Data protection is a minefield of complex rules and regulations. It is an area of law that impacts on every organisation, large or small, that handles personal data.

A User's Guide to Data Protection: Law and Policy, Third Edition sets out all the compliance issues that organisations need to be aware of in order to successfully comply with UK data protection rules and regulations, along with a full assessment of the EU Data Protection Regulations and their impact on UK practice.

The work is a first-port-of-call text providing clear guidance through the complex web of data protection issues and regulation, in relation to internal issues affecting employees, agents, contractors, etc. It also addresses external issues concerning customers, prospective customers and users across all areas of data interface.

The third edition has been fully updated and includes coverage and analysis of:
- The General Data Protection Regulations (GDPR) to be implemented by May 2018
- Coverage of the new UK Data Protection Bill
- Latest Information Commissioner Office investigations, reports and guidance, office cases, complaint decisions and penalties
- Brexit negotiation issues and post-Brexit data protection implications
- Significant increased fines and penalties regime, and data protection competition law comparisons
- Right to be Forgotten updates and new cases
- The Conservative election proposals for the Right to be Forgotten
- International developments and issues, Cloud, internet, revenge porn, online abuse
- New security law and new data protection e-commerce and electronic communications data protection law

Sharenting: balancing the conflicting rights of parents and children
Claire Bessant
Are children more than ‘clickbait’ in the 21st century?
Baroness Beeban Kidron
Interpreting the child-related provisions of the GDPR
Lisa Atkinson
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
The transparency challenge: making children aware of their data protection rights and the risks online
Anna Morgan

CASE NOTES & COMMENTS
RECENT DEVELOPMENTS
Communications Law Vol. 23, No. 1, 2018

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. Contributions to the Journal will be asked to be duly given (free of charge) to publishers 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 above email address.

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

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),

In Brief

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 around the privacy 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, 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 (2016/679) 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 sharing personal media privacy setting generate. In her view, the misuse of private information 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 IPC’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 an urgent need to safeguard 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 participatory 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 these 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’s online privacy in the GDPR, although it may jeopardise child development. 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 participatory 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 these 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’s online privacy in the GDPR, although it may jeopardise child development. 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 participatory 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 these 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’s online privacy in the GDPR, although it may jeopardise child development. 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 participatory 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 these 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’s online privacy in the GDPR, although it may jeopardise child development. 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 participatory 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 these 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’s online privacy in the GDPR, although it may jeopardise child development. 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 participatory 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 these 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’s online privacy in the GDPR, although it may jeopardise child development. 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 participatory 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.
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
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 enable 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 at 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.

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 at 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 (ECC) 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 communications 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 Code of Practice to accompany the changes to the Electronic Communications Code.
Communications Law Vol. 23, No. 1, 2018

In Brief

- 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 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 in 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 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.

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 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 in 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 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.2 Although in the United Kingdom far fewer parents admit to sharing their children’s information online,3 many parents will post hundreds of photographs of their children before they reach their fifth birthday.4 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’.5

Parents are often considered the ‘guardians,’ or ‘gatekeepers’ of their children’s personal information. Their role in providing consent to use their children’s information is recognised in European Union legislation and the jurisprudence of the European Court of Human Rights (ECtHR).6 The English judiciary also seemingly acknowledge that parents are the best people to decide whether a child’s information is shared.7 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.8 Whilst that story has since been denounced as untrue,9 it nonetheless raises an interesting question: could a child successfully use 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.10 Photographs are often shared.11 Indeed, sharenting frequently begins before birth, with the uploading of foetal ultrasound photographs.12 Significant numbers of parents blog.13 Whilst some bloggers use pseudonyms or avoid posting their children’s faces, others openly disclose their children’s names, images and locations.14 Some parents use websites such as YouTube to vlog.15 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.16

Parents are often considered the ‘guardians,’ or ‘gatekeepers’ of their children’s personal information. Their role in providing consent to use their children’s information is recognised in European Union legislation and the jurisprudence of the European Court of Human Rights (ECtHR). The English judiciary also seemingly acknowledge that parents are the best people to decide whether a child’s information is shared. 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. Whilst that story has since been denounced as untrue, it nonetheless raises an interesting question: could a child successfully use 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. Photographs are often shared. Indeed, sharenting frequently begins before birth, with the uploading of foetal ultrasound photographs. Significant numbers of parents blog. Whilst some bloggers use pseudonyms or avoid posting their children’s faces, others openly disclose their children’s names, images and locations. Some parents use websites such as YouTube to vlog. 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.
Sharenting: the positives

Parents sharent for many different reasons. Sharenting allows parents to broadcast their children’s achievements. Sharenting also helps parents to avoid isolation, to maintain emotional, practical and social support, and to share parenting advice. Where third parties comment harshly upon their children’s achievements or behaviours, they might themselves engage in unflattering or倫(419,308),(493,336)

Sharenting: the negatives

Parents have always shared stories and photos with friends and family. Sharenting, however, takes sharing to a different level. Sharenting involves a child’s story being told without their consent. Many parents express concern about ‘over-sharing’, where parents share too much, or share inappropriate, embarrassing information. A 2017 Oxford survey suggests most UK parents who share online carefully who can view photos or videos and would not share information their child would be unhappy with. 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, and the feelings parents might never reveal to their children’s faces. Some adults with chronic disabilities have expressed concern about parents discussing their children’s disabilities, emphasising the nature of a child’s disability, or the challenges they face. Some adults with chronic disabilities have expressed concern about parents discussing their children’s disabilities, emphasising the nature of a child’s disability, or the challenges they face.

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 parents to stop sharing, and to remove any objectionable information. If a parent refuses to do so, however, several civil regimes provide the child with means to seek an injunction to stop ongoing dissemination. The first remedy which will be considered is the law of confidentiality. The law of confidentiality has long been used by private individuals to protect personal information, private images, details of home and family life and medical information. In recent years, the law of confidentiality has been widely used by private individuals to protect personal information. The law of confidentiality has long been used by private individuals to protect personal information, private images, details of home and family life and medical information. In recent years.

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 parents to stop sharing, and to remove any objectionable information. If a parent refuses to do so, however, several civil regimes provide the child with means to seek an injunction to stop ongoing dissemination. The first remedy which will be considered is the law of confidentiality. The law of confidentiality has long been used by private individuals to protect personal information, private images, details of home and family life and medical information. In recent years.
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. 65 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 the information. While in Megarry J’s original formulation disclosure need not be to ‘the claimant’s detriment’, subsequent case law refinements indicate that this is no longer necessary. 66 Indeed in the 2013 Supreme Court decision in Vestergaard Frandsen v Vestergaard Frandsen Ltd Neuberger suggested 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 he had agreed, or ought to have appreciated, that it was confidential’. 67

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

Confidential information

Where an injunction is sought the court must determine 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. 68 Health-related information will, however, ordinarily be assumed to lack capacity. 69 Indeed in the 2013 Supreme Court decision in McKennitt v Ash it could certainly be argued that sharing information about such activities does not breach any duty of confidence. However, an alternative argument could also be made.

In Tchenguiz v Inman Lord Neuberger recognised concerns about ‘confounding the developing law of privacy under article 8 and the traditional law of this action has developed, and ‘branched off into two general forms’. 70 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). 71 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”,’ 72 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’. 73

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. 74 This requirement will prove particularly challenging for younger children, who are generally assumed to lack capacity. 75 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. 76 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 the information. While in Megarry J’s original formulation disclosure need not be to ‘the claimant’s detriment’, subsequent case law refinements indicate that this is no longer necessary. 77 Indeed in the 2013 Supreme Court decision in Vestergaard Frandsen Ltd 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 he had agreed, or ought to have appreciated, that it was confidential’. 78

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

Confidential information

Where an injunction is sought the court must determine 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. 79 Health-related information will, however, ordinarily be considered confidential. 80 Given Lord Buxton’s comments in McKennitt v Ash that ‘events in a person’s home’ cannot be lightly regarded as public knowledge, 81 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. 82 Where children’s activities are undertaken outside the family home and viewed by or enjoyed alongside many other people, Woodward v Hutchins 83 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, 84 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 could also be made.

In Tchenguiz v Inman Lord Neuberger recognised concerns about ‘confounding the developing law of privacy under article 8 and the traditional law of this action has developed, and ‘branched off into two general forms’. 70 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). 71 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”,’ 72 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’. 73

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. 74 This requirement will prove particularly challenging for younger children, who are generally assumed to lack capacity. 75 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. 65 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 the information. While in Megarry J’s original formulation disclosure need not be to ‘the claimant’s detriment’, subsequent case law refinements indicate that this is no longer necessary. 66 Indeed in the 2013 Supreme Court decision in Vestergaard Frandsen v Vestergaard Frandsen Ltd Neuberger suggested 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 he had agreed, or ought to have appreciated, that it was confidential’. 67

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

Confidential information

Where an injunction is sought the court must determine 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. 68 Health-related information will, however, ordinarily be considered confidential. 69 Given Lord Buxton’s comments in McKennitt v Ash that ‘events in a person’s home’ cannot be lightly regarded as public knowledge, 81 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. 82 Where children’s activities are undertaken outside the family home and viewed by or enjoyed alongside many other people, Woodward v Hutchins 83 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, 84 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 could also be made.

In Tchenguiz v Inman Lord Neuberger recognised concerns about ‘confounding the developing law of privacy under article 8 and the traditional law of
confidential. 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’ in respect of the information in issue, is, … a good test to apply when considering whether a claim for confidence is well founded. It shines well with the test suggested in classic commercial confidence cases by Megarry J in Coco v N Clark (Engineers) Ltd [1969] RPC 41, page 47, namely whether the information had the ‘necessary quality of confidence’ and had been ‘imported in circumstances importing an obligation of confidence’.77

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, in contrast, in Weller and in Murray the Court of Appeal were prepared to accept that where children were engaged in family activities, and were subject to the expectations generated by those activities, those children had a reasonable expectation of privacy, in public. The most recent case to consider a child’s expectation of privacy in public is Re JR 38,78 a case which saw the Supreme Court divided 3-2. Whilst in this case the majority were not prepared to accept that it’s a child’s reasonable expectation of privacy in public or its ‘expected confidence’79 in respect of the information in issue, is, … a good test to apply when considering whether a claim for confidence is well founded. It shines well with the test suggested in classic commercial confidence cases by Megarry J in Coco v N Clark (Engineers) Ltd [1969] RPC 41, page 47, namely whether the information had the ‘necessary quality of confidence’ and had been ‘imported in circumstances importing an obligation of confidence’.77

A key difficulty in the sharenting context is that parents enjoy many of the same experiences as their children. The information they share online with others often tell a story not only of the child’s life, but of the parents’ life. This poses problems where a parent is the owner of the sharented information.80 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?81 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 Mr Ash unconvincingly raised similar arguments as Mr McKerr in McKeown v Ash,82 the reality was that in McKeown the court was more focused on the disclosure of information about the child’s own experiences, which the court was more willing to protect.

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. 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’ in respect of the information in issue, is, … a good test to apply when considering whether a claim for confidence is well founded. It shines well with the test suggested in classic commercial confidence cases by Megarry J in Coco v N Clark (Engineers) Ltd [1969] RPC 41, page 47, namely whether the information had the ‘necessary quality of confidence’ and had been ‘imported in circumstances importing an obligation of confidence’.77

This does not, of course guarantee that the courts will treat information about such activities as confidential, but, if not, as discussed above, the OMP in McKerr v Ash,83 in the McKeown v Ash,84 the reality was that in McKerr the claimant was very much the focus of the disclosure. Where a parent genuinely wishes to share information about their own experiences the position may be less clear. As Buxton reminds us in McKerr of all these cases are fact sensitive.85

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.

Sharenting: balancing the conflicting rights of parents and children

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.

Confidentiality: the relationship between parents and children

Confidentiality: the relationship between parents and children

Confidentiality: the relationship between parents and children

Confidentiality: the relationship between parents and children

Confidentiality: the relationship between parents and children

Confidentiality: the relationship between parents and children

Confidentiality: the relationship between parents and children
Commonly defendants will justify disclosure on the basis that disclosure is in the public interest or that the information is in the public domain.82

To justify their sharenting a parent might argue, for example, that disclosure was 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.83 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 established 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 in the public domain and ‘cannot be regarded as confidential’. 84 In such circumstances, the parent might argue that there is no purpose to be gained from an injunction. Certainly, in Eady v Mirror Group Newspapers Ltd and Thomas 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,’ 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.85 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’. 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. 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’.86 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’.87 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 it is 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’, 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. 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.

Mooreham 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.’ 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. 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’.86 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’.87 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 it is 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’, 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. 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.

Mooreham 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.’ This comment is clearly supported by the analysis above. Fortunately, the MOPI action offers the child a possible alternative cause of action.
The tort of misuse of private information

To succeed in their MOPI claim the child must satisfy both limbs of a two-stage test. **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 test 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. 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.’ 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 for the purposes for which the information came into the hands of the publisher.

In Weller Lord Dyson considered the application of these factors where a newspaper had taken and published photographs of three children. Concluding that the children did not 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. **Weller concerned proceedings brought by celebrity parents who had deliberately kept their children out of the public eye; manifestly Lord Dyson’s comments might be applicable to a child who objects to parental sharenting.**

Stein 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 situation, the protection 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. **Weller concerned proceedings brought by celebrity parents who had deliberately kept their children out of the public eye; manifestly Lord Dyson’s comments might be applicable to a child who objects to parental sharenting.**

Stein 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 situation, the protection 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. **Weller concerned proceedings brought by celebrity parents who had deliberately kept their children out of the public eye; manifestly Lord Dyson’s comments might be applicable to a child who objects to parental sharenting.**

The tort of misuse of private information

To succeed in their MOPI claim the child must satisfy both limbs of a two-stage test. **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 test 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. 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.’ 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 for the purposes for which the information came into the hands of the publisher.

Stein 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 situation, the protection 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. **Weller concerned proceedings brought by celebrity parents who had deliberately kept their children out of the public eye; manifestly Lord Dyson’s comments might be applicable to a child who objects to parental sharenting.**

Stein 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 situation, the protection 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. **Weller concerned proceedings brought by celebrity parents who had deliberately kept their children out of the public eye; manifestly Lord Dyson’s comments might be applicable to a child who objects to parental sharenting.**

Stein 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 situation, the protection 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. **Weller concerned proceedings brought by celebrity parents who had deliberately kept their children out of the public eye; manifestly Lord Dyson’s comments might be applicable to a child who objects to parental sharenting.**

Stein 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 situation, the protection 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. **Weller concerned proceedings brought by celebrity parents who had deliberately kept their children out of the public eye; manifestly Lord Dyson’s comments might be applicable to a child who objects to parental sharenting.**
Concerns have, however been raised about such an expectation. In a number of cases, the ECHR 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 Dassouris v Greece112 and Bogomolova v Russia,113 the ECHR 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 ECHR 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 photographs of the child in order to promote their own interests, the position would or might have been different from a case like this, where the parents have taken care to keep their children out of the public gaze.114

This line of reasoning is controversial.115 It suggests that a parent’s expectations and decisions on a child’s right to privacy 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.116 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 rights of children are in the hands of their parents may have not been problematic in Reklos, Murray or Weller, but in some respects 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.117 Murray, Sir Anthony Clarke acknowledges that a “child has his own right to respect for his privacy distinct from that of his parents.”118 Subsequent decisions do not, however, adequately recognise that children have an absolute right to privacy, independent of their parents, and that children should, as they mature, be entitled to enforce that right, irrespective of whether their parents value privacy.119 A child should

Sharenting: balancing the conflicting rights of parents and children

to adults. Indeed, Stein identifies striking differences in the normative expectations of adults and children.110 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 shall also require further consideration. In a number of cases, the ECHR 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 Dassouris v Greece112 and Bogomolova v Russia,113 the ECHR 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 ECHR 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 photographs of the child in order to promote their own interests, the position would or might have been different from a case like this, where the parents have taken care to keep their children out of the public gaze.114

This line of reasoning is controversial.115 It suggests that a parent’s expectations and decisions on a child’s right to privacy 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.116 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 rights of children are in the hands of their parents may have not been problematic in Reklos, Murray or Weller, but in some respects 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.117 Murray, Sir Anthony Clarke acknowledges that a “child has his own right to respect for his privacy distinct from that of his parents.”118 Subsequent decisions do not, however, adequately recognise that children have an absolute right to privacy, independent of their parents, and that children should, as they mature, be entitled to enforce that right, irrespective of whether their parents value privacy.119 A child should
Sharenting: balancing the conflicting rights of parents and children

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

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. 126 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 those 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 of comparable importance.

Firstly, neither article has as such precedence over the other. Secondly, where the values under the two articles are in conflict, the court must ensure that the comparative importance of the specific rights being claimed in the individual case is necessary. Thirdly, the justification for interference with or restricting Article 8 rights is the public interest, which accords with the requirements of Article 3 of the 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 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 a 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 his or her sharenting on the basis that they are exercising their 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.

However, whilst the balancing tests in MOPI cases and the sharenting case 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. 132 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. 133 In Re J a father, who objected to the removal of his fourth child into local authority care, used social media to share his concerns. 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.’ 126 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 family court’s jurisprudence seems also to lend weight to the child’s privacy claim. 133 In Re J a father, who objected to the removal of his fourth child into local authority care, used social media to share
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 J (adult: court’s jurisdiction):

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, the child’s best interests are the primary consideration. However, the question of whether this matter 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 sharing 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?

The English courts have not considered in the context of a MOPI claim how the parental right to respect for family life conflicts with the child’s best interests, the child’s best interests are the primary consideration. However, the question of whether the court is to be allowed to go so far as to prejudice the rights of the individual children involved in a MOPI claim how the parental 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.
Sharing: balancing the conflicting rights of parents and children

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.

Obligations imposed on data controllers by the DPA

The Directive and the DPA stipulate certain conditions that apply where an individual processes personal data. The leading European case of Lindqvist146 confirms that where one person refers to another individual on an internet page, identifying them 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 states to and identifies their child, they will be considered to fall within the remit of the Directive. The Directive requires those who process personal data 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 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 technologies 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 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,142 a focus on harm may prevent a child from obtaining a remedy under the MOPC 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.141 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.142 Privacy also potentially affords children with a remedy against sharenting. Not only are such harms not always easy to identify or quantify,142 a focus on harm may prevent a child from obtaining a remedy under the MOPC tort if their only objection is to the dissemination of their private information.

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.142 Privacy also potentially affords children with a remedy against sharenting. Not only are such harms not always easy to identify or quantify,142 a focus on harm may prevent a child from obtaining a remedy under the MOPC tort if their only objection is to the dissemination of their private information.

Sharenting: balancing the conflicting rights of parents and children

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.

Obligations imposed on data controllers by the DPA

The Directive and the DPA stipulate certain conditions that apply where an individual processes personal data. The leading European case of Lindqvist146 confirms that where one person refers to another individual on an internet page, identifying them 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 states to and identifies their child, they will be considered to fall within the remit of the Directive. The Directive requires those who process personal data 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 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 technologies 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. 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.155

Parents will be able to satisfy a Schedule 2 condition, if their child consents to the sharenting,149 or where (The 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. A parent might argue that they have a legitimate interest in sharing their child’s information with friends and family, and/or that they are sharing information as permitted by their 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.150 The child’s consent is thus relevant both under Schedule 2 and under Schedule 3. One must question, however, how many parents seek their child’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.156 This costs nothing. If the ICO is satisfied that there has been a serious breach of the data protection principles, the ICO may seize a legally binding enforcement measure requiring their parents to erase the objectionable information.157

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.152 (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.’)153 Assuming that the child has not consented to the sharing, the parent must respond within one day to confirm either that they have complied with, or to what extent they will comply with, or stating why they consider the request unjustified.154 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, sharenting is not always curtailed when 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.” The position in European Union law is that the personal and household exemptions 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. Communications Law Vol. 23, No. 1, 2018

**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.156 This costs nothing. If the ICO is satisfied that there has been a serious breach of the data protection principles, the ICO may seize a legally binding enforcement measure requiring their parents to erase the objectionable information.157

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.152 (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.’)153 Assuming that the child has not consented to the sharing, the parent must respond within one day to confirm either that they have complied with, or to what extent they will comply with, or stating why they consider the request unjustified.154 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 parent has 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 parent has 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.
number of people. The Article 29 Working Party 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). 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. In the UK, strikingly, the ICO has taken an entirely different approach.

Section 36 DPA is significantly broader than Article 32(2), stating that “'personal 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 personal, family or household affairs (including recreational purposes) 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). 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. In the UK, strikingly, the ICO has taken an entirely different approach.

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, 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. 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. Concerns have been raised that the GDPR does not appear to provide children (such as those whose information is shared by their parents) with significantly increased protection. 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 than the Directive. This is important. It has been suggested that parents should be seeking their children’s consent before they share. 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.

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. 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. Concerns have been raised that the GDPR does not appear to provide children (such as those whose information is shared by their parents) with significantly increased protection. 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 than the Directive. This is important. It has been suggested that parents should be seeking their children’s consent before they share. 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.

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.
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. 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 outstanding legitimate grounds for processing.

Fully cognisant of its obligations to comply with the GDPR, the Queen’s speech 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. 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 that there is no requirement to have reached 18 years old before the right to erasure may be exercised. Whilst the government has not explicitly considered how a child might use the right 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 during their childhood. There is clearly scope to use the right for this purpose.

Communication Law
Vol. 23, No. 1, 2018

Of course, anyone can ask a social media provider such as Facebook to remove information posted online by a third party. However, the claim is likely to be high. The emotional costs and the potential damage to the family unit cannot be ignored. 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. 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 after a set time, and WhatsApp which contains messages to a ‘third party’ could be considered by both parents and children. These provide protection to the child’s privacy, and they do not require a 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. 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. 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. 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, 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’ and data protection ‘at the core of their operations’, it is questionable whether Facebook is meeting these expectations.180 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

While several legal remedies are available to children who object to sharenting, none are guaranteed to succeed. 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. 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. 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 after a set time, and WhatsApp which contains messages to a ‘third party’ could be considered by both parents and children. These provide protection to the child’s privacy, and they do not require a 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. 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. 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. 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, 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’ and data protection ‘at the core of their operations’, it is questionable whether Facebook is meeting these expectations.180
Sharenting: balancing the conflicting rights of parents and children

group, have been suggested as a means to manage different levels of broadcasting. Although of course screenshots of snapshots that are 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, Family, Family Wall, JuxFamily, MymyFamily, Rootsy, Google+, Instagram, Family Leaf). Ammar et al also reported that a number of participants in their research used ‘Dropbox, Google+, LiveJournal, Flickr, Shutterfly, Snaps, Instagram and Cloud 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). Translations

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 not sharing pictures revealing their children’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.

Whilst there is 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 arisen about who should undertake this crucial educational role. In France and Germany the police have used social media to advise parents of the dangers inherent in sharing and the need to protect the private life of minors. Sharenting is unlikely to result in commission of any criminal offence in the UK, unless it can clearly be said that it is in the best interests of the child or children involved. The child’s age and capacity will already be known to many. Parents do, however, seem to

Sharenting: balancing the conflicting rights of parents and children

The sense of self and well-being. This includes a right to privacy threats. In the sharenting context it is problem-atic that children’s privacy expectations are inextri-cably bound up with their parent’s expectations for the child’s privacy. If children are to be able to effec-tively use existing remedies, such as the MOPI tort, to remove information which violates their privacy, English law may need to be reinterpreted to recogn-ise that children have a right to privacy, indepen-dent from their parents’ privacy expectations’. 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.

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 interfer-ence, saw where interference is necessary to protect vulnerable family members, is a core principle of the long underpinned English law. It is a principle that has been recognised both in the ECtHR and the UNCRC. In the sharenting context, however, it is not clear whether a parent’s right to determine how their family’s informa-tion is used goes way to the child’s right to privacy. This is a particularly difficult issue when the informa-tion that a parent wishes to share relates to both their child’s and the other 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 legiti-mate to share that information, which will already be known to many. Parents do, however, seem to

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 dissemi-nation of their personal, private or confidential infor-mation. 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 having children’s privacy expectations. 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 not sharing pictures revealing their children’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.

Whilst there is 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 arisen about who should undertake this crucial educational role. In France and Germany the police have used social media to advise parents of the dangers inherent in sharing and the need to protect the private life of minors. Sharenting is unlikely to result in commission of any criminal offence in the UK, unless it can clearly be said that it is in the best interests of the child or children involved. The child’s age and capacity will already be known to many. Parents do, however, seem to

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 dissemi-nation of their personal, private or confidential infor-mation. 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 having children’s privacy expectations. 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 not sharing pictures revealing their children’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.

Whilst there is 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 arisen about who should undertake this crucial educational role. In France and Germany the police have used social media to advise parents of the dangers inherent in sharing and the need to protect the private life of minors. Sharenting is unlikely to result in commission of any criminal offence in the UK, unless it can clearly be said that it is in the best interests of the child or children involved. The child’s age and capacity will already be known to many. Parents do, however, seem to

Conclusions
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 ICD has made clear that it does 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

Sharenting: balancing the conflicting rights of parents and children

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 ICD has made clear that it does 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

Sharenting: balancing the conflicting rights of parents and children

Notes

1 House of Lords Select Committee on Communications 2nd report of 2016-17 ‘Growing up with the internet’ HL Paper 31 (2016), Written evidence from Evan Diplodian, Research Economist, University of Nottingham.

41 42% of UK parents admit to regularly sharing 50% 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 (PDOM. The Communications Market Report 2017 https://www.norma.uk/research-and-data/multi-sector-research/norma-2017, 35).

5 Megan Rose, ‘The average parent shares almost 1,500 images of their child online before their 5th birthday’ http://parentsone.

8 (App No 13812/09) judgment 20 June 2017.

9 See EU: General Data Protection Regulation (GDPR) authorises consumers to request that their personal data be erased. For a court applying a ‘reasonable expectation of privacy’ test this is problematic. For a court applying a ‘reasonable expectation of privacy’ test this is problematic. For a court applying a ‘reasonable expectation of privacy’ test this is problematic.


15 More than 4 million parents in the United States read or write their child online before their 5th birthday’. http://parentzone.

16 Ibid.

17 Article 8 General Data Protection Regulation (GDPR) authorises consumers to request that their personal data be erased. For a court applying a ‘reasonable expectation of privacy’ test this is problematic. For a court applying a ‘reasonable expectation of privacy’ test this is problematic. For a court applying a ‘reasonable expectation of privacy’ test this is problematic.


20 4% of UK parents admit to regularly sharing 50% 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 (PDOM. The Communications Market Report 2017 https://www.norma.uk/research-and-data/multi-sector-research/norma-2017, 35).

21 Duggan et al, ibid, 4; CS Mott Children’s Hospital National Poll on Children’s Health: Parents on Social Media, Likes and Children’s Online Identity (2015-23 22) (2015-23 22); Kumar and Schoenebeck in (3), 1302 and 1304.

22 Kumar and Schoenebeck in (3), 1302.

23 Kate Oliphant Johnson, ‘Mummy blogs and Representations of Motherhood: “Bad mothers” and their Readers’ 2017 Social
The focus of this article is the removal of images from the internet. In addition to the three main remedies discussed below, where it is recognised that third parties have subsequently shared images, a child might consider using the Children, Family and Civil Procedure Rules in England and Wales. This is the right of a minor to consent to medical treatment. Under-16s must prove they have ‘sufficient understanding’ to make for the removal of personal information https://www.oste.org.uk/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 consent to the removal of images/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 consent to the removal of images and are able to interpret the information they receive. See SCOI, 8.4 that has the right to request your personal information? https://www.oste.org.uk/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 consent to the removal of images.

...
Shrieking: balancing the conflicting rights of parents and children

...
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 be 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 194 signatories. A glaring exception is the country host to the major tech companies, but nonetheless the UN Convention 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 test on the Crown Prosecution Service when
Are children more than ‘clickbait’ in the 21st century?

considering prosecuting older children, we don’t allow adults to hold children to contractual obligations, we put pedestrians crossing through school zones at rate films according to the developmental stages of childhood; children have special protections around smoking, drinking and gambling and even take steps to protect them in environments where adults smoke, drink and gamble.

In short, the prevailing understanding is that society must, above all 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 immunities 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 is that a digital environment does not reflect this consensus.

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 is that a digital environment does not reflect this consensus.

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 is that a digital environment does not reflect this consensus.
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 recognize 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. 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 inequalities, 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 commodifies.

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 spent so much of their time. This bundle of technologies is not the only science to capture a person’s attention and keeping them in ‘rapture’, which can include:

- soft rhythmic sounds or music to block out real life;
- 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;
- random confirmations – from algorithms that feel your wanting activity;
- personal streaks
- community streaks
- 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 recognize 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. 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 inequalities, 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 commodifies.

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
Are children more than ‘clickbait’ in the 21st century?

Communications Law

Are children more than ‘clickbait’ in the 21st century?

decided the problematic use of technology against its
users. Jaron Lanier accused tech of having gone over
a threshold into behaving as 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 space-time algorithms to ensure that a
child is perpetually bombarded with a bespoke recipe
of emotional and technological pull. 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, a service
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 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 oversupervised.
It cannot be a good use of technology to allow its
brightest and finest to ignore the needs of most vulne-
rable 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
safely. 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. These 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 partici-
pant 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 opera-
tional 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
constantly refuse to collect and publish data on
children’s complaints or monitor under-age use of
their services.

B. Some tech is not very interested in children.
The real interest is in drones and driverless cars,
conquering space and cryogenics, and opera-
tional 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
constantly refuse to collect and publish data on
children’s complaints or monitor under-age use of
their services.

C. 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. These 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 partici-
pant 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 opera-
tional 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

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 tech is the choice is between children using adult services or nothing. This is, at best, disorientating, nearly a billion current users are children, so they should be cast out or unambiguously 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 phenomenon. 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 the need to work on your 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 all will have 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.

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 tech is the choice is between children using adult services or nothing. This is, at best, disorientating, nearly a billion current users are children, so should they be cast out or unambiguously 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 phenomenon. 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 the need to work on your 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 all will have 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.’ 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 Hanard[3], 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 amend-
ments 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.

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 inten-
tional. 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 clickbaits 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

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 report1 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

1 Interestingly, a 2013 report 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 38 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.

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 into 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 inadequacies 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).

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, 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, should feature prominently in such a holistic approach.

1. Introduction

The General Data Protection Regulation that enters into 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 inadequacies 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).

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, should feature prominently in such a holistic approach.
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, 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. 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 child's personal data in relation to information society services after children's personal data. However, consent is a problematic data as to whether and, if so, at what age children understand those decisions does not exist. Moreover, the provision leaves Member States discretion to set the legal age. Thus, 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 so limited, or even illusory. The instrument of consent in the GDPR is fallible as a protective tool for a number of reasons. Consent suggests that we are in control over the processing of our personal data. However, it implies that we have a meaningful choice and understand processes by which data subjects become increasingly transparent to corporations that are intentionally invisible to us, as they form part 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 practices by which data subjects become increasingly transparent to corporations are intentionally invisible to us, as they form part 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 practices by which data subjects become increasingly transparent to corporations are intentionally invisible to us, as they form part 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 practices by which data subjects become increasingly transparent to corporations are intentionally invisible to us, as they form part 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 practices by which data subjects become increasingly transparent to corporations are intentionally invisible to us, as they form part 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 practices by which data subjects become increasingly transparent to corporations are intentionally invisible to us, as they form part 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 practices by which data subjects become increasingly transparent to corporations are intentionally invisible to us, as they form part 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 practices by which data subjects become increasingly transparent to corporations are intentionally invisible to us, as they form part 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 practices by which data subjects become increasingly transparent to corporations are intentionally invisible to us, as they form part 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.
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 includes, 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 processors27 have the obligation to take into account the best interests and rights of the child,28 when implementing them within or applying them to their organisational and technical processes as well as, desirably, to adapt a rights-based approach – 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.29 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).

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 includes, 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 processors27 have the obligation to take into account the best interests and rights of the child,28 when implementing them within or applying them to their organisational and technical processes as well as, desirably, to adapt a rights-based approach – 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.29 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:

- when developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfill 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 fulfill 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 designed in a child-centred manner, several examples immediately spring to mind. Some data subject rights, being express manifestations of data processing principles, are 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’ that specifically mention that privacy by design and default is desirable. As a consequence, such an obligation would be further reaching than Article 5(1)(a) GDPR, to which Article 25 refers, clearly have particular importance in relation to children, either as explicit manifestation of data protection principles or as data protection principles can and are likely to be furthered by certification schemes (Art 25 GDPR) and codes of conduct (Art 40(4)(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 measures 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 would benefit from implementations of these principles, similar 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, 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’ that specifically mention that privacy by design and default is desirable. As a consequence, such an obligation would be further reaching than Article 5(1)(a) GDPR, to which Article 25 refers, clearly have particular importance in relation to children, either as explicit manifestation of data processing principles or as data protection principles can and are likely to be furthered by certification schemes (Art 25 GDPR) and codes of conduct (Art 40(4)(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 measures 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.

Fortunately, the GDPR does not make that connection, not explicitly at least. Obviously, children would benefit from implementations of these principles, similar 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, 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’ that specifically mention that privacy by design and default is desirable. As a consequence, such an obligation would be further reaching than Article 5(1)(a) GDPR, to which Article 25 refers, clearly have particular importance in relation to children, either as explicit manifestation of data processing principles or as data protection principles can and are likely to be furthered by certification schemes (Art 25 GDPR) and codes of conduct (Art 40(4)(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 measures 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.
practices and data subject rights 'in a concise, trans-
parent, intelligible and easily accessible form, using
clear and plain language, in particular for any infor-
mation addressed specifically to a child' (Art 12(1)).34
Article 12(7) mentions the use of icons27 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 protec-
tion by design solution would entail making transpa-
rency an integral part of the process of data processing
practices, eg by clearly and instantaneous 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
guided to their perceptions, experiences and expec-
tations. 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 fact that their capacities are still developing
means that data profiling 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.39
Second, under the GDPR data subjects have in prin-
ciple37 the right not to be subjected to automated
decision-making, including profiling (Art 22).30 Although Article 22 does not explicitly refer to
children, the protection given in Article 19 GDPR on
the right to erasure, which is based solely on automa-
ted decision-making, including profiling (Art 19 GDPR).
Third, the right to erasure in the GDPR, more
popularly called the 'right to be forgotten', entails a
data subject's right to have personal data processed
on them or her which is based solely on automated
decision-making, including profiling (Art 19 GDPR).
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
compliance with data protection regulation. Data processing processes can thus be designed31 in ways that automatically rule out personal data which holds attributes pertai-
nng to persons under 1831 as well as refrain from
applying the results of profiling processes to these
persons.
Once children reach the age of majority, organi-
sations that have collected and used personal
information should no longer be permitted to
continue to do so. This is based on the view that a child's
legal 'minority' and should be required to remove
the information immediately unless the newly
and/or her now adult self are satisfied that
in the continued collection, use and possible future
disclosure of their personal information gathered
during their minority they will still be able to comprehend
and consent to the continued use and possible future
disclosure of their personal information gathered
during their minority.36
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
compliance with data protection regulation. Data processing processes can thus be designed30 in ways that automatically rule out personal data which holds attributes pertai-
nng to persons under 1830 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's right to have personal data processed
on them or her which is based solely on automated
decision-making, including profiling (Art 19 GDPR).
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
compliance with data protection regulation. Data processing processes can thus be designed31 in ways that automatically rule out personal data which holds attributes pertai-
nng to persons under 1831 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's right to have personal data processed
on them or her which is based solely on automated
decision-making, including profiling (Art 19 GDPR).
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
compliance with data protection regulation. Data processing processes can thus be designed30 in ways that automatically rule out personal data which holds attributes pertai-
nng to persons under 1830 as well as refrain from
applying the results of profiling processes to these
persons.
The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR

Obviously, this ties in with the principle of privacy by default (e.g., no publishing 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 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. 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)’.

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 consider the processing of personal data of children as such to be a processing activity that carries a high risk, 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.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluation or scoring</td>
<td>Art. 29 WP</td>
</tr>
<tr>
<td>Automated decision-making w/legal effect</td>
<td></td>
</tr>
<tr>
<td>Systematic monitoring</td>
<td></td>
</tr>
<tr>
<td>Sensitive data</td>
<td></td>
</tr>
<tr>
<td>Data processed on a large scale</td>
<td></td>
</tr>
<tr>
<td>Matching or combining datasets</td>
<td></td>
</tr>
<tr>
<td>Vulnerable data subjects</td>
<td></td>
</tr>
<tr>
<td>Innovative use or new solutions</td>
<td></td>
</tr>
<tr>
<td>Preventing data subjects from exercising a right</td>
<td></td>
</tr>
</tbody>
</table>

The GDPR does not explicitly consider the processing of personal data of children as such to be a processing activity that carries a high risk, 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.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluation or scoring</td>
<td>Art. 29 WP</td>
</tr>
<tr>
<td>Automated decision-making w/legal effect</td>
<td></td>
</tr>
<tr>
<td>Systematic monitoring</td>
<td></td>
</tr>
<tr>
<td>Sensitive data</td>
<td></td>
</tr>
<tr>
<td>Data processed on a large scale</td>
<td></td>
</tr>
<tr>
<td>Matching or combining datasets</td>
<td></td>
</tr>
<tr>
<td>Vulnerable data subjects</td>
<td></td>
</tr>
<tr>
<td>Innovative use or new solutions</td>
<td></td>
</tr>
<tr>
<td>Preventing data subjects from exercising a right</td>
<td></td>
</tr>
</tbody>
</table>

3.3.3 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. 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)’.
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.46 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.47

Notwithstanding the interpretation of whether or not a DPIA 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.48 In other words, this principle requires governments, public and private bodies to consider children’s rights when assessing and evaluating the impact of any proposed policy, law or decision on children’s rights.49 The ’right to development’ is given 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 the Processing of Personal Data of Children’ the importance of the ‘right to development’ to be inherent in 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’.50 Second, the Article 29 Working Party has emphasised that the processing of a child’s data is not a ‘one-time exercise’.51 This means process- ing 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.52 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

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.46 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.47

Notwithstanding the interpretation of whether or not a DPIA 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.48 In other words, this principle requires governments, public and private bodies to consider children’s rights when assessing and evaluating the impact of any proposed policy, law or decision on children’s rights.49 The ’right to development’ is given 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 the Processing of Personal Data of Children’ the importance of the ‘right to development’ to be inherent in 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’.50 Second, the Article 29 Working Party has emphasised that the processing of a child’s data is not a ‘one-time exercise’.51 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.52 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
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’. 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

Part 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


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.49

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’. 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


The importance of privacy by design and data protection impact assessments is strengthened by protection of children’s personal data under the GDPR

Notes

1 Article 24 of the Charter of Fundamental Rights of the European Union also acknowledges the attribution of fundamental rights to children: ‘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 in matters which concern them in an adequate manner, taking into account 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. ’. 1
2 Article 6 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 only if and to the extent that consent is given by or on behalf of the holder of parental responsibility over the child. Consent shall be given by a person who has legal capacity to act on behalf of the holder of parental responsibility over the child. Articles 6(1) and 7 GDPR on (the conditions for) consent. (2) Consent must be given freely and in such a manner that the child is not under any form of coercion. 3 The aim of this section is not to provide a full-blown analysis of Art 6 GDPR, but rather to focus on the reason 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 & Verdovd (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 See further Schermer, Custers, Van der Hof (2014) and Van der Hof (2017). 7 See Arts 4(11) and 7 GDPR on (the conditions for) consent. (2) Consent must be given freely and in such a manner that the child is not under any form of coercion. 8 See Arts 6(1) and 7 GDPR on (the conditions for) consent. (2) Consent must be given freely and in such a manner that the child is not under any form of coercion.
9 Pollach (2017).
10 J Koetsier, 40% of top-selling smartphone apps have no privacy policy, Forbes (24 March 2016), https://www.forbes.com/sites/roberts/2016/03/24/40-pop-selling-smartphone-apps-have-no-privacy-policy/57ke4mber7a1-#57ke4mber7a1-#.
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 3 UN CRC), which may entail that older children must be let a sufficient amount of freedom and independence from their parents or caregivers.
12 Shmatikov, Blich-Pragt (2013).
The importance of privacy by design and data protection impact assessments in strengthening protection of children’s personal data under the GDPR

30 For the purpose of our argumentation here, we will assume that giving guidance and direction to children is dependent on their evolving capacities.

35 See for exceptions Art 17(3) GDPR.

36 The text reads as follows: ‘That right is relevant in particular where processing is ‘likely to result in a high risk’ for the data subject, being 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) on a large scale, at least in proportion to the amount of personal data processed, involving sensitive personal data or data relating to criminal convictions and offences referred to in Article 10; or (c) on a systematic basis to evaluate certain aspects concerning the 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 22 GDPR).

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 the right Fundamentalassigndroit [Federal Constitutional Court] December 15, 1983, 65 BVerfGE 1 (2009) (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 For a discussion of privacy by design strategies see Google Ads are understood only by a minority of 12-15s; see families.google.com/familylink/faq/.

41 Recital 91 GDPR.

42 Article 29 Data Protection Working Party (2017) Guidelines on Data Protection Impact Assessment (GDPIA) and determining whether processing is ‘likely to result in a high risk’ for the data subject, being 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) on a large scale, at least in proportion to the amount of personal data processed, involving sensitive personal data or data relating to criminal convictions and offences referred to in Article 10; or (c) on a systematic basis to evaluate certain aspects concerning the 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 22 GDPR).


44 Note, however, that in Recital 75 in relation to the responsibility of the controller concerning children’s personal data, it is stated that ‘the controller shall be responsible for the protection of personal data relating to criminal convictions and offences referred to in Article 10, or (c) a systematic basis to evaluate certain aspects concerning the 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’.

45 Article 29 Data Protection Working Party (2017) Guidelines on Data Protection Impact Assessment (GDPIA) and determining whether processing is ‘likely to result in a high risk’ for the data subject, being 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) on a large scale, at least in proportion to the amount of personal data processed, involving sensitive personal data or data relating to criminal convictions and offences referred to in Article 10; or (c) on a systematic basis to evaluate certain aspects concerning the 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’.

46 Article 29 Data Protection Working Party (2017) Guidelines on Data Protection Impact Assessment (GDPIA) and determining whether processing is ‘likely to result in a high risk’ for the data subject, being 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) on a large scale, at least in proportion to the amount of personal data processed, involving sensitive personal data or data relating to criminal convictions and offences referred to in Article 10; or (c) on a systematic basis to evaluate certain aspects concerning the 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’.


49 For an interdisciplinary discussion concerning the necessity of profiling in children’s social contexts see Goetz et al (2015).
The importance of privacy by design and data protection impact assessments in strengthening protection of children’s personal data under the GDPR


- 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.

- Ibid.


- Ibid.

- Information Commissioner’s Office (2017).


- Ibid.

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

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 (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 out4, these internet users are often operating in a world that was not originally designed with them in mind and still fail to recognise them as key players.

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.

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 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 to 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.5 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 to grasp for the average individual, let alone comprehensible by child users.4

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 Ofcom5 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 resolutions6 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 20157 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 63 per cent of the sites and apps examined had collected children’s personal data, only 22 per cent tailored their data protection communications to children.

“Children merit specific protection”

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(2) of the GDPR, with Article 12.3 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 of the 1995 Data Protection Directive) and is set out in Articles 13 and 14. 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. In文旅 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 of the GDPR, which makes it clear that because the context of children’s specific protection, any information and communication concerning the processing of a child’s data should be in 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 practice for data controllers, such as the tech giants that run the social media, gaming, messaging and photo-sharing websites and apps that are popular with children? The answer varies and is bound up in one of the most important phrases in Article 12, namely the requirement in Article 12.1 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 and statements have traditionally been expressed in lengthy legalistic and specialist terms which can be difficult to grasp for the average individual, let alone comprehensible by child users.4

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 Ofcom5 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 resolutions6 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 20157 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 63 per cent of the sites and apps examined had collected children’s personal data, only 22 per cent tailored their data protection communications to children.

“Children merit specific protection”

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(2) of the GDPR, with Article 12.3 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 of the 1995 Data Protection Directive) and is set out in Articles 13 and 14. 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. In文旅 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 of the GDPR, which makes it clear that because the context of children’s specific protection, any information and communication concerning the processing of a child’s data should be in 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 practice for data controllers, such as the tech giants that run the social media, gaming, messaging and photo-sharing websites and apps that are popular with children? The answer varies and is bound up in one of the most important phrases in Article 12, namely the requirement in Article 12.1 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 communications 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, infographics 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 used by the child. This necessarily means no ‘legalese’, no technical terms, jargon or ambiguous phrases that are out of the reach 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 in ways that children can understand. Privacy education is essential to ensuring 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 information is telling them, then the risk is that they will seize 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 report27 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 submissions26 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 such as 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.28

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, for many children, they are growing up in a world where children – and indeed adults – expect and seek out transparent information from those organisations who collect, use and profit from personal data.29 So children, and adults, can make smart, informed choices about how, and when, and to what extent, they choose to share their most invaluable asset – their personal data.
The transparency challenge: making children aware of their data protection rights and the risks online

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 Sustaining Rights’.


4 See, for example, the IPEPC bulletin ‘Cyber safety is the child protection issue of our time’ issued by the IPEPC (IPEPC/Childline) on 25 October 2017.

5 The right to respect for private and family life (Art 8) and the right to Protection of Personal Data (Art 6) are fundamental rights under the Charter of Fundamental Rights of the European Union.

6 Recital 18 of the General Data Protection Regulation: ‘Children... 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 and use of personal data with regard to children when using services offered directly to a child.’


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 For example, the IPEPC bulletin ‘Cyber safety is the child protection issue of our time’ issued by the IPEPC (IPEPC/Childline) on 25 October 2017.

10 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 Sustaining Rights’.

11 See, for example, the IPEPC bulletin ‘Cyber safety is the child protection issue of our time’ issued by the IPEPC (IPEPC/Childline) on 25 October 2017.

12 Article 13 of the GDPR: ‘Information to be provided where personal data are collected from the data subject.’

13 Article 11.2, Recital 18 of the General Data Protection Regulation: ‘Children... 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 and use of personal data with regard to children when using services offered directly to a child.’

14 Article 12 of the GDPR: ‘The controller shall inform the data subject... using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided 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 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 a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.’

15 Article 13 of the GDPR: Information to be provided where personal data are collected from the data subject.

16 Article 11.4 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 processing of action 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 are processed and to whom they are disclosed. In the context 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.’

16 Article 11.4 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 processing of action 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 are processed and to whom they are disclosed. In the context 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.’

17 Article 11.4 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 processing of action 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 are processed and to whom they are disclosed. In the context 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.’


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 processing of action 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 are processed and to whom they are disclosed. In the context 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 in 15 above.

21 See, for example, the International Conference on Data Protection and Privacy Commissioners, ‘Children’s Privacy Protection Commissioner: Process Committee’ (9 February 2017).

22 See, for example, Twitter ‘@ISPCC’ @ISPCC, ‘Covid-19: children’s rights are protected in healthcare’ (28 March 2020).

23 See, for example, the IPEPC bulletin ‘Cyber safety is the child protection issue of our time’ issued by the IPEPC (IPEPC/Childline) on 25 October 2017.

24 See, for example, the IPEPC bulletin ‘Cyber safety is the child protection issue of our time’ issued by the IPEPC (IPEPC/Childline) on 25 October 2017.

25 See, for example, the IPEPC bulletin ‘Cyber safety is the child protection issue of our time’ issued by the IPEPC (IPEPC/Childline) on 25 October 2017.

26 See, for example, the IPEPC bulletin ‘Cyber safety is the child protection issue of our time’ issued by the IPEPC (IPEPC/Childline) on 25 October 2017.

27 See, for example, the IPEPC bulletin ‘Cyber safety is the child protection issue of our time’ issued by the IPEPC (IPEPC/Childline) on 25 October 2017.

28 See, for example, the IPEPC bulletin ‘Cyber safety is the child protection issue of our time’ issued by the IPEPC (IPEPC/Childline) on 25 October 2017.

29 See, for example, the IPEPC bulletin ‘Cyber safety is the child protection issue of our time’ issued by the IPEPC (IPEPC/Childline) on 25 October 2017.

30 See, for example, the IPEPC bulletin ‘Cyber safety is the child protection issue of our time’ issued by the IPEPC (IPEPC/Childline) on 25 October 2017.

31 See, for example, the IPEPC bulletin ‘Cyber safety is the child protection issue of our time’ issued by the IPEPC (IPEPC/Childline) on 25 October 2017.

32 See, for example, the IPEPC bulletin ‘Cyber safety is the child protection issue of our time’ issued by the IPEPC (IPEPC/Childline) on 25 October 2017.

33 See, for example, the IPEPC bulletin ‘Cyber safety is the child protection issue of our time’ issued by the IPEPC (IPEPC/Childline) on 25 October 2017.
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 Nicol in 2017 – both formerly of SBH 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 on how 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 Communications List, has provided a welcome and refreshing development

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 Nicol in 2017 – both formerly of SBH 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 on how 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 Communications List, has provided a welcome and refreshing development

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 latter category also included proposals which would require primary legislation, which would be a matter for Parliament rather than the Judiciary. It was pleasing 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 (PMP), 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 who 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 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

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 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 defama-
tion 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 photos 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, 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 *Oswaa v Jackson* (C-281/2002) [2003] QB 801 and *Maltex 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 (as internal to the United Kingdom).

By contrast, in *Oswaa v Jackson and Maltex* 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

**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 photos 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, 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 *Oswaa v Jackson* (C-281/2002) [2003] QB 801 and *Maltex 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 (as internal to the United Kingdom).

By contrast, in *Oswaa v Jackson and Maltex* 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 compe-
ting courts. It was thus not easy to see why the regula-
tion could be read as requiring that the competing claims
ever 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 juris-
diction internally as between the various consti-
tuent ‘nations’ or parts of the UK was governed
by section 16 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
concerning a complaint of publication “by a person
domiciled in one part may be said in the courts for
the place where the harmful act occurred (or may
occur). There were therefore two issues to which the
doctrine of forum non conveniens should be applied 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 – clashing in respect of damages actually
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.

It was appropriate to have in mind the principles
expressed in Shevill v Press Alliance [1995] 2 AC
18. Where a libel was published in several jurisdic-
tions, a litigant would be entitled to address issues
concerning a claim 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 ‘connec-
ting 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
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 specific exceptions,
etablished the fundamental test
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

other jurisdictions did not entail any issue of compe-
ting courts. It was thus not easy to see why the regula-
tion could be read as requiring that the competing claims
were 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 juris-
diction internally as between the various consti-
tuent ‘nations’ or parts of the UK was governed
by section 16 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
concerning a complaint of publication “by a person
domiciled in one part may be said in the courts for
the place where the harmful act occurred (or may
occur). There were therefore two issues to which the
doctrine of forum non conveniens should be applied 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 – clashing in respect of damages actually
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.

It was appropriate to have in mind the principles
expressed in Shevill v Press Alliance [1995] 2 AC
18. Where a libel was published in several jurisdic-
tions, a litigant would be entitled to address issues
concerning a claim 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 ‘connec-
ting 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
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 specific exceptions,
etablished the fundamental test
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

other jurisdictions did not entail any issue of compe-
ting courts. It was thus not easy to see why the regula-
tion could be read as requiring that the competing claims
were 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 juris-
diction internally as between the various consti-
tuent ‘nations’ or parts of the UK was governed
by section 16 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
concerning a complaint of publication “by a person
domiciled in one part may be said in the courts for
the place where the harmful act occurred (or may
occur). There were therefore two issues to which the
doctrine of forum non conveniens should be applied 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 – clashing in respect of damages actually
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.

It was appropriate to have in mind the principles
expressed in Shevill v Press Alliance [1995] 2 AC
18. Where a libel was published in several jurisdic-
tions, a litigant would be entitled to address issues
concerning a claim 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 ‘connec-
ting 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
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 specific exceptions,
etablished the fundamental test
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 those 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 Schedule 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 a plausible task to show that non-substantial justice required that the case remain in England and the stay was granted.

So far as a claim for global damages 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 Schepel v Press Alliance [1995] 2 AC 17, 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 draw a subtle, novel model of discretion – 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 one where there was room for the application of forum non conveniens within the Member State, and moreover that Parliament had approached matters in parallel to those under the Recital Regulation – including those under Schedule 4. Schepel 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 recognize 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 necessary to consider both 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

GH v Persons Unknown (Responsible for the Publication of Webpages) [2017] EWHC 3360 (QB) before Mr Justice Warby

The claimant 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 information. The claimant maintained, as part of her claim, and as an action without notice to the defendant for an interim disclosure order on persons unknown, coupled with a stay of proceedings. The claimant also maintained, as part of her argument in support of an injunction, that some of them were both defamatory and untrue.

The claimant said ‘persons unknown’, coupled with descriptive wording referring to two worldwide 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’ as the natural forum for bringing 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.

Harassment and interim non-disclosure order on persons unknown

GH v Persons Unknown (Responsible for the Publication of Webpages) [2017] EWHC 3360 (QB) before Mr Justice Warby

The claimant 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 information. The claimant maintained, as part of her claim, and as an action without notice to the defendant for an interim disclosure order on persons unknown, coupled with a stay of proceedings. The claimant also maintained, as part of her argument in support of an injunction, that some of them were both defamatory and untrue.

The claimant said ‘persons unknown’, coupled with descriptive wording referring to two worldwide 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’ as the natural forum for bringing 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.

GH v Persons Unknown (Responsible for the Publication of Webpages) [2017] EWHC 3360 (QB) before Mr Justice Warby

The claimant 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 information. The claimant maintained, as part of her claim, and as an action without notice to the defendant for an interim disclosure order on persons unknown, coupled with a stay of proceedings. The claimant also maintained, as part of her argument in support of an injunction, that some of them were both defamatory and untrue.

The claimant said ‘persons unknown’, coupled with descriptive wording referring to two worldwide 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’ as the natural forum for bringing 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 clearly sensitive nature, including information about sexual life, 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 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 publishing 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 in the review of the day. The review contained a description of the claimant, her attributes, the flat, and what the two of them had said to each other. There was no 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 private 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 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 in the review of the day. The review contained a description of the claimant, her attributes, the flat, and what the two of them had said to each other. There was no 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 private 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 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 publishing 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 in the review of the day. The review contained a description of the claimant, her attributes, the flat, and what the two of them had said to each other. There was no 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 private 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.
about the claimant. The fact that some such informa-
tion was false did not undermine the claim. It tended
rather to support it. The fact that some of the informa-
tion happened to be defamatory should not under-
mine 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 under-
mine 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 conside-
ration 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.

Recent Developments