone else will see the competitive advantage in developing services for them. But more insidious is Silicon Valley's corporate attitude to young people. It does seem that self-regulation is little more than leaving the fox in charge of the henhouse.

And just to be an unreliable commentator, my ABC has a D. This is no longer a new environment. At 27 years old, it is, unlike many of its users, fully adult and grown. Much like all the information technologies, all the industrial sectors, and all the global companies before them, tech is ready to take on and live up to its adult responsibilities. If you earn and own more than most nation states, your responsibilities – and allocating the resources to meet them – are self-evident. Equally self-evident is that year on year kids are having a harder and harder time online.

It really is time to bring this brave new world of tech into the real world of the 21st century, where every other business corporation, state and civil society actor – and indeed every human on the planet – lives, or fails to live, by a set of agreed standards upheld by regulation. What is needed is a global agreement that has at its heart some key provisions about the rights of users. Like others who take a close interest in this subject, I see a future where we will all be individual data providers, and commercial companies and other organisations will access us on terms and conditions that we set to reflect our limits, our tolerances and our interests. But returning to the present, it is important to dispel the double-myth inherent in the digital environment that it cannot reflect jurisdictions, and that it cannot be regulated. We have seen a number of push backs on several fronts and in many sectors.

Taking regulatory action

In Germany, a new law was introduced in 2017 that places an obligation on online services to remove obviously illegal hate speech within 24 hours, or face fines of up to €50 million. Cities all over the world have responded to digital services, such AirBnB and Uber, in a way that reflects local concerns and existing regulatory frameworks. The extensive provisions for Member State derogations in the GDPR anticipates not just the feasibility of, but the need for, bespoke, national solutions. The GDPR, imperfect as it is, provides proof that principles-based regulation, instigated in this case by the EU, can act as a global catalyst as companies roll the standards out worldwide.

The IT lead of one of the biggest pharmaceutical companies in the word recently said to me, and I paraphrase: 'Whilst the rules of the GDPR are perhaps a little opaque its intention is clear. So, we are working to the intention – because that is the right thing to do'. I, with the support of colleagues right across the political divide, tabled a set of amendments to the Data Protection Bill that established an 'age-appropriate design code' as a requirement for processing the data of children under 18.

The amendments, set out in detail in *Hansard* [2], represent a step towards a better digital future for children by:

- crucially, connecting design of services with the development needs of children – recognising that childhood is a graduated journey from dependence to autonomy;
- introducing a code that will set out the standards by which online services protect children's data;
- setting standards that are directly related to a child's age and the vulnerabilities associated with that age;
- clarifying the expectation on services to design data practices that put the 'best interests' of the child above any other consideration, including their own commercial interests;
- establishing the standards by which the Information Commissioner will judge services on behalf of child users.

Subsequent amendments deal with creating guidance on age-appropriate design and Parliamentary oversight. One small set of amendments to a data Bill in one country, on one specific part of a child's digital

life, is not a complete solution – but these amendments achieve a few key things in that they:

- separate a child's data from that of an adult;
- build on the industry norms of personalisation, and take existing technology and set it to work for the child user (as one boy said to me, 'how come if they know I like red Nikes they don't know I am 12?');
- meet the United Kingdom's current obligation to ensure that our national legislation is compatible with the GDPR, and safeguard our prospects of securing an adequacy agreement post-Brexit;
- enshrine the long-held view that the first duty of any government is to protect its citizens – and most importantly, those who are too vulnerable to protect themselves – and fulfil our duty of care to children.

Detailed guidelines are necessary in the future, but what the amendment I put forward asks the Information Commissioner to take into account are such matters as a child's need for high privacy settings by default; not revealing their GPS location; using their data only to enable them to use a service as they wish and no more; and not automatically excluding children if they will not give up vast swathes of data – however nicely they are asked.

If the Commissioner so wished, guidelines could also extend to giving a child time off by not sending endless notifications during school hours or sleep hours, and deactivating features designed to promote extended use; making commercially driven content, whether a vlogger or a direct marketing campaign, visible to and understood by a minor; and insisting on reporting processes with an end-point and a reasonable expectation of resolution.

None of the regulatory measures referred to above are beyond technology. They are not overbearing, do not hold back innovation, and do not discriminate between one set of data processors and another. They will, like the GDPR or accessible design, simply become industry standards – a price of doing business.

No system will ever protect all children at all times from risks and transgressions – accidental or intentional. But to start by acknowledging their special status as children in an environment – that is the environment in which their childhood plays out – can only be a good thing. In an industry dominated by data, children's data needs its own special consideration.

The world has just short of a billion children online. They have a right to be more than clickbait toiling in the fields of Silicon Valley. It is up to all of us to advocate for this right and to fulfil the founders' vision of a better digital world.

Baroness Beeban Kidron
The author is an award-winning film director, Crossbench member of the House of Lords, and a member of the House of Lords Communications Committee. She sits on the UN Broadband Commission for Sustainable Development and the Royal Foundation's Taskforce on the Prevention of Cyberbullying, and is the founder of 5Rights, a campaign which delivers the established rights of children in the digital environment.

Notes

1 https://www.commonsensemedia.org/sites/default/files/uploads/research/2016_csm_technology_addiction_executive_summary.pdf

2 Hansard, (HC) Vol 787, col 1427 (11 December 2017).

Interpreting the child-related provisions of the GDPR

Lisa Atkinson

My focus, both professionally and in this article, is on what the General Data Protection Regulation (GDPR) says about children's personal data, and the landscape that has led to those provisions. In 2015 the Global Privacy Enforcement Network, made up of data protection authorities from around the world, did a sweep of websites and apps that were targeted at, or popular with, children. Sweepers indicated that they would be uncomfortable with children using 41 per cent of the websites reviewed. Their concerns included:

- the over-collection of personal data;
- failure to use language that children could understand;
- disclosure of information to third parties for vague or unspecified reasons; and
- the facility for children to overshare personal data through unmonitored chat rooms.

On the positive side, they also commented that: 'One third of websites or apps that were swept demonstrated that they could be successful, appealing and dynamic without the need to collect any personal information at all.'

Interestingly, a 2013 report[1] which raised concerns about the misuse of children's personal information accounted for less than 3 per cent of the online risks that children themselves were worried about. But is that because there is nothing for them to worry about? Or because they haven't yet developed the critical reasoning abilities to know they need to worry? It is in this kind of context that the text of the General Data Protection Regulation was debated and agreed.

Recital 38 to the GDPR sets the overall tone for the treatment of children's personal data when it says that: 'Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.' It calls for particular care in the contexts of marketing and profiling, and when offering online services.

One of the provisions which have caused the most debate and consternation is the online consent requirement. Article 8 of the GDPR says that when consent is relied upon as the basis for processing personal data, only children over a certain age (to be decided at national level) will be able to provide their own consent. For anyone under that age of digital consent, consent from a holder of parental responsibility will have to be sought and verified.

The UK has provisionally set this age at 13, though the Parliamentary debate about this continues. It should be emphasised that article 8 is not a revolutionary new requirement. Under the Data Protection Act (DPA), data controllers who rely upon consent

are already required to make sure that that consent is 'freely given, specific and *informed'* [my emphasis]. The existing 'Guide to data protection' produced by the Information Commissioner's Office (ICO) is clear this means that consent must already be 'appropriate to the age and capacity of the individual and to the particular circumstances of the case.'

The 'new challenges' of article 8, are, in the ICO's view, just existing challenges that have been brought into sharper focus by the GDPR. What article 8 seeks to do is to give providers of online services to children some certainty in what is an existing grey area by providing a set age at which they can assume that children are competent to provide their own consent.

The GDPR also brings the requirement to have a lawful basis for processing 'up front and central'. Conditions for processing have always been a requirement under the DPA, but the GDPR states that controllers have to tell data subjects the lawful basis they are relying upon in their privacy notice before they start the processing.

This ties in neatly to the additional focus on Data Protection Impact Assessments, which the ICO regards as a vital tool in helping controllers to assess the risks of the processing of children's personal data, mitigate these risks, and ultimately, decide whether the processing can be justified and if so under which lawful basis. This is one of the ICO's key messages in relation to children's personal data. Controllers need to think about the children up front, when they are designing the processing, to make sure that they give them the specific protection they merit. Controllers also need to be clear what data is being processed under which lawful basis.

There are also more comprehensive transparency requirements in the GDPR. For children these requirements are clarified by the recital 58 statement that says 'any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand'. Again, the ICO considers that this brings into focus existing advice in our Privacy Notices Code of Practices. For example, we already say that data controllers need to draft privacy notices that are appropriate to the level of understanding of the audience being addressed and not exploit any lack of understanding. We already recommend the use of methods such as 'just in time notices', ICONS and clear preference settings.

The GDPR also brings in new provisions about profiling and automated decision-making, and there has been some debate about whether recital 38 amounts to a complete prohibition on automated decision-making based on the processing of children's personal data. The Article 29 Working Party has clarified that this is not the case in its recently published opinion on profiling, but the ICO believes great care is still needed in this area and controllers will really need to be able to justify what they are doing in this context, and in the context of marketing.

Finally, the right to erasure provision gives particular recognition to the rights of data subjects who gave their consent to processing as children, and now wish to have their data erased.

To sum up, the ICO welcomes the new focus on children's privacy that the GDPR brings to data controllers and to our own work and priorities. It is an opportunity to reflect and recalibrate. This can only be a good thing, and we await further developments and debate with interest

Lisa Atkinson
The author is a Group Manager in the Policy and Engagement Department of the Information Commissioner's Office. She is leading the ICO's work on interpreting the child-related provisions of the GDPR.

Notes

1 In their own words – what bothers kids online, report of a survey by EU Kids Online.

The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR

Simone van der Hof and Eva Lievens

1. Introduction

The General Data Protection Regulation that enters in to force on 25 May 2018 aims specifically to protect children and their personal data in the digital world. According to Recital 38, children 'may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data'. Although indeed a laudable and relevant measure, the GDPR demonstrates many questions as to what said protection entails and how it can be effectively achieved. It is for instance highly questionable whether parental consent, as required by Article 8 GDPR, will actually be an adequate mechanism to protect children (Van der Hof, 2017). Consent is completely ineffective in practice due to consent overload, information overload, complexity of data processing, and lack of actual choice (Schermer et al, 2014). What is more, depending on how strictly this provision is enforced and implemented, negative side effects may emerge that endanger, rather than protect or respect, a whole range of children's fundamental rights. A genuine risk, for instance, exists of children being excluded from online services, which might adversely impact their rights to development, information, freedom of expression, association, privacy, play, and education laid down in the 1989 United Nations Convention on the Rights of the Child (UNCRC).[1]

However, despite its inadequacies the GDPR also provides opportunities to protect children's personal data in a more meaningful way. To realise this, a comprehensive approach towards the protection of children's personal data is needed, which adopts a rights-based perspective (focused not only on protection, but also on emancipation/participation and development) and takes advantage of the full potential of protective mechanisms offered under the GDPR. Provisions that do not explicitly mention children but are especially important for them, such as the principles of privacy by design and privacy by default as well as data protection impact assessments, should feature prominently in such a holistic approach.

This article aims to explore to what extent the current illusion of autonomy and control by data subjects, including children and parents, based on consent can potentially be mitigated, or even reversed, by putting more emphasis on other tools of protection and empowerment in the GDPR and their opportunities for children. Suggestions will be put forward as to how the adoption of such tools may enhance children's rights and how they could be put into practice by data protection authorities (DPAs) and data controllers. This article starts by setting out how Article 8 GDPR intends to protect children of certain ages and how such protection seems illusory given the complexities of the digital world, which is largely dominated by commercial interests and even clashes with other interests and rights of children (section 2). The article will then explore how other data protection instruments, ie privacy by design and data protection

impact assessments, might potentially relieve some of the issues identified in earlier sections, eg by filling some of the existing gaps in protection of children or by balancing control over children's personal data with other children's interests and rights (section 3). The article wraps up with conclusions (section 4).

2. Children's and parental consent: an ineffective means of child protection

The aim of protecting children in the GDPR most clearly stands out in its Article 8,[2] which is fully dedicated to assigning legal capacity with respect to decisions over lawful processing of children's personal data to parents (or their (legal) representatives) when children are still too uncomprehending and unaware to make those decisions themselves.[3] The GDPR assumes that children of 16 and younger fall in that category, because that is the age stipulated in Article 8 GDPR until which parents are required to give consent for the lawful processing of their children's personal data in relation to information society services after children's personal data. However, conclusive empirical data as to whether and, if so, at what age children understand those decisions does not exist.[4] Moreover, the provision leaves Member States discretional power to diverge from the general rule by setting a lower age as long as they do not go below 13.[5] Apparently, this is a consequence of divergent ages for legal capacity of children in Member States' private laws and, again, not in any way evidence-based.[6] Besides the lack of evidence on what children understand as consumers of the digital economy, Article 8 GDPR raises other problems with respect to protecting children.

First, the protection it offers to data subjects may be very limited, or even illusory. The instrument of consent is fallible as a protective tool for a number of reasons.[7] Consent suggests that we are in control over the processing of our personal data, but this implies that we have a meaningful choice and understand data processing practices of controllers. Consent requires free choice,[8] but if you want to sign up for online services or apps, there normally is no choice other than saying yes to a company's privacy policy (and hence data processing practices), or leave it be altogether, given that privacy policies (and hence the use of the app or online service) are offered on a take-it-or-leave-it basis. Moreover, individuals often do not know what they consent to – privacy policies are not read (too difficult, too time-consuming) – [9] nor would it be enlightening if they were read because they mostly use vague terms anyway. A lot of apps do not even have privacy policies.[10]

Second, the requirement of parental consent for children below a certain age potentially might put the emancipation and participation rights of those children under pressure. The requirement can lead to excessive parental supervision which potentially violates the privacy rights of children.[11] For teens, absence of parents and having their own spaces – also online – free from parental supervision can be perceived as important privacy needs.[12] Moreover, the requirement can, and in some instances already does, ban children from certain online services, if and when social media and other online service providers set age limits for use or subscription in order to avoid the – rather burdensome – parental consent requirement. An example is Google, which does not allow children for whom parental consent is required to have own accounts on its platforms.[13] Hence, even *if* protection of children's personal data could be guaranteed by Article 8, paradoxically it might still infringe on other fundamental rights of children (such as freedom of expression, laid down in Art 13 UNCRC) and defy important freedoms in those areas.

Third, there are significant gaps in the development of children when it comes to understanding the digital environment in which they must consent to the processing of their personal data.[14] Although the situation may differ amongst countries, digital citizenship education may not always be part of the curriculum of schools, and if it is, it may not focus specifically on the digital economy. In order to make decisions about the processing of one's personal data, however, it is imperative to understand the underlying profit-induced processes of the digital economy, which have their own dynamics and are not – necessarily – an extension of the offline world, to the extent that that world still exists anyway. What is more, many of these processes by which data subjects become increasingly transparent to corporations are intentionally invisible to us so as not to undermine their effectiveness – what Keymolen calls 'invisible visibility'.[15] Moreover, they have become so complex that even opening up the black box would not necessarily result in the transparency that we seek.[16]

3. Other tools of child protection and empowerment in the GDPR: novel opportunities

3.1 Introduction

The GDPR provides instruments for protection that are focused on data subjects irrespective of age or capacity, and hence include, but are not specifically geared towards, the situation of children and therefore the protection of their personal data. In the following sections, we will discuss more particularly the principles of privacy by design and privacy by default, as well as data protection impact assessments. Even though these tools are of a more general nature, we argue that from a children's rights perspective controllers and processors[17] have the obligation to take into account the best interests and rights of the child,[18] when implementing them within or applying them to their organisational and technical processes as well as, desirably, to adapt a rights-based approach – ie an implementation that besides protection also focuses on participation and development of children. In the following sections, we will first address the principles of privacy by design and default (section 3.2.) and then data protection impact assessments (section 3.3.).

3.2 The principles of data protection by design and privacy by default

Although not entirely new concepts, the inclusion of the principles of data protection by default and data protection by design in the GDPR are regulatory innovations that can boost the protection of children if implemented well and with children in mind. These principles require that controllers implement data protection principles into the design of their data processing systems. As mentioned previously neither of these principles is focused specifically on children, but with the aim of the GDPR to protect children in mind these principles particularly hold opportunities that might mitigate some of the problems with individual – children's or parental – control over personal data.[19] First, they can ensure that data protection becomes part and parcel of data processing systems without individuals necessarily needing to fully comprehend the frequently complex internal data processing practices of controllers. Second, they provide opportunities to integrate individual control rights into the data systems operation, hence potentially making them both more transparent and effective. Obviously, the impact of these principles depends largely on the ways in which they are implemented and the extent to which engineers will both be capable and willing to effectively shape data protection arrangements in the systems' architecture. This part of the article will set out the meaning of each of these principles (section 3.2.1.) and explore ways of implementing them in view of the need to guarantee the rights of children and the protection of their personal data (section 3.2.2.).

3.2.1. The principles of data protection by design and default

The principles of data protection by design and default are regulated in Article 25 GDPR, which more specifically elaborates the responsibility of controllers already stated under Article 24 GDPR.

According to Article 25 (1) GDPR, controllers must:

> *implement appropriate* ***technical and organisational measures****, such as pseudonymisation, which are designed to* ***implement data-protection principles****, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects* (privacy by design, authors' emphasis).

The data protection principles to which the provision refers are those specified in Article 5 GDPR. These principles are:

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage limitation;
- integrity and confidentiality.

According to Article 25 (2) GDPR, controllers must:

> *implement appropriate technical and organisational measures for ensuring that,* ***by default, only personal data which are necessary for each specific purpose of the processing*** *are processed* (privacy by default, authors' emphasis).

Although these principles are often mostly associated with value-sensitive *technological* design, clearly they also encompass *organisational* measures, such as internal business policies and practices. Measures could more specifically include, amongst others, 'minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features' (Recital 78). The implementation of measures based on these principles is also tantamount to encouraging compliance by controllers (and others) with respect to observing the rights of data subjects and fulfilling their obligations pursuant to the GDPR more generally, ie:

> *[w]hen developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task,* ***producers of the products, services and applications*** *should be encouraged to* ***take into account the right to data protection when developing and designing such products, services and applications*** *and, with due regard to the state of the art, to make sure that controllers and processors are able* ***to fulfil their data protection obligations*** (Recital 78, authors' emphasis).

One example of a technical measure that controllers can implement in their systems design is the pseudonymisation of personal data, which entails a process pursuant to which personal data can no longer be attributed to a particular individual without the use of additional information which is kept securely apart (see Art 4(5) GDPR). Hence, the process can be potentially reversed which distinguishes it from anonymisation, although the difference between the two is not straightforward in practice.[20] However, as the previous explanations reveal, the principles clearly go beyond mere minimisation of personal data, even though an important data protection principle in and of itself. Moreover, the implementation of these principles can and are likely to be furthered by certification schemes (Art 25 GDPR) and codes of conduct (Art 40(2)(h) GDPR).

3.2.2. A child-centred approach towards data protection by design and default

Since children are a dedicated category of individuals demanding stricter data protection under the GDPR, the principles of data protection by design and default seem particularly apt to encourage and ensure the protection of their personal data – and, at the same time, guarantee their rights more generally. Unfortunately, the GDPR does not make that connection, not explicitly at least. Obviously, children might benefit from implementations of these principles similarly to adults, not necessarily needing specifically child-focused privacy by design and default measures. However, their exceptional position under the GDPR, given the profound concerns in respect of their vulnerability,[21] certainly justifies a child-centred implementation of data protection by design in relation to data processing activities that involve children's personal data. This is also recognised in the context of the Council of Europe Strategy for the Rights of the Child, which has resulted in draft 'Guidelines to promote, protect and fulfil children's rights in the digital environment'[22] that specifically mention that privacy by design and default must take into account the best interests of the child.[23] This first raises the question on which children such a child-centred approach should be focused given the lack of a definition of 'child' in the GDPR. Since the GDPR has only explicitly determined ages in a specific situation (children's and parental consent, Art 8 GDPR) we argue that it is most logical to turn to the generally accepted definition of the UNCRC, ie a person under the age of 18,[24] in those instances where the GDPR has left this matter open. In the same fashion, we would argue that in each situation where it is likely, or at least not excluded, that personal data of children will processed by the controller (and others),[25] a child-centred approach towards data protection by design and default is desirable. As a consequence, such an obligation would be further reaching than Article 8's limitation to information society services that are offered directly to a child and also encompasses, for example, youth-care or school-administration systems.

When it comes to the implementation of the principles of data protection by design and default in a child-centred manner, several examples immediately spring to mind. Some data subject rights, being express manifestations of data processing principles to which Article 25 refers, clearly have particular importance in relation to children, either as explicitly recognised by the GDPR (eg right to transparency and right not to be subjected to certain types of profiling) or because these rights are perceived as especially beneficial to children (eg right to erasure, also called the 'right to be forgotten'). Each of these three examples will be briefly elaborated on.

First, the GDPR explicitly mentions the protection of children in relation to transparency of data processing practices and profiling. The principle of transparency (see Art 5(1)(a) GDPR) has been developed in Arts 12, 13 and 14 GDPR, which puts a duty on controllers to provide information on their data processing

practices and data subject rights 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child' (Art 12(1)).[26] Article 12(7) mentions the use of icons[27] to convey 'in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing'. Such icons must be machine-readable if presented electronically, which clearly indicates a transparency by design solution that can be understood as covered more broadly by the principle of data protection by design. However, a more far-reaching data protection by design solution would entail making transparency an integral part of the process of data processing practices, eg by clearly and instantaneously showing important events or changes in data processing systems to users, or by giving them a visualisation and accessible tools to tweak data processing in a control panel. Here we will not go further into the question of what could potentially be effective ways of data protection by design for transparency purposes, but in relation to children it is important that they need to be geared to their perceptions, experiences and expectations. This is not an easy task and requires research into what works for children and at what ages, given that their capacities are still developing.[28] Moreover, the extent to which they will be able to comprehend data processing practices in a meaningful way is also dependent upon their level of understanding of the power dynamics in the digital data economy and how they impact on them as individuals – and hence the choices that they make – and society as a whole.[29]

Second, under the GDPR data subjects have in principle[30] the right not to be subject to automated individual decision-making, including profiling (Art 22).[31] Although Article 22 does not explicitly refer to children, Recital 71 states that '[s]uch a measure should not concern a child'. Given that it refers to 'measure' as 'evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her', we can assume that profiling is meant. As a consequence, organisations need to distinguish between children and adults[32] when profiling data subjects leading to decisions that produce legal effects or similarly significantly affect them, assuming that profiling is otherwise in compliance with data protection regulation. Data processing processes can thus be designed[33] in ways that automatically rule out personal data which holds attributes pertaining to persons under 18[34] as well as refrain from applying the results of profiling processes to these persons.

Third, the right to erasure in the GDPR, more popularly called the 'right to be forgotten', entails a data subject right to have own personal data erased, for, amongst other reasons, when personal data is no longer necessary given processing purposes; the data subject withdraws his or her consent or objects to the processing of personal data; or personal data is unlawfully processed (Art 17(1) GDPR).[35] Given their vulnerability, the right is perceived as especially important with respect to personal data processed while the data subject was still a child (Recital 65).[36] The right to erasure is grounded in the idea that individuals should have control over their personal data[37] and is often phrased in terms of the 'clean slate' argument: whatever youthful sins while growing up, they should not haunt a person into adulthood.[38] Also, personal data that has been collected in relation to the offer of information society services directly to children must be erased at the request of the data subject (see Art 8(1)(f) GDPR). If personal data has been published or shared with third parties, controllers have an obligation to attempt to inform third party controllers of data subject erasure requests (Art 17(2) and 19 GDPR). Although the right to erasure is triggered at the request of the data subject for which accessible and easy-to-use electronic procedures should be in place in the digital environment (see Recital 59 GDPR), it might also be implemented as a privacy by design strategy. This would fit with a proposal by the Canadian Public Interest Advocacy Centre (PIAC) that could be implemented as a default erasure function, unless consent is obtained from or renewed while the child has come of age:

> *Once children reach the age of majority, organisations that have collected and used personal information should no longer be permitted to retain the information gathered during the child's 'legal minority' and should be required to remove the information immediately unless the newly adult person gives his or her explicit consent to the continued collection, use and possible future disclosure of their personal information gathered during their minority.*[39]

Given the right to control own personal data as well as other fundamental rights (notably the rights to freedom of expression, freedom of association and privacy), such a function necessarily depends on the consent of the data subject. Controllers cannot assume that data subjects will want their personal data collected during youth erased, nor are they likely to be inclined to act without further notice by data subjects. However, the possibility must nonetheless be part of internal organisation processes and can be proactively offered to data subjects.

Obviously, this ties in with the principle of privacy by default (eg no publishng of personal data in a social media profile unless the data subject has opted otherwise) and providing data subjects access to data processing practices in relation to their personal data (see Art 15 GDPR, on the right of access of the subject)[40] as well as the opportunity to request a restriction on the processing of their personal data (see Art 18 GDPR). Again, despite effective implementation, exercising such control requires sufficient understanding of data processing practices and their – potential – implications for the data subject.

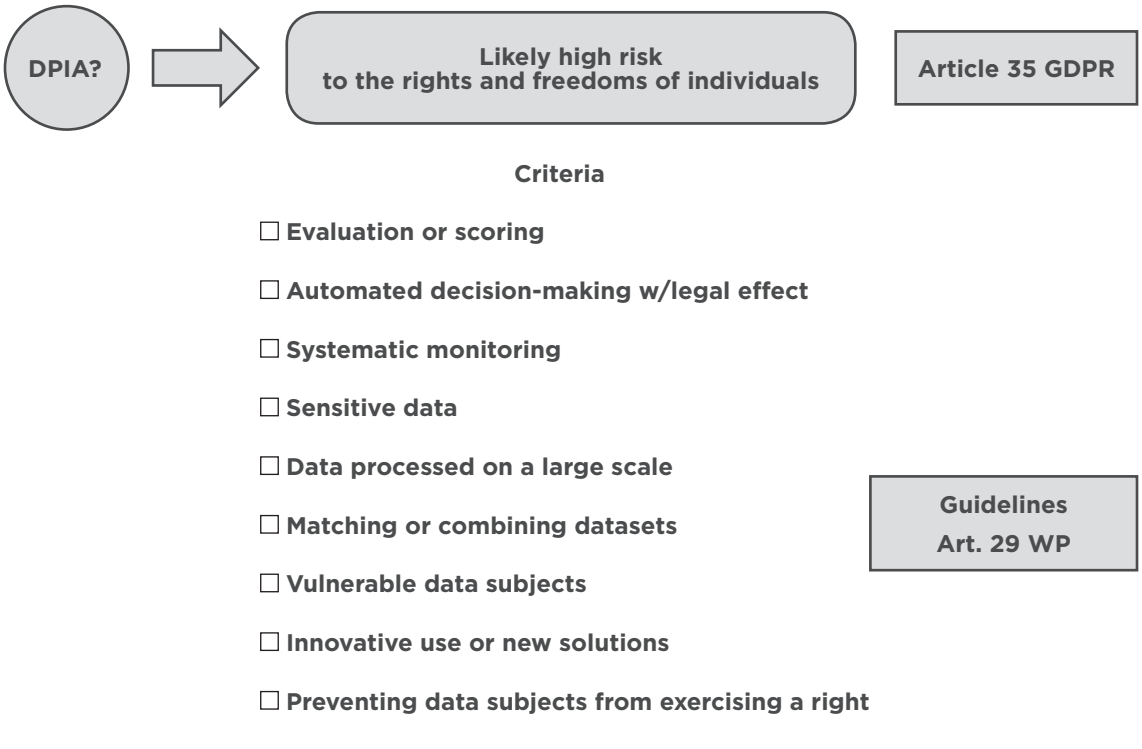
3.3 Data protection impact assessments

3.3.1 Data protection impact assessments in the GDPR

Aside from the potential of the principles of privacy by design and by default, there is another interesting tool that could enhance meaningful protection of the processing of children's personal data. The GDPR includes in Article 35 an obligation for data controllers to assess the impact of processing operations that are likely to result in a high risk to the rights and freedoms of data subjects prior to processing. Such a 'data protection impact assessment' (DPIA) must, for instance, be carried out when personal data is processed for taking decisions regarding specific natural persons based on profiling.[41] According to the Article 29 Working Party's 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679', a DPIA is a 'process designed to describe the processing, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data (by assessing them and determining the measures to address them)'.[42]

3.3.2 Should a data protection impact assessment be carried out for the processing of personal data of children?

The GDPR does not explicitly[43] consider the processing of personal of data of children as such to be a processing activity that carries a *high* risk,[44] but in the light of Recital 38 it could be argued that it is a good practice to carry out a DPIA in such cases. Furthermore, the Article 29 Working Party has identified a number of criteria in order to assess whether a DPIA should be carried out, listed in the figure below.



One of the criteria relates to *data concerning vulnerable data subjects*. According to the Working Party the processing of such data can require a DPIA because of the 'increased power imbalance between the data subject and the data controller, meaning the individual may be unable to consent to, or oppose, the processing of his or her data'. Children specifically are singled out as not being 'able to knowingly and thoughtfully oppose or consent to the processing of their data'. Even though it is considered that the more criteria are fulfilled by the processing operation, the more likely it is to raise a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA, it is also explicitly acknowledged that in some cases, a processing where only one of these criteria is present will require a DPIA.[45] The UK Information Commissioner's Office draft 'Children and the GDPR guidance' also recommends the carrying out of DPIAs, for instance by data controllers that regularly or systematically process personal data of children, to decide what steps need to be taken to verify age and parental responsibility, or to assess the proportionality of restricting children's freedom to learn, develop and explore.[46]

Notwithstanding the interpretation of whether or not DPIAs should be carried out for the processing of children's personal data based on the text of the GDPR, Article 3 UNCRC requires that in all actions concerning children their best interests should be the *primary* consideration.[47] In other words, this principle requires governments, public and private bodies to conduct child (rights) impact assessments and evaluate the impact of any proposed law, policy or decision on children's rights.[48] This requirement in itself provides a strong incentive to assess the risks to children's rights resulting from the processing of their personal data.

3.3.3 How should a child rights-oriented DPIA be carried out?

When undertaking a DPIA a data controller should adopt a children's rights perspective that takes into account the full range of children's rights at stake. The Article 29 Working Party stressed in its 'Guidelines on Data Protection Impact Assessment' that 'the reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion'. Data controllers should realise that other – essential – rights that are attributed to children by the UNCRC may be at risk when their personal data is processed. It has been argued, for instance, that advertising targeted at children on the basis of profiling their personal characteristics or behaviour may not only compartmentalise children, but may also shape their preferences and interests accordingly, ultimately affecting their autonomy and their right to development.[49] Inspiration for undertaking a child rights-oriented DPIA could be gathered from more general child rights impact assessment tools, such as the ones developed by UNICEF.[50]

In relation to the 'best interests' assessment mentioned under the previous section, the UN Committee on the Rights of the Child considers this a general assessment of all relevant elements of the child's best interests, the weight of each element depending on the others.[51] Two additional important principles that are put forward by the Committee are also helpful in thinking about child rights-oriented DPIAs. First, in situations where 'protection' factors affecting a child (eg which may imply limitation or restriction of rights) need to be assessed in relation to measures of 'empowerment' (which implies full exercise of children's rights without restriction), the age and maturity of the child should be guiding factors.[52] This means that different measures may be considered for younger and older children.[53] Second, data controllers must consider that the capacities of children are not fixed, but will evolve. This entails that measures must be revised or adjusted based on physical, emotional, educational and other needs, and that possible scenarios for children's development must be assessed and analysed in the short and long term.[54]

From a more practical perspective, a number of important principles must be taken into account. First and foremost, the DPIA must be carried out *prior* to the processing. This is necessary to be able to mitigate possible risks before the processing starts, and is also inherently linked to the principles of privacy by design and by default. As the Information Commissioner's Office has pointed out: '[i]t is usually easier to incorporate child friendly design into a system or product as part of your initial design brief than to try and add it in later'.[55] Second, the Article 29 Working Party has emphasised that undertaking a DPIA is not a 'one-time exercise'.[56] This means processing practices should be continuously reviewed and regularly re-assessed. Third, it is important for a data controller to be transparent about DPIAs. Whereas the publication of a DPIA is not explicitly required by the GDPR, it is at least good practice to publish the summary or conclusion.[57] When a DPIA concerns the processing of personal data of children, a child-friendly publication is recommended. Finally, taking into account Article 12 UNCRC, which encompasses

the child's right to be heard, participation of children, in accordance with their age and maturity, should be integrated in the DPIA process. They are an important external stakeholder whose views and voices should be actively sought, on the one hand, and duly taken into account, on the other hand.[58]

4. Conclusions

Adopting a child-centred approach to the processing of personal data of children naturally follows the rights of the child, but goes beyond mere compliance with data protection law, and a sole focus on 'protection'. It is essential to keep in mind that the rights to privacy and data protection have important participatory dimensions for children, as they are essential for their individual autonomy and self-determination, and preconditions for 'participation'.[59]

Moreover, as important 'protective' methods that are at the centre of the GDPR – such as parental consent – lead to the illusion of protection rather than meaningful control, a child rights-oriented approach must acknowledge the importance of emphasising the accountability of the data controller, and empowering children and parents. Putting the principles of privacy by design and default into practice and carrying out DPIAs in a child-centred manner has enormous potential in this regard. This will necessitate an interdisciplinary approach, in which cooperation between lawyers, engineers and product or service developers will be simply indispensable.

Finally, and equally essentially, the putting into practice of these promising tools must be based on solid evidence on the understanding and practices of children vis-à-vis processing operations, both now and with regard to emerging trends.

Simone van der Hof
Professor of Law and Digital Technologies, Leiden University

Eva Lievens
Assistant Professor of Law and Technology, Ghent University

Parts of this article build on research carried out in the project 'A children's rights perspective on privacy and data protection in the digital age: a critical and forward-looking analysis of the GDPR and its implementation with respect to children and youth' (Special Research Fund of Ghent University).

References

Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679', (2017) 17/EN WP 248. http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

Berg, B van den, Hof, S van der, 'What happens to my data? A novel approach to informing users of data processing practices' (2012) *First Monday*, 17(7).

Bunn, A, 'The curious case of the right to be forgotten' (2015) *Computer Law & Security Review*, 31(3), 336–50.

Bygrave, L, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017): https://www.idunn.no/file/pdf/66974311/data_protection_by_design_and_by_default_deciphering_the_.pdf.

Colesky, M, Hoepman, J-H, & Hillen, C ,'A Critical Analysis of Privacy Design Strategies', in (2016) IEEE Security and Privacy Workshops (SPW) (2016) 33–40, IEEE.

Friedman, B, Kahn, P H, & Borning, A, 'Value Sensitive Design and Information Systems' in *The Handbook of Information and Computer Ethics* (John Wiley & Sons, Inc, 2008) 69-101.

Hoepman, J H ,'Privacy design strategies' in N Cuppens-Boulahia, F Cuppen, S Jajodia, A A El Kalam, & T Sans (eds), *ICT Systems Security and Privacy Protection* (Berlin, Springer, 2014) 446-59.

Information Commissioner's Office , 'Children and the GDPR guidance' (2017): https://ico.org.uk/media/about-the-ico/consultations/2172913/children-and-the-gdpr-consultation-guidance-20171221.pdf.

van der Hof, S, & Keymolen, E, 'Shaping minors with major shifts: Electronic child records in the Netherlands' (2010) *Information Polity*, 15(4).

van der Hof, S,'I Agree...or Do I? — A Rights-Based Analysis of the Law on Children's Consent in the Digital World' (2016) *Wisconsin International Law Journal*, 34(2), 409–45.

Kloza, D, Van Dijk, N, Gellert, R M, Borocz, I M, Tanas, A, Mantovani, E, & Quinn, P, 'Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals: d.pia.lab' (2017)

Policy Brief 1/2017: http://virthost.vub.ac.be/LSTS/dpialab/images/dpialabcontent/dpialab_pb2017-1_final.pdf.

Lievens, E, & Verdoodt, V, 'Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation' (2017) *Computer Law & Security Review: The International Journal of Technology Law and Practice*.

Lievens E, Livingstone, S, O'Neill, B, McLoughlin, S & Verdoodt, V, 'Children's rights and digital technologies' in Liefaard, T, & Kilkelly, U (eds) *International Human Rights. International Children's Rights Law* (Springer, 2018, forthcoming).

Montgomery KC, & Chester J, 'Data Protection for Youth in the Digital Age' (2015) 1(4) *European Data Protection Law Review* 277.

Narayanan, A, & Shmatikov, V, 'De-anonymizing social networks', in *Proceedings - IEEE Symposium on Security and Privacy* (2009) 173-87.

Ohm, P, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) *UCLA Law Review* 57(6), 1701–777.

Pollach, I, 'What's wrong with online privacy policies?', Communications of the ACM, 50(9), (2007) 103–108. https://doi.org/10.1145/1284621.1284627.

Schermer, B W, Custers, B, & van der Hof, S, 'The crisis of consent: How stronger legal protection may lead to weaker consent in data protection' (2014) *Ethics and Information Technology* 16(2), 171–82.

Shmueli, B, & Blecher-Prigat, A, 'Privacy for Children' (2014) *Columbia Human Rights Law Review* 42(3), 759–95.

UN Committee on the Rights on the Child, 'General Comment No 14 on the right of the child to have his or her best interests taken as a primary consideration (Art 3, para 1)' (2013) CRC/C/GC/14.

Verdoodt V, & Lievens E, 'Targeting Children with Personalised Advertising: How to Reconcile the Best Interests of Children and Advertisers' in Vermeulen G , & Lievens E (eds), *Data Protection and Privacy Under Pressure: Transatlantic tensions, EU surveillance, and big data* (Antwerpen, Maklu, 2017) 313-37.

Wachter, S, Mittelstadt, B, & Floridi, L, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2016) SSRN Electronic Journal.

Zuiderveen Borgesius, F J, 'Singling out people without knowing their names–behavioural targeting, pseudonymous data, and the new Data Protection Regulation' (2016) *Computer Law & Security Review*, 32, 256–71.

Notes

1 Article 24 of the Charter of Fundamental Rights of the European Union also acknowledges the attribution of fundamental rights to children: '1. Children shall have the right to such protection and care as is necessary for their well-being. They may express their views freely. Such views shall be taken into consideration on matters which concern them in accordance with their age and maturity. 2. In all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration. […]'.

2 Article 8 GDPR reads as follows:
(1) 'Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years. (2) The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology. (3) Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.'

3 The aim of this section is not to provide a full-blown analysis of Art 8 GDPR, but rather to focus on the reasons why we think it is not likely to protect children in ways the drafters of the GDPR had in mind. For a more thorough analysis of this provision, we refer to Lievens & Verdoodt (2017) and Van der Hof (2017).

4 At least we are not aware of such evidence, nor does the GDPR explain on what evidence it has based the ages it stipulates.

5 See however the UK Data Protection Bill that sets the age at twelve years.

6 Supra n 4.

7 See further Schermer, Custers, Van der Hof (2014) and Van der Hof (2017).

8 See Arts 4(11) and 7 GDPR on (the conditions for) consent.

9 Pollach (2007).

10 J Koetsier, 40% of top-selling smartphone apps have no privacy policy, Forbes (24 March 2016), https://www.forbes.com/forbes/welcome/?toURL=https://www.forbes.com/sites/johnkoetsier/2016/03/24/40-of-top-selling-smartphone-apps-have-no-privacy-policy/&refURL=&referrer=#.

11 Under the UN CRC, children have a right to privacy pursuant to article 16 and parents must adjust their guidance to the evolving capacities of their children (Art 5 UN CRC), which may entail that older children must be left a sufficient amount of freedom and independence from their parents or caregivers.

12 Shmueli, Blecher-Prigat (2011).

13 Through Google Family Link, parents can however add children to their own account to control their mobile phone use, https://families.google.com/familylink/faq/.
14 For instance, even quite straightforward commercial practices such as Google Ads are understood only by a minority of 12-15s; see Ofcom (2015).
15 Van der Hof, Keymolen (2010).
16 Hence, the reason why algorithmic accountability is an important topic to be explored and fleshed out in relation to the GDPR; see also Arts 12a, 13(2)f and 14(2)g GDPR. See on this topic, eg, Wachter, Mittelstadt, Floridi (2016).
17 According to Art 4 (7) and (8) respectively 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law; and 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
18 The foundation for our reasoning is the UN Convention on the Rights of the Child 1989 (UNCRC), which recognises children as holders of fundamental rights rather than mere objects of protection. The best interest of the child entails that '*in all actions concerning children* […] the best interests of the child shall be the primary consideration' (Art 3 UNCRC, authors' emphasis).
19 As acknowledged by the UK Information Commissioner's Office draft 'Children and the GDPR guidance', Information Commissioner's Office (2017), Children and the GDPR guidance, https://ico.org.uk/media/about-the-ico/consultations/2172913/children-and-the-gdpr-consultation-guidance-20171221.pdf.
20 See Zuiderveen Borgesius (2016). On de-anonymisation see Ohm (2009) and Narayanan, Shmatikov (2009).
21 The extent of which is still unclear given the lack of evidence (see section 2).
22 Available at https://www.coe.int/en/web/children/-/call-for-consultation-guidelines-for-member-states-to-promote-protect-and-fulfil-children-s-rights-in-the-digital-environment?inheritRedirect=true (last visited 1 November 2017).
23 Supra n 18.
24 In an earlier draft of the GDPR this definition was explicitly included, yet removed later for reasons unknown to us.
25 Although Art 25 only mentions controllers, seemingly the GDPR also imposes responsibly 'downstream' to processors and 'upstream' to technology developers', see Bygrave (2017), p 116.
26 See also Recital 58. Article 40(2)(g) GDPR mentions the principle of transparency in relation to children also as a matter that may be regulated as part of codes of conduct of controllers.
27 Given the complexity of data processing icons seem too simple a way of conveying relevant information to data subjects, see eg Van den berg, Van der Hof, 2012 with references to other literature. Nonetheless, transparency solutions that encompass an element of visualisation should not be disregarded as helpful in this regard.
28 Although focused primarily on parents, Art 5 UNCRC recognises that giving guidance and direction to children is dependent on their evolving capacities.
29 See further on the development perspective under children's rights law, Van der Hof, 2017.
30 For the purpose of our argumentation here, we will assume that the exceptions to this right pursuant to in Art 22(2) GDPR do not apply.
31 'Profiling' means 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements' (Art 4(4) GDPR).
32 This may potentially be seen as problematic – how to identify children and in ways that observe the data minimisation principle – however we assume that methods exist or will be developed, preferably privacy-sensitive ones, to enable just that.
33 See Hoepman (2012), Colesky et al (2016) for a more detailed discussion of privacy by design strategies.
34 Strictly speaking the processing of a child's personal data may still be in compliance with data protection law, even if the subsequent of profiling is not; see the exact wording of Recital 71.
35 See for exceptions Art 17(3) GDPR.
36 The text reads as follows: 'That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child.'
37 As more fundamentally embodied in the right to informational self-determination which although not explicitly recognised in the GDPR nonetheless heavily influences European data protection law; see on this right Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] December 15, 1983, 65 BVerfGE 1, 2008 (Ger) (Population Census case) in which the German Constitutional Court recognised the right to informational self-determination as a part of a general personal right.
38 See Bunn (2015); the clean slate notion is recognised in other legal areas, most notably criminal law, as well.
39 PIAC, Public Interest Advocacy Centre (PIAC) Submission to the Government Consultation on A Digital Economy Strategy for Canada, 2010, https://corporationscanada.ic.gc.ca/eic/site/028.nsf/eng/00217.html#p3.2.3.
40 See also Recital 65 GDPR.
41 Recital 91 GDPR.
42 Article 29 Data Protection Working Party (2017) Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Reg 2016/679, 17/EN WP 248, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083, p 4.
43 Unlike, for instance, in the case of '(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale' (Art 35 GDPR). The Article 29 Working Party notes that this is a non-exhaustive list, see Article 29 Data Protection Working Party 'Guidelines on Data Protection Impact Assessment'.
44 Note, however, that in Recital 75 in relation to the responsibility of the controller processing of 'personal data of vulnerable natural persons, in particular of children' is considered a potential 'risk to the rights and freedoms of natural persons'.
45 Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment, p 10.
46 Information Commissioner's Office, Children and the GDPR guidance (2017), n 19.
47 General UN Committee on the Rights of the Child, 'General Comment No 5 (2003) General Measures of Implementation of the Convention on the Rights of the Child (Arts 4, 42 and 44, para 6)' (2003).
48 Ibid.
49 Verdoodt, Lievens (2017).
50 See: https://www.unicef.org/csr/css/Children_s_Rights_in_Impact_Assessments_Web_161213.pdf. Also, for another proposal for child specific privacy impact assessments: Milda Macenaite, Daniel Le Métayer, and Sourya Joyee De, Constructing Child

Specific Privacy Impact Assessments, forthcoming.

51 UN Committee on the Rights on the Child, General Comment No 14 on the right of the child to have his or her best interests taken as a primary consideration (2013) (Art 3, para 1). CRC/C/GC/14.

52 Ibid.

53 Montgomery, Chester, (2015).

54 Ibid.

55 Information Commissioner's Office (2017).

56 Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment', p 13.

57 Article 29 Data Protection Working Party ,'Guidelines on Data Protection Impact Assessment' (DPIA), p17. Also Kloza, Van Dijk, Gellert, Borocz, Tamas, Mantovani, Quinn (2017), p 2.

58 Ibid.

59 Verdoodt, Lievens E, (2017).

The transparency challenge: making children aware of their data protection rights and the risks online[1]

Anna Morgan

Lifting the veil of invisibility

It is timely to focus on children as key stakeholders in the digital ecosystem as we look towards 25 May 2018 and the application of the General Data Protection Regulation[2] (GDPR) across Europe. Post 25 May 2018, for the first time there will be a data protection law at EU level which lifts the veil of invisibility that some would say has hitherto shrouded child users of online and digital services. As recent academic research has highlighted, an estimated one third of internet users across the globe are under 18s.[3] However, as child safety organisations such as the Irish Society for the Prevention of Cruelty to Children have pointed out[4], these internet users are often operating in a world that was not originally designed with them in mind and still fails to recognise them as key players.

However, from 25 May 2018, children are very much at the front and centre of the data protection landscape in Europe. The GDPR attributes special protection to children and so it will shine an unremitting spotlight upon data controllers in relation to safeguarding child users of online services. Effective protection of children in the labyrinthine online and digital environments will involve enabling children to exercise their legal and fundamental rights[5] in a way that minimises the risks to them. This in turn means maximising children's understanding of the cyber-terrain they inhabit as a large part of their everyday lives. As Recital 38[6] of the GDPR states:

Children merit specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.

Central to that core issue of understandability and awareness is the obligation of transparency upon data controllers under the GDPR.

Transparency – a reconstructed and recalibrated obligation

Transparency under the GDPR[7] is not so much a brand new concept in the data protection regulatory regime as a reconstructed and recalibrated obligation, albeit one that has now been very much shunted centre stage. Anyone who has ever 'gone online' will be familiar with the concept of privacy policies or privacy statements on websites which data controllers are required to provide as part of the obligation of fair processing of personal data under the current EU law, the 1995 Data Protection Directive.[8] That obligation of fair processing requires certain minimum information to be provided to data subjects, including the fact of their data being processed, why that processing is happening and who the data controller is. However, there has been an enduring apprehension about the utility of that limited information and whether it truly enables data subjects to take control of their personal data. Such apprehension is particularly pertinent in an online context given that privacy policies

and statements have traditionally been expressed in lengthy legalistic and specialist terms which can be difficult for the average adult user to understand, let alone comprehensible by child users.[9]

Regulatory disquietude

The online world with all its permutations is clearly an intrinsic part of children's everyday lives, and it seems that the age at which children start regularly accessing the web is becoming lower and lower. According to Ofcom[10] in a report published in 2016, based on parents' estimates 3-4 year olds are now spending an average of 8 hours and 18 minutes per week online. Arguably, 21st century children's use of online services is effectively ubiquitous, with many children now more digitally literate than their parents – sharing photos and videos, sending messages, using social media platforms, playing games and accessing entertainment amongst other activities. The issue of transparency in services targeted at children has long been a topic of global concern in the data protection sphere. The International Conference of Data Protection and Privacy Commissioners has issued a number of resolutions[11] in recent years addressing children's online privacy and the need for educational initiatives, and ventilating disquietude about the online encroachment into the private lives of children and the fact that children are often unaware that their information, habits and behaviour are being tracked online. Such regulatory anxiety was arguably validated by the results of the Global Privacy Enforcement Network Privacy Sweep of 2015[12] which saw 29 data protection regulators around the world, including the Irish Data Protection Commissioner and the Information Commissioner's Office in the UK, examine a total of 1,494 websites and apps which were targeted at, or popular amongst, children. The results raised concerns particularly around the volume of children's personal information that was collected by those websites and apps, and later shared with third parties. Among its findings, the study revealed that while 67 per cent of the sites and apps examined collected children's personal data, only 22 per cent tailored their data protection communications to children.

'Children merit specific protection'[13]

The understandability gap in information that data controllers must provide to individuals, particularly where those individuals are children, is what the newly enunciated transparency obligation under the GDPR seeks to address. The core transparency obligation is found in Article 12[14] of the GDPR, with Article 12.1 requiring data controllers to take appropriate measures to provide the required information, related to processing of personal data, to data subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The specific information that must be provided by the data controller to a data subject is now extensive (in comparison with the equivalent information requirements applicable under Articles 10 and 11[15] of the 1995 Data Protection Directive) and is set out in Articles 13[16] and 14[17]. It includes information about who the data controller is, how the personal data will be used, who it will be shared with, whether it will be transferred internationally, the period for which it will be stored, and very importantly, what the data subject's rights are – for example, the right to access, rectification, and erasure of personal data and to make a complaint with a data protection authority. Insofar as providing information to and communicating with children is concerned, it is hugely significant that Article 12.1 of the GDPR carves out an explicit transparency obligation on data controllers for any information which is 'addressed specifically to a child'.[18] This ties in with Recital 58[19] of the GDPR, which makes it clear that because children merit specific protection, any information and communication concerning the processing of a child's data 'should be in such a clear and plain language that the child can easily understand'.

Appropriate measures to achieve transparency

So, what does this new GDPR transparency obligation mean in practical terms for data controllers, such as the tech giants that run the social media, gaming, messaging and photo-sharing websites and apps that are so popular with children? The answer to this is bound up in one of the most important phrases in Article 12, namely the requirement in Article 12.1[20] that data controllers take 'appropriate measures' to provide the required information to data subjects in a concise, transparent, intelligible and easily accessible form. According to Article 12.1, such information is to be provided in writing, or by other means, including where appropriate, by electronic means. However, the term 'appropriate measures' clearly does not provide a fixed benchmark for all data controllers. Instead, it denotes an inherent variability depending on the circumstances in which the data controller is processing personal data. Fundamental to a data controller's ability to comply with the obligation to take 'appropriate measures' to convey the

necessary information to a data subject is that the data controller must first know their audience and then tailor the communication of the information to data subjects in a way that is appropriate to that audience. Therefore, if a data controller knows (as it should do) that its audience consists of, or includes, child users, then it should tailor its privacy information and communications so that child users can readily understand what is happening to their personal data and what their rights are. This necessitates the data controller assessing what the most effective modality will be for conveying the information required under Articles 13 and 14 of the GDPR. Such an assessment may include a consideration of the content and accessibility of written statements, as well as the potential use of more visually based techniques such as cartoons, pictograms, infograms and videos. It should also involve an evaluation of the appropriateness of electronic tools such as layered information notices, pop-up notices, hover-over notices or voice alerts. Of course, central to such considerations is the type of device that is being used, and whether, for example, the device is a tablet, mobile phone or an internet-of-things device (including so-called 'smart' toys). Whatever the device, it is essential that the measures chosen for conveying the information are appropriate to the device being used by the child. With written statements, the overriding requirement for clear and plain language means that privacy notices that are addressed to child users, or users including children, must employ a vocabulary, tone and style of the language that is appropriate to and resonates with children. This necessarily means no 'legalese', no technical terms, jargon or ambiguous phrases that are devoid of any real meaning and may be particularly difficult for children to understand.

The biggest transparency challenge of all?

However, the data protection transparency challenge is not simply about ensuring data controller organisations provide information and communicate in ways that children can understand. Privacy education is essential to encouraging an awareness amongst children of what their personal data is, what their rights are and what the risks are when they share their information online or digitally.[21] No matter how accessibly or appealingly privacy information is presented on a website or an app used by children, if child users do not appreciate the significance of what that information is telling them, then the risk is that they will swipe right past it without taking any notice of it. So perhaps the biggest transparency challenge is getting children to *want* to understand how and why their personal data is used and processed. That challenge has to be embraced not only by data controllers but also by data protection authorities, policy makers, educators, and parents who all have vital roles to play when it comes to educating children and young people about their rights and risks online. The UK Children's Commissioner, in the 'Growing Up Digital' taskforce report[22] in January 2017, called for the creation of a digital citizenship programme to be compulsory in every school from the age of 4 to 14. Similar sentiments were echoed recently in submissions[23] made to an Irish Parliamentary Committee on Children and Youth Affairs in the context of its examination of cyber security for children and young adults. Indeed, digital literacy is already a focus of many educational programmes but in addition to taking account of the more high profile risks around issues like cyber bullying and general online harassment which attract much attention, children also need to be educated about the perhaps more oblique risks arising from their personal data being collected in the digital ecosystem.[24]

Awareness of the right to transparency in personal data processing is growing, and societally it seems that there is movement in the right direction, particularly with the incoming GDPR obligations on transparency. However, arguably technology is currently winning the race over transparency in the privacy arena. There is still a lot of catching up to do in fostering a culture where children – and indeed adults – expect and seek out transparent information from those organisations who collect, use and profit from personal data[25] so that children, and adults, can make smart, informed choices about how, and when, and to what extent, they chose to share their most invaluable asset – their personal data.

Anna Morgan
The author is a solicitor and Deputy Commissioner (Head of Legal) with the Data Protection Commissioner for Ireland. She is the lead rapporteur for the Article 29 Working Party Guidelines on Transparency under the GDPR.

Notes

1 This paper was presented by the author at the Institute of Advanced Legal Studies Information Law and Policy Centre Annual Conference 2017, the theme of which was 'Children and Digital Rights: Regulating Freedoms and Safeguards'.
2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Dir 95/46/EC (General Data Protection Regulation).
3 Sonia Livingstone, John Carr and Jasmina Byrne, 'One in Three: Internet Governance and Children's Rights', Innocenti Discussion Paper No 2016-01 (UNICEF Office of Research, Florence, 2016) 10.
4 See, for example, the ISPCC leaflet 'Cyber safety is the child protection issue of our time' tweeted by the ISPCC (@ ISPCCChildline) on 25 October 2017.
5 The right to Respect for Private and Family Life (Art 7) and the right to Protection of Personal Data (Art 8) are fundamental rights under the Charter of Fundamental Rights of the European Union.
6 Recital 38 of the General Data Protection Regulation: 'Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection 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.'
7 The Article 29 Working Party has published Guidelines on Transparency under the GDPR, a final version of which will be issued following the conclusion of a public consultation (running until 23 January 2018) on the guidelines: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1310&tpa_id=6936
8 See Art 10 (Information in cases of collection of data from the data subject) of Dir 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
9 See, for example, the Article 29 Working Party Opinion 10/2004 on More Harmonised Information Provisions at p 5, para 4.
10 'Children and parents: media use and attitudes report' (Ofcom, 2016), p 47, fig 17.
11 30th International Conference of Data Protection and Privacy Commissioners (2008, Strasbourg), 'Resolution on Children's Online Privacy', 38th International Conference of Data Protection and Privacy Commissioners (2016, Marrakesh), 'Resolution for the Adoption of an International Competency Framework on Privacy Education'.
12 For more information on the results of the 2015 Global Privacy Enforcement Network Privacy (GPEN) sweep, see the GPEN 2015 Annual Report. https://www.privacyenforcement.net/sites/default/files/Annual%20Report%20Final%20Version.pdf and also https://www.dataprotection.ie/documents/GPen/GPEN2015.pdf
13 Recital 38. The principle is also referred to in Recital 58 of the GDPR, as considered further below.
14 Article 12 of the GDPR: Transparent information, communication and modalities for the exercise of the rights of the data subject.
15 Article 10: Information in cases of collection of data from the data subject) and Art 11: Information where the data have not been obtained from the data subject.
16 Article 13 of the GDPR: Information to be provided where personal data are collected from the data subject.
17 Article 14 of the GDPR: Information to be provided where personal data have not been obtained from the data subject.
18 Article 12.1 states: 'The controller shall take *appropriate measures* to provide any information referred to in Arts 13 and 14 and any communication under Arts 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, *in particular for any information addressed specifically to a child*. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means' (emphasis added).
19 Recital 58 states: 'The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.'
20 See n 18 above.
21 See, for example, the International Conference of Data Protection and Privacy Commissioners, 'Personal Data Protection Competency Framework for School Students' (October 2016), p4: 'In the digital age, responsible, ethical and civic-minded education in the use of new technologies is a priority for action, particularly young people in school. A key component of digital education is highlighting privacy and personal data protection. Educators have a key role to play in this digital education of citizens': https://edps.europa.eu/sites/edp/files/publication/16-10-18_resolution-competency-framework_en.pdf.
22 Children's Commissioner, 'Growing Up Digital: A report of the Growing Up Digital Taskforce '(January 2017), p3: https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/Growing-Up-Digital-Taskforce-Report-January-2017_0.pdf
23 Submissions to the Joint Oireachtas Committee on Children and Youth Affairs can be accessed under September 2017 and October 2017 at: http://www.oireachtas.ie/parliament/oireachtasbusiness/committees_list/cya/presentations/
24 As illustrated, for example, by dialogue with children recorded by the 5Rights movement at: http://5rightsframework.com/the-5-rights/5rights-by-young-people.html
25 See, for example, p 22 of the Better Internet For Kids Roundtable Report (June 2016) on 'The General Data Protection Regulation and children's rights: questions and answers for legislators, DPAs, industry, education, stakeholders and civil society': https://www.betterinternetforkids.eu/documents/167024/2013511/GDPRRoundtable_June2017_FullReport.pdf/e6998eb6-ba3c-4b5d-a2a6-145e2af594f2

Case Notes & Comments

New approach to media cases at the Royal Courts of Justice is a welcome and refreshing development

In 2012 Mr Justice Tugendhat, ahead of his retirement in 2014, made a plea for more media specialist barristers and solicitors to consider a judicial role: 'As the recruiting posters put it: Your country needs you.' He emphasised the particular burden of freedom of expression cases, which require judges, for example, to consider the rights of third parties, 'even if those third parties choose not to attend court' and to provide reasons for the granting of injunctions at very short notice. Without expert knowledge of the applicable law, this is no easy task. Fortunately, media law cases have not fallen apart with the respective retirements of Sir Michael Tugendhat and Sir David Eady, and recent specialists to join the High Court include Mr Justice Warby in 2014, and Mr Justice Nicklin in 2017 – both formerly of 5RB chambers.

The arrival of Warby J, who was given the newly created role of 'Judge in charge of the Media and Communications List', has provided a welcome opportunity to propose changes to the procedure of media litigation in the Queen's Bench Division, where the majority of English defamation and privacy claims are heard. Since taking on responsibility for the cases involving one or more of the main media torts – including defamation, misuse of private information and breach of duty under the Data Protection 1998 – Warby J has spoken about his hopes and plans for the list, and also conducted a consultation among those who litigate in the area, as well as other interested parties. The consultation considered the adequacy of Civil Procedure Rules and Practice Directions; the adequacy of the regime for monitoring statistics on privacy injunctions; and support for the creation of a new committee. As a socio-legal researcher rather than legal practitioner, my interest was piqued by the latter two questions. For some time, I have been concerned that efforts by the Judiciary and the Ministry of Justice to collect and publish anonymised privacy injunction data have been insufficient, and also that the availability of information about media cases could be improved more generally.

My own efforts to access case files and records in 2011-13, to update research conducted by Eric Barendt and others in the mid 1990s, and to interrogate assertions of defamation's 'chilling effect', proved largely unsuccessful and I was astonished how rudimentary and paper-based internal systems at the Royal Courts of Justice appeared to be. Although public observers are entitled to access certain documents – such as claim forms – the cost and difficulty in locating claim numbers prohibits any kind of useful bulk research which would allow more sophisticated qualitative and quantitative analysis of media litigation. I jumped, therefore, at the opportunity of the consultation to raise my concerns about the injunctions data, and to support the creation of a new user group committee. My submission with Paul Magrath and Julie Doughty, on behalf of the Transparency Project charity, made suggestions for revising the injunctions data collection process, including the introduction of an audit procedure to check information was being recorded systematically and accurately.

Following the consultation, Warby J held a large meeting at the RCJ for all respondents and other interested parties at which he shared a table of proposals from the consultation, provisionally ranked as 'most feasible', 'more difficult' and 'most difficult'. The last category also included proposals which would require primary legislation, which would be a matter for Parliament rather than the Judiciary. I was pleased that our initial proposals on the transparency of injunctions data have been deemed practical and feasible in the first instance. Also considered achievable are some of the proposals related to case management and listings, updating the pre-action protocol (PAP), the Queen's Bench Guide, and civil practice directions in light of developments in privacy, data protection and defamation litigation and press regulation (not least to reflect the Defamation Act 2013).

This meeting also established the creation of a new Media and Communications List User Group (MACLUG) to which a range of representatives have been appointed. The group comprises members of the Bar and private practice solicitors (including both claimant and defendant specialists), in-house counsel, clerks, and a costs practitioner. Additionally, I have joined as a representative of public interest groups – ie those engaged in academic research and third sector work. The new committee met for the first time at the end of 2017, and members have formed smaller working groups to take forward the 'feasible' proposals, which will be discussed with our respective constituencies in due course, and where relevant, eventually proposed to the Civil Procedure Rule Committee to consider.

In a speech to the Annual Conference of the Media Law Resource Center in September 2017 Warby J identified his overall aims for the 'big picture' and landscape of media litigation: to resolve disputes fairly, promptly, and at reasonable cost. All of which were 'easier said than done', in his words. Quite so. But it is right that it should be attempted, and with judicial input where appropriate. Warby J's efforts to date are to be applauded, and in particular, his open approach in addressing some of the flaws and inconsistencies of current practice, and evaluating structural and systemic issues.

That said, a committee formed by the judiciary is constrained in its remit, quite rightly. The consideration of changes to primary legislation should fall to Parliament. It is therefore important that media law practitioners and other stakeholders also work with the Ministry of Justice and HMCTS to inform ongoing work on courts modernisation, and push for wider consultation and involvement in reforms. A further challenge is to persuade government and parliamentarians to take on any issues requiring changes to legislation. Part I of the Leveson Inquiry addressing, in part, the relationship between media proprietors, editors and politicians showed that the process of consultation on public policy affecting the news media has been subject to undue influence by certain private interests and insufficiently transparent. To this end, perhaps the new Lord Chancellor and Secretary of State for Justice, David Gauke MP, and the new Secretary of State for Digital, Culture, Media and Sport, Matt Hancock MP, might consider ways in which they can consult more openly and fairly in their development of policy and draft legislation on freedom of expression, reputation and privacy.

Dr Judith Townend
Lecturer in media and information law at the University of Sussex, and a member of the Queen's Bench Division Media and Communications List User Group Committee

Recent Developments

Forum non conveniens

In *Kennedy v National Trust for Scotland* [2017] EWHC 3368 (QB) before Sir David Eady, the claimant, who was domiciled in Scotland, sought damages and other remedies in England against the National Trust for Scotland in respect of a number of allegations published in both jurisdictions as well as in Italy, France and Brazil. He relied not only on defamation but also on negligence and on alleged breaches of the Data Protection Act 1998. The dispute arose over the claimant's attendance at Craigievar Castle in Aberdeenshire, when he took a series of photographs of a naked model for commercial purposes. He claimed that he did so pursuant to an oral contract with a representative of the defendant, which expressly authorised that activity. This episode came to the attention of a National Trust donor who protested that the castle had been used for taking nude photographs. Her remarks caught the attention of a journalist who made enquiries and was given a statement by or on behalf of the defendant which was reported in the *Scottish Mail on Sunday*.

Thereafter, the defendant also issued a press release which denied that the taking of the photographs had been authorised. This was sent to a number of media outlets.

The defendant argued that jurisdiction should be declined on the basis that Scotland would be the more appropriate forum. The claimant resisted this, not only because the discretion would be exercised in favour of England and a stay refused, but also because issues of *forum conveniens* were altogether precluded because this was not 'a purely domestic case'.

Section 49 of the Civil Jurisdiction and Judgments Act 1982 provided that:

> *Nothing in this Act shall prevent any court in the United Kingdom from staying, sisting, striking out or dismissing any proceedings before it, on the ground of forum non conveniens or otherwise, where to do so is not inconsistent with the 1968 Convention or, as the case may be, the Lugano Convention or the 2005 Hague Convention.*

However, because the claimant complained of re-publication of the defamatory words in France and Italy, he suggested that this was not 'a purely domestic case'. He argued that jurisdictional matters were governed by the Brussels Recast Regulation 2012/1215, which would take precedence over the 1982 Act. Where that regulation applied, it followed from *Owusu v Jackson* (C-281/2002) [2005] QB 801 and *Maletic v lastminute.com GmbH* (C-478-12) [2014] QB 424 that the English court was deprived of any discretion to stay on grounds of *non conveniens*. The court considered whether there was indeed an international element such as to take this case out of the category of 'domestic, and if so, and if the Recast Regulation did apply, considered whether its operation would override the rules of national law contained in Schedule 4 of the 1982 Act (including the doctrine of *forum non conveniens*)?

The rule of general jurisdiction derived from Article 4(1) provided that, subject to specific exceptions, a person domiciled in a Member State shall be sued in the courts of that Member State. The exceptions were contained in sections 2 to 7 of chapter II. There were, for example, the rules of special jurisdiction in section 2 at Article 7. It was provided in Article 7(2) that in matters relating to tort, delict or quasi-delict, a person domiciled in a member state may be sued in the courts for 'the place where the harmful event occurred or may occur'. The purpose of the regulation, and of the rule of general jurisdiction, was to regularise issues of jurisdiction as between different states. No such question arose here, because the only potential competition was between the courts of Scotland and England & Wales (ie internal to the United Kingdom).

By contrast, in *Owusu v Jackson* and *Maletic* there was clearly an international element. In the present case, one defendant had been sued in the UK, where it was to be treated as domiciled, and the fact that remedies were sought against it in respect of re-publications in

other jurisdictions did not entail any issue of competing courts. It was thus not easy to see why the regulation should be engaged. The competing claims would appear to be matters for internal determination by the courts of the UK. The claimant pointed to a passage in *Briggs on Civil Jurisdiction and Judgments* (6th edn) at 2.28, cited in *Cook v Virgin Media Ltd* [2016] 1 WLR 1672 at [25]. There, a hypothetical illustration was discussed of a defamation case which raised an issue concerning a complaint of publication 'by a person outside the United Kingdom, whether the defendant or another'. He relied on this scenario as giving rise to an international element sufficient to engage the regulation. But the present scenario was different. There was only one defendant and it was sued in this Member State, where it was treated as domiciled. The only dispute was internal, as between the courts of Scotland and England. There was no reason for the regulation to be engaged and the court was not precluded from addressing issues of *forum non conveniens*.

Sir David Eady then considered the court's approach to jurisdiction within the UK. The allocation of jurisdiction internally as between the various constituent 'nations' or parts of the UK was governed by section16 and Schedule 4 of the 1982 Act (as amended to take account of changes in the Brussels Recast Regulation). The structure and wording of Schedule 4 corresponded closely to those of the current regulation.

In the present context, what mattered was rule 3(c), which acknowledged a special jurisdiction 'in matters relating to tort, delict or quasi-delict' such that a person domiciled in one part may be sued in the courts for the place where the harmful act occurred (or may occur). These provisions were subject to those of section 49 and the doctrine of *forum non conveniens*.

It was appropriate to have in mind the principles expounded in *Shevill v Presse Alliance* [1995] 2 AC 18. Where a libel was published in several jurisdictions, a litigant was given the choice of suing where the defendant was domiciled, where he could recover all relevant remedies, or suing in each of the countries where harm was said to have been incurred. Here, such a policy would require that the claimant choose between Scotland (where the defendant was domiciled or conducted its affairs) and the courts of Italy, France, Brazil and England (where the other offending publications were said to have occurred and where at least some harm was alleged to have been incurred). He had chosen to sue only in England but had not confined his claim to the harm incurred in that jurisdiction.

The court considered whether (1) the action should be stayed under section 49 and (2) whether the claims for global damages be struck out. There was no doubt that 'substantial justice' could be achieved in the courts of Scotland. The question was whether Scotland was clearly more appropriate for resolving the issues in the interests of all the parties and the ends of justice. That was initially for the defendant to establish. Could it be shown that there were 'connecting factors' which pointed to the conclusion that it was with Scotland that the action had the most real and substantial connection? In such circumstances, a stay would ordinarily be granted unless the claimant could demonstrate that there were *nonetheless* circumstances such that justice required that a stay should be refused. The defendant pointed to many 'connecting factors' which indicated Scotland to be the natural and clearly more appropriate forum. Such factors included the convenience of the parties and witnesses, the expense of the litigation, the applicable law, and the place(s) where the parties respectively resided or carried on their business. The policy that a citizen of the EU was, subject to specified exceptions, entitled to assume that he would be sued in his state of domicile, was a connecting factor which should be put in the forefront of the court's consideration. Both parties were domiciled in Scotland and the primary focus of their businesses was also there. The courts in England had only a limited jurisdiction, in the sense that they would only be able to address such damage as was alleged to have occurred in England & Wales, under the special jurisdiction contemplated by rule 3 of Schedule 4, whereas the Scottish courts would be able to adjudicate upon the whole of the damages claim – including in respect of damage (if any) accrued in other jurisdictions. If the claimant chose to sue on matters going wider than harm done in England & Wales, it was difficult to see why he should be permitted to do so outside the jurisdiction of the defendant's domicile.

The defendant's solicitor also relied on the events underlying this dispute all which took place in Scotland. The likely defences would be truth and qualified privilege involving evidence from members of the defendant's staff and those who prepared the press statement. The issues of negligence would also largely turn on evidence relating to what took place in Scotland. So far as data protection was concerned, the processing took place in Scotland and the evidence would again overlap considerably with that to be called on the other causes of action. It was always important to remember the fundamental test of 'substantial justice'. If one was confident that this could be achieved, as had been conceded in relation to Scotland, then the court should guard against giving

any of these supposed advantages disproportionate significance. The Scottish courts were more than capable of providing substantial justice in this dispute. Most of the connecting factors indicated Scotland as the natural forum, in particular the parties were domiciled or based in Scotland (and the defendant should be sued there in accordance with the general jurisdiction indicated in r 1 of Sched 4). Further the Scottish courts could deal with all the remedies sought, and would not be confined to dealing with the 'harm' alleged to have been incurred in Scotland, whereas the English courts would (by reason of the special jurisdiction) be limited to assessing damage suffered in England. Since the claim had such real and substantial connections with Scotland, the claimant had an impossible task to show that *nonetheless* justice required that the case remain in England and the stay was granted.

So far as a claim for global damaged was concerned, the defendant argued that if the claim were to go ahead in England that the claim for damages would need to be substantially restricted. The claimant should be limited to recovering in respect of England & Wales. The claims relating to Scotland, Italy, France and Brazil should be struck out. This was based on the reasoning in *Shevill v Presse Alliance* [1995] 2 AC 18, which was authority for the proposition that global damages would be recoverable only in the courts of the contracting state (the expression now used was 'Member State') where the defendant was domiciled. The relevant contracting state here was of course the UK.

The claimant argued that the court was being asked to develop a novel sub-national model of *Shevill*, such that only courts of the sub-national place where the publisher was domiciled would have jurisdiction to award global damages – and all other courts within the UK would be restricted to awarding damages for harm occurring within their relevant regions. But such a proposition was not odd where there was room for the application of *forum non conveniens* within the Member State, and moreover that Parliament had approved rules in parallel to those under the Recast Regulation – including those under Schedule 4. *Shevill* presented a perfectly defensible framework for bringing consistency to international jurisdiction issues in the context of publication cases. If it was right that the courts in England would only have jurisdiction by reason of rule 3 of Schedule 4 (the special jurisdiction), it was difficult to understand why the global damages should be left in. The logical course was to recognise that the claim was intended to embrace a range of matters outside the special jurisdiction; accordingly, those should be determined under the general jurisdiction (ie of the courts of the place where the defendant was domiciled or, for that matter, had its 'centre of interests'). If and in so far as the claim was allowed to proceed in England, it would be right to confine the issues to those properly arising under the special jurisdiction. On that rather artificial hypothesis, it was right to strike out the global damages claims.

Harassment and interim non-disclosure order on persons unknown

GYH v Persons Unknown (Responsible for the Publication of Webpages) [2017] EWHC 3360 (QB) before Mr Justice Warby concerned an application without notice to the defendant for an interim non-disclosure order to restrain a campaign of harassment. The claimant was a transgender woman who worked as an escort, and provided sexual and companionship services to her clients under a work name. The campaign consisted mainly of the publication of various items or categories of personal information or purported information about the claimant. These included allegations that the claimant had HIV/AIDS, and other information or purported information about her sexual life, and her physical and mental health. It was the claimant's case that the allegation that she had HIV/AIDS was false, as was some of the other information about her. Such information continued to be published online at several locations. The claimant's case was that the publications had caused her considerable distress. They were said to amount to harassment by the misuse of private information. The claimant also maintained, as part of her claim, and as part of her argument in support of an injunction, that some of them were both defamatory and untrue.

The claimant sued 'persons unknown', coupled with descriptive wording referring to two world wide web addresses at which content of which the claimant complained had been published. It was open to a claimant who could not identify those responsible for the conduct complained of to sue 'persons unknown.' Section 12(2) of the Human Rights Act 1998 prohibited the court from granting relief which might affect the exercise of the Convention right to freedom of expression unless it was satisfied 'that there are compelling reasons why the respondent should not be notified or that the applicant has taken all practicable steps to notify the respondent.' There was no suggestion that there were any good reasons for not notifying the defendant and the court was satisfied that the claimant has taken all the steps that could have been taken to identify a defendant who might be served with the claim.

In relation to the claim there were some categories of personal information that were of an intimate and plainly sensitive nature: information about sexual life, about sexual health, about physical health, and about mental health. Information about a person's sexual conduct and practices, about sexually transmitted diseases they had, and about their mental health, was all information about the person's private life. The right to control what was done with such information, and the right to respect for information of these kinds, ranked towards the upper end of the Article 8 hierarchy. That remained true in this case, even if some of the information was also information relating to and relevant to the claimant's occupation. That factor was relevant but it did not mean the information was not private.

The fact that the claimant was an escort providing sexual services was undoubtedly relevant to the assessment of her claims. A person's past conduct might be relevant to whether they had a reasonable expectation of privacy. Work of this kind did not disqualify a person from the protection given to private life. But the claimant's role inevitably meant that she was likely to have made public or placed beyond her control some information about her sexual life and, on the evidence, she plainly had done so. Someone who made information about herself public might have no reasonable expectation of privacy in relation to that or similar information and hence no right to prevent others from disclosing it. It was well-established, however, that there was no question of a person waiving her right to privacy in a particular zone of her private life, merely by publicising some information falling within that zone. The 'zonal' approach to reasonable expectations of privacy was discredited. The court's approach had to be more tailored than that.

The court's attention was drawn to a review of the claimant's services on a website seemingly devoted to providing UK 'punters' with consumer information, and to the claimant's own response posted later the same day. The review contained a description of the claimant, her attributes, the flat, and what the two of them did, with a list of positives and negatives, and an overall evaluation. A number of questions and comments followed from two others, before the claimant's response, accompanied by seven pictures of herself.

The claimant could be taken to have approved and consented to the disclosure of the information in the review and her response. The claimant acknowledged that the nature of her work meant that she accepted the disclosure of some private information about her online; however, such disclosures and such approval and consent did not mean that the claimant had entirely surrendered control over her privacy and online identity. The campaign of which she complained was a sweeping attack on the values of autonomy and dignity which were at the heart of the right to privacy. That was an argument which would prevail at any trial of the claim. The information which was the target of this application was of a different nature entirely from the information that the claimant appeared to have distributed herself, or to have approved.

It would be going too far to say that a person providing sexual services for reward as an escort had an unqualified right to decide what information about themselves could be made public. A person in that business might have to put up with some unwanted disclosures about themselves. On appropriate facts, no doubt, there would be a public interest in the circulation of information which the person concerned would not want distributed. If a sex worker practised unsafe sex and had contracted HIV/AIDS yet continued to work there would be a clear justification for warning those who might suffer the consequences. In Convention terms, the Article 10 rights involved would outweigh the Article 8 rights. But the communications complained of in this case were not cast in the form of public health warnings, and nor would the channels of distribution seem well-suited to that purpose. More importantly, and fundamentally, there was credible and uncontradicted evidence that these allegations were false. Here, the claimant stated that she did not practise unsafe sex, and was HIV negative. There was no public interest in the distribution of false information of this kind, nor was it reasonable to publish false allegations to this effect.

Similar reasoning applied, if examined from the viewpoint of defamation law. Some at least of the publications complained of conveyed defamatory meanings to the effect that the claimant carried on business as an escort providing sexual services even though she had practised unsafe sex and contracted a sexually transmitted disease. The claimant was justified in her assertion that imputations of that kind caused serious harm to reputation. The credible and uncontradicted evidence was that such imputations were false. There could be no other defence available, at least so far as future publication was concerned.

Objectively assessed, the 'nub' of the claimant's claim was a complaint of harassment. Her evidence of distress was detailed and convincing. The principal means by which the harassing conduct had been carried out was by the misuse of private information

about the claimant. The fact that some such information was false did not undermine the claim. It tended rather to support it. The fact that some of the information happened to be defamatory should not undermine the claim, either. This was not an instance of a claimant abusing the process by 'shopping' for a cause of action which would help her avoid the application of the defamation rule.

It was apparent that this claim had a commercial motive behind it, as well as a personal and private one. If a claim was brought to protect a reputation for commercial reasons, that could tend to weaken if not undermine a claim to restrain publication as a misuse of private information. That might be so because it weakened the case that the information was private. However, the information about sexual conduct and sexual health was inherently both private and commercial. A commercial interest could undermine an injunction application of this kind for at least two other reasons: (a) because it would mean that the defamation rule applied; and (b) because damages would be an adequate remedy: The first consideration did not operate here and the second did not apply because, there was a sincere and credible case that the claimant continued to suffer distress which could not in principle or in practice be compensated by money.

The claimant had persuaded the court that she would succeed at trial in establishing that the continuing publication and other harassing conduct should be restrained, and she was therefore entitled in principle to an injunction to prevent the continuation of the harassment to which she had been subjected.