Children: a special case for privacy?

CHILDREN: A SPECIAL CASE FOR PRIVACY?

As the world absorbs the impact of Europe's GDPR, **SONIA LIVINGSTONE** asks if data protection can work for children's privacy – or if a wider view is needed for all ages of user

High-profile data breaches, some involving children's personal data, resulting from insufficient protections built into the emerging generation of smart devices, have raised urgent questions about whether children's privacy is sufficiently valued in personal data regulation. The rapid growth in technologies and services whose business model is based on personal data collection and analysis – from social network services and personalised marketing to learning analytics, wearables and home assistants – raises yet further concerns. While it is likely that the technology industry will get better at preventing hacks, it is equally likely to get better at harnessing the value – mainly for commercial but sometimes public benefit – of the "datafication" of seemingly every dimension of people's lives.

In Europe, the General Data Protection Regulation (GDPR) became applicable on 25 May 2018. Several years in the making, it has been designed as a concerted, holistic and unifying effort to regulate personal data at a time when data has rapidly become "the new oil" for public, private and third sector organisations. As European commissioner for justice, consumers and gender equality, Věra Jourová, put it: "Privacy is much more than just a luxury. It is a necessity." And so, therefore, is its protection for all citizens, since "personal data protection is a fundamental right in the EU".

Until recently, talk of the GDPR was rather esoteric, confined to deliberations among legal, regulatory and technical experts. But spring 2018 saw the public in Europe and beyond bombarded with demands to update social media privacy settings and respond to a flood of (sometimes inappropriate) email requests to re-consent to marketing and mailing lists, all the while hearing in the mass media about scandals about political microtargeting (especially based on personal data illegally collected via Facebook by Cambridge Analytica) or fights over the so-called "digital age of consent", as contested across Europe, most notably in Ireland and France. All this has brought a heightened awareness (and uncertainty), including among many parents and children, though doubtless unequally distributed, of the new privacy regulation and, relatedly, the ways in which personal data may be used or misused.

Public awareness matters, not just because of its potential to trigger action by policymakers but because the public is a key stakeholder in the regulation of personal data. Aggregated together, public actions and choices in the digital environment have significant consequences for politics, markets, regulatory effectiveness, equity and the direction of socio-technical change.

> **"Children's voices are particularly absent, rarely consulted or included in deliberations."**

But ordinary people's voices are too little heard in multistakeholder deliberations, notwithstanding the legitimacy of their interests. Children's voices are particularly absent, being rarely consulted or included in national or international deliberations, notwithstanding that they constitute a valued and valuable segment of internet users, being often pioneering in their adoption of new services and experimental in their digital practices, yet not easily incorporated into considerations of the "population" or the "public" or "users" as a generality. This is a problematic omission, because child welfare advocates believe it is crucial to take steps to ensure that children benefit from the wealth of opportunities enabled by the internet, now and in the future, without being simultaneously exploited, surveilled or "monetised".

Already there is a host of uncertainties regarding interpretation and implementation of the GDPR, with stakeholders responding in diverse and sometimes misguided ways as they seek to comply.[1] As Britain's information commissioner observed, while "the proper use of personal data can achieve

remarkable things", it is not before but after 25 May that "the real journey begins", with "a lot of work to be done along the way".[2]

In this article, I identify some problematic actions, unresolved challenges and unintended consequences of the GDPR, focusing on children's privacy. I conclude that while the new regulation is likely to improve children's data protection insofar as children are treated like other internet users, it may make matters worse insofar as they are singled out for special treatment as children.

HOW DOES THE GDPR SET OUT TO IMPROVE THE PROTECTION OF CHILDREN'S PRIVACY?

Widely billed as a far-ranging, even radical effort to give European citizens greater control and choice over the uses of their personal data, through privacy-by-design, privacy-by-default and governance mechanisms, the whole GDPR is too complex to summarise here (see instead the guide from the UK Information Commissioner's Office, ICO).[3] Suffice to say that, as regards the information relating to identifiable persons, the legislation obliges data controllers and processors:

- To process personal data lawfully, securely and fairly, in ways that are transparent to and comprehensible by data subjects
- To collect and process data and, if they engage in profiling, to do so in ways which are limited to specific, explicit and legitimate purposes, taking account of special provisions for the treatment of "sensitive" data (e.g. political views, sexual orientation, medical records or biometric data)
- To facilitate individuals' rights to access, rectify, erase and retrieve their personal data under specific circumstances
- To meet a host of governance requirements to ensure compliance, informed by the conduct of risk-related impact assessments.

These obligations are designed to benefit individuals and organisations alike. They will surely, therefore, benefit children also. However, the GDPR makes some additional requirements in respect of children's data, for reasons set out in Recital 38:

"Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child."

This rationale contains much of merit, not least as it is the first time that the EU has considered children's data as specifically worthy of protection. Yet it raises some conceptual and practical issues that should, ideally, be grounded in a stronger empirical basis than exists at present. These concern, first, children's media literacy (what is their awareness of the risks associated with personal data processing and of their rights in this regard?), second, the harm that the regulation seeks to avoid (especially that relating to commercial profiling), and third the implied nature of family relations (parental responsibility, parental media literacy, children's need for privacy from parents, and the readiness of families to act as assumed by the regulation).

The messy world of real families – who may lack time, share devices, have secrets or conflict with each other – fits ill with the GDPR's implied world of conscientious parents and dutiful children. This has proved particularly fraught in relation to privacy, since it may be critical for a child's wellbeing that their access to preventive or counselling services does not depend on parental consent; yet such a protection is only mentioned in Recital 38, and not included in an article (though in the UK's Data Protection Act, a specific clause was added to address this).

Although (just) a recital rather than an actual article in the GDPR, Recital 38 informs the "higher threshold of protection for the processing of children's data"[4] specified in Article 8, which states that:

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member states may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

In a recent Media Policy Project roundtable at the London School of Economics and Political Science, it emerged that Article 8 leaves scope for interpretation, indeed confusion, regarding the definition of an information society service (ISS), the meaning of the phrase "directly offered to a child", and what higher threshold of protection is provided over and above the requirement of parental consent.[1] Also contested in the GDPR more generally are the rules on profiling children, how decisions are to be made regarding the legal basis for processing (including, crucially, when it should be based on consent), how parental consent is to be verified, and when and how risk-based impact assessments should be conducted (including how they should attend to intended or actual users). Further, it is not clear how, in practice, children can claim their rights or seek redress when their privacy is infringed unless, perhaps, the mechanisms specified in the UN Convention on the Rights of the Child (UNCRC Articles 43-54) will be made available to them in this context or, alternatively, national data protection authorities will resource specialised channels both to enhance children's data literacy and to find solutions to problems children encounter.

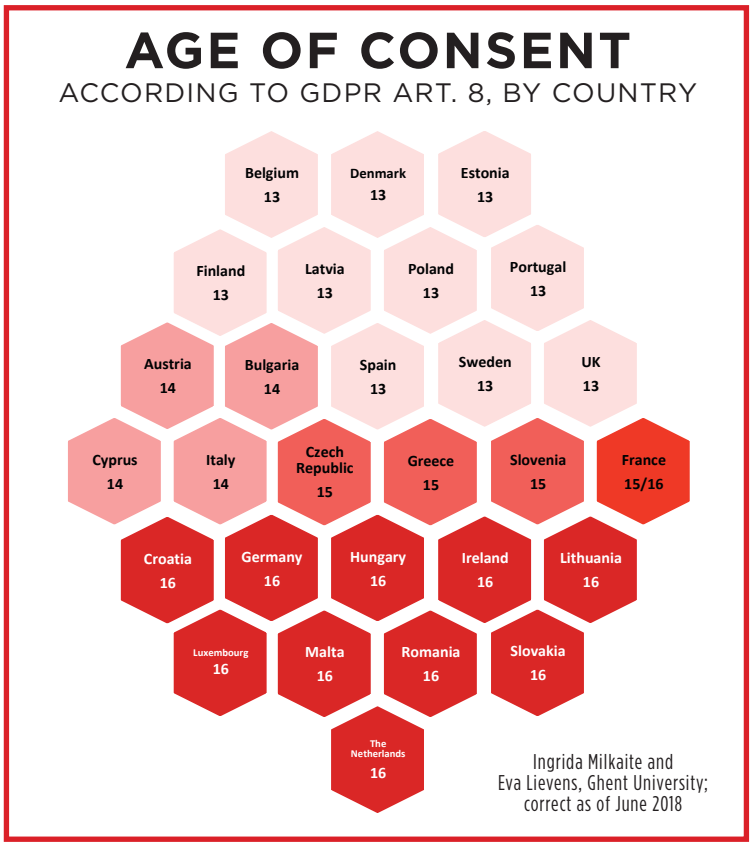
"It is not clear how children can claim their rights or seek redress when their privacy is infringed."

CONTESTATION AND CONFUSION OVER THE 'DIGITAL AGE OF CONSENT'

During 2017/18, Article 8 of the GDPR attracted considerable attention among the child rights, safety and welfare community, sometimes spilling over into the public domain, regarding children's rights to protection and privacy online, on the one hand, but also to participation, information and expression online, on the other (all these being rights established in the UNCRC). Since a higher age of consent (if not routinely flouted) would favour protection rights and a lower age would favour participation rights, the stakeholder community has been divided in trying to determine where and how to strike the optimal balance.

Adding to the heated nature of this debate is the fact that, although the GDPR was designed to protect users' personal data and privacy, personal data mediates not only commercial but also interpersonal interactions online and, thus, the potential harms at issue are not only commercial but also interpersonal (such as bullying, harassment, hate, grooming); hence the efforts of those on the protectionist side of the debate to raise the age at which children can use online services. Hence, too, the interest of the child safety community in whether and how it will now be the GDPR rather than safety specific regulation that, for instance, specifies the age at which children can access services, the conditions under which children can request removal of problematic content ("the right to be forgotten") or the requirement for parental oversight (via consent mechanisms) as well as, more broadly, the requirement on platforms to conduct risk impact assessments.

This debate played out differently across European member states, resulting in all possible



ages between 13 and 16 being chosen as the "digital age of consent" (see figure, page 20). It appears that these national decisions made little reference either to research evidence regarding children's developing media literacy during adolescence or to direct consultation with children or child advocates regarding their best interests (UNCRC Article 3), although internationally all countries apart from the US have ratified the UNCRC in which Article 12 states that the child has a right to be heard "in all matters affecting them".

So why such different decisions about the age of consent? Do we imagine that children mature at different rates across Europe? There is little evidence for this. It seems more likely that European countries vary culturally and politically in how they weigh children's rights to protection and participation.[5] The result is a notable lack of harmonisation across Europe, affecting both children and businesses, along with some unresolved cross-border issues.

In the UK, a hard-fought debate over the Data Protection Bill (now, Act) in the House of Lords and a tacit government defeat resulted in an interesting compromise – namely, agreeing the age of 13 (to support teenagers' participation rights) for Article 8 but additionally requiring an "age-appropriate design code" for online providers for all children – as is consistent with the UNCRC Article 1 definition of a "child" as all those under 18 years old. Just how privacy-by-design, itself a principle promoted by the GDPR, can be implemented by a service provider who may not know whether a user is a child or whether they are below a certain age threshold, remains to be seen.

The UK ICO will now produce and enforce a code with distinct provisions for children according to their age, to ensure that providers fulfil the GDPR's requirements for transparency and interpretability (or legibility) of terms and conditions, use of risk impact assessments, mechanisms for the right to withdraw consent and erase data, and for support and redress. Since there is a group able to use online services without parental consent (being 13+) yet are still in need of child protection (being under 18), this places a particular responsibility on service providers (and on enforcement of the ICO's code).

Matters should be simpler for the under 13s, insofar as both providers and parents are responsible for their internet use. But since many children use services underage (51% of UK children have a social media profile by the age of 12, despite most platforms setting a minimum age of 13),[6] and since many providers simply require a self-declaration of age, the unintended consequence of the regulation is that under 13s may appear to providers as adults, so missing out on child- (or teen-) specific protections.

The Article 29 Data Protection Working Party says: *"Although the need to undertake reasonable efforts to verify age is not explicit in the GDPR it is implicitly required, for if a child gives consent while not old enough to provide valid consent on their own behalf, then this will render the processing of data unlawful."*[7] This raises some interesting questions about those services – including the most popular social media companies – that assume the self-declared age is valid, especially when the evidence suggests that underage users experience harm online.[5]

During April 2018, it became apparent that much of the fuss regarding Article 8 was due to a widespread misapprehension that this specifies a "digital age of consent" relevant to children's access to all online services, rather than only those where an information society service is being directly offered to a child and where the processing of personal data is based on consent. In other words, the prefatory phrase, "Where point (a) of Article 6(1) applies", was widely missed. GDPR Article 6(1) states the six lawful bases for processing personal data (of which consent, point (a), is but one, with relevant others including what is necessary for the performance of a contract, point (b), and the legitimate interests of the data controller, point (f)).

Such a confusion can be traced to the two meanings of consent – first, the requirement on the data subject to consent to a service (as when ticking "I agree" to terms and conditions) and, second, the data controller's decision to rely on consent as the lawful basis for processing personal data. This confusion will surely extend to users who are unlikely to distinguish consenting to a service to gain access to it (for instance, when signing up to Facebook) from the lawful basis on which their data is processed.

In the run up to 25 May 2018, as users were required to update their privacy settings, it became apparent that not only have different member states adopted different approaches as regards children, but so too have different providers:

- Facebook appears to be keeping the age of 13 as the minimum to use the service (as long required by COPPA – the US Children's Online Privacy Protection Act 1998) by processing personal data on the lawful basis of contract (for adults and teenagers if permitted legally to make a contract in their country), and on the basis of legitimate interest (for teens 13+ not permitted to make a contract). Additionally, it processes sensitive data and profiles users (as defined by GDPR Article 9) on the basis of consent (thus applying EU member states' different ages of consent for Article 8 only in relation to sensitive data and targeted advertising)[8]
- WhatsApp (owned by Facebook but taking a different approach) announced that it would henceforth restrict its services in Europe to those aged 16+ (based on a simple self-declaration of age), thus obviating the need to collect information about age and so enabling data minimisation[9]
- Instagram (also owned by Facebook) began asking its users if they were 18+, stating this affects the use of their data for targeting adverts (i.e. profiling), though it also has implications for the safety provisions applied for 13-17 year olds
- Twitter invited users (at least in the UK) to agree that they're over 13 years of age, also removing some users believed to have been under 13 when they first signed up to the service.

The implications for children now deemed underage – in the UK, 55% of 12-15 year olds use

Facebook, 43% use Instagram and 24% use WhatsApp[6] – are only now emerging. It would be problematic if children were to be faced with the decision either to lose access to a service they value or to lie about their age to retain access (and, thereby, find themselves treated as an adult rather than benefiting from the protections due to them as a child). The position for their parents is also problematic, for they would surely wish their child could engage honestly online while in receipt of appropriate protections but, instead, are likely to find themselves complicit in various workarounds so their child can access services.

The legal implications are also unclear. For instance, whether Facebook's decision to process personal data partially on the basis of legitimate interests, itself unexpected to many, may prove unsustainable given the upcoming revision of the EU's e-privacy directive, in which legitimate interest is currently not foreseen as a ground for tracking or profiling.[10] Then there are the legal challenges, such as that brought by Austrian privacy activist Max Schrems[11] – on the grounds that the all-or-nothing consent required by key companies constitutes illegal "bundling" and "forced consent",[12] contra the intention of the GDPR to empower internet users with transparent, graduated and genuine choices in the uses of their personal data.

Last, it's noteworthy that UNICEF asserts: "Although other legal bases for data processing may exist, obtaining free and informed consent is the approach most consistent with children's rights."[13] This would mean, however, that the age of consent shown in the figure on page 20 would apply to teenagers' use of all of a social networking service, as originally expected by many, in most countries, thereby protecting them but also restricting their participation for longer.

WHAT IF WE TAKE INTO ACCOUNT RESEARCH WITH CHILDREN AND PARENTS?

There are many questions that have been – and should yet be – researched regarding the views and understandings of children and parents as regards the complex and changing digital environment in general and privacy in particular. Here I select just two indicative sources of evidence regarding children's developing competence, both of which suggest the inadequacy of a regulatory approach that seeks to protect children's data via implementation of a rigid age threshold.

Ofcom, the UK regulator, asked a nationally representative sample of UK children to respond to the statement, "When you use Google to look for something online, you are given a list of websites in the Google results page", and to choose from the answer options shown in the figure below, with the top green line being the "right" answer.[14] The results suggest that with increasing age, children gain the commercial literacy to realise that some but not all search engine results can be trusted. However, there is no strong increase in understanding through the early teens, the main gain being among younger children.

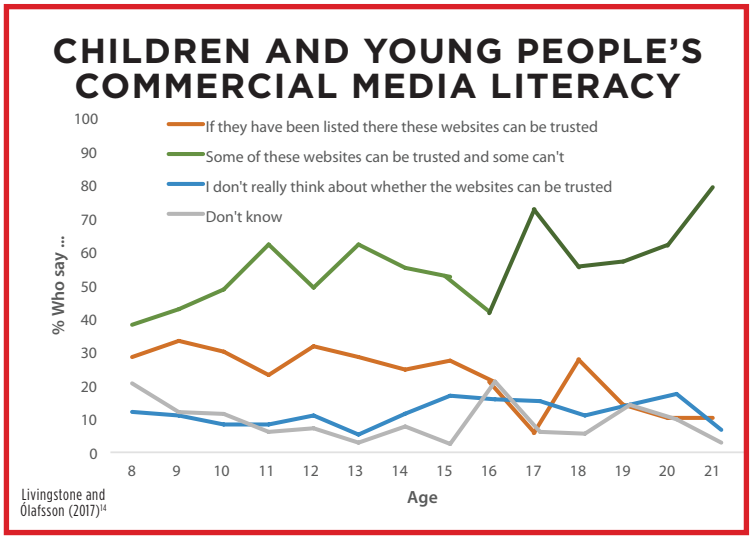
One might conclude that 13 year olds are almost as literate as 16 year olds (it being younger internet users who lack commercial literacy). Development in understanding thereafter (ages 16-21 and, using other indicators, for older ages also) is variable, offering little evidence of a magic switch in maturity when children turn 13 (or 16) and so hardly justifying setting an age threshold as a "bright line rule"[15] by which those in need of greater protection can be identified.

The Parenting for a Digital Future project asked a nationally representative sample of UK parents to answer the question, "At what age do you think your child will be or was old enough to make their own decisions about the websites or apps they use?" This is a view of their child's "age of independence", as they were asked to assess their child's maturity rather than to consider the legal question of consent. The average age chosen by parents of children aged 0-17 was 13, although the most common answer (the mode) was 16. But as shown in the figure on page 23, what was more striking was that parents' views vary greatly according to the age of their child.[16]

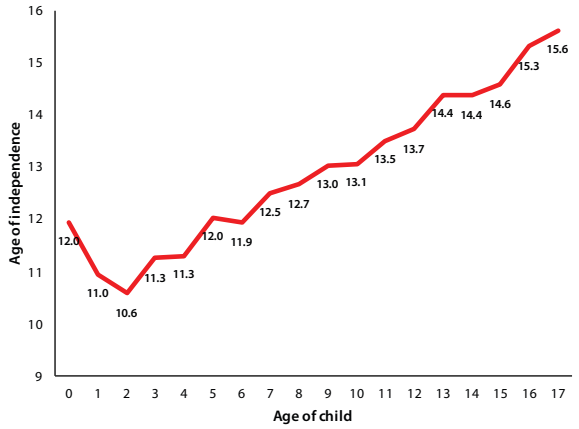
So, while parents of young children consider 13 a reasonable age, parents of teenagers take a different view, clearly thinking that they should stay involved in their children's decisions about internet use. Parents of teenagers aged 13 to 17, therefore, think that the UK government's chosen age of consent of 13 is too young: 79% of this group think their child should be at least 14 before making decisions about whether to consent to online services, with the ideal age of consent averaging 15. Also interesting was the finding that more digitally skilled parents such as those able to create their own websites or videos and parents who have had negative online experiences also favoured an older age of consent.

ADVANCING CHILDREN'S RIGHTS IN THE DIGITAL AGE

In a digital age in which children's every communication and action is tracked and recorded, it is becoming clear that privacy (UNCRC Article 16) is vital to children's "best interests" (UNCRC Article 3) and their opportunity to develop to their full potential (Article 29). Increasingly, digital privacy mediates children's negative rights – the avoidance



PARENTS' VIEWS ON THE AGE OF INDEPENDENCE OF THEIR CHILD



Livingstone and Ólafsson (2018)[16]

of harm, insofar as infringements of privacy place a child at risk, and also their positive rights, "insofar as it is part and parcel of individual autonomy, a necessary precondition of participation".[17] With the ink not yet dry on the GDPR nor on the policies of public and private sector organisations designed to implement it, it is too soon to be sure whether children's rights will be fulfilled or, at worst, undermined by a regulation that only partially takes account of their specific needs and circumstances.

At present, the lack of harmonisation across countries and services (itself counter to the EU's goal of easing the regulatory burden on businesses while improving clarity and accountability for users) combined with the practical ease of circumventing protections provided for those of different ages and continued legal uncertainties over implementation, is creating an unsatisfactory regulatory context.

In the future, it is possible that the public may make different choices in managing their privacy online as they gain what we might call "data literacy". This term has been variously defined by different disciplines[18] but should now capture not only a knowledge of data processing but also a critical understanding of data flows and the data lifecycle. But data literacy, like media literacy and other literacies, always depends on legibility: people cannot "read" or understand or responsibly engage with that which is illegible.

Hence the GDPR, and the "datafication" of society more generally, is accompanied not only by insistent calls for the mainstreaming of media literacy education and awareness-raising, but also for policymakers to enhance data controllers' public-facing mechanisms, including transparency, accountability and redress. Some of these requirements are built into the GDPR, but some must be engineered by the state, business or wider society to support, complement or enforce the implementation of the GDPR if personal data is to be protected effectively.

As with the canary in the coal mine, children often find themselves in the vanguard of digital innovation and their problematic experiences of privacy online turn out to indicate problems also significant for the wider population. After all, it is not only children who do not read or understand terms and conditions, not only children who are prepared to trade their personal data for free services, and not only children who struggle in practice to exercise their right to protect or retrieve or delete their data.

As I argued recently, one problem with the problem of treating children as a special subgroup is that this conjures a problematic normative vision of all other users as somehow invulnerable and invincible.[19] Not only is this wrong (for user vulnerabilities extend far beyond childhood) but, once provision has been made for some, further calls for special protection are likely.

In future, it may work better for data controllers to protect the rights (and limit the commercial exploitation) of all users than to try to identify children (and other vulnerable users) so as to treat them differently (not least because the very process of identifying children may undermine the principle of data minimisation which protects their privacy). Designing systems for the minority of users who are white, educated, middle-aged, able-bodied and resilient may prove unwise and expensive in the long run, as well as counter to many people's rights.

In other words, it may be that a governance regime that treats children fairly will be one that works for everyone, and it may also prove more efficient and effective than one that addresses (some) adults' needs first and then tacks on children's as an afterthought.

SONIA LIVINGSTONE *is a professor in the Department of Media and Communications at the London School of Economics and Political Science. She is the author of 20 books on children's online opportunities and risks, advises on children's rights in digital environments, directs the projects Global Kids Online and Parenting for a Digital Future, and founded the EU Kids Online research network. See www.sonialivingstone.net*

Thanks to John Carr, Jeff Chester, Stephan Dreyer, Eva Lievens and Mariya Stoilova for comments on this article.

REFERENCES **1** Livingstone S, Yoo D (2018). What does the European General Data Protection Regulation mean for children in the UK? Report on an LSE Media Policy Project roundtable. LSE Media Policy Project. bit.ly/2yuWJmW **2** Denham E (2018). Opening speech to the Data Protection Practitioners' Conference. Manchester. bit.ly/2saRX7s **3** Information Commissioner's Office (2018). Guide to the General Data Protection Regulation (GDPR). bit.ly/2A10ayF **4** Centre for Information Policy Leadership (2018). White paper: GDRP implementation in respect of children's data and consent. bit.ly/2FIlhxJ **5** Livingstone S et al. (Eds) (2012). Children, Risk and Safety Online: Research and policy challenges in comparative perspective. Policy Press. **6** Ofcom (2017). Children and parents: media use and attitudes report 2017. bit.ly/2BPfVKb **7** Article 29 Data Protection Working Party (2018). Guidelines on consent under Regulation 2016/679, as last revised and adopted on 10 April 2018. bit.ly/2HTXFIE **8** Facebook/Instagram legal bases. bit.ly/2tgQi1D **9** As for Facebook and Instagram, WhatsApp's privacy policy documents a reliance on a mix of lawful bases for processing (contract, consent and legitimate interests). bit.ly/2teKyFx **10** Lee P (2018). GDPR + e-Privacy = :-(bit.ly/2K88n8F **11** Brandom R (2018). Facebook and Google hit with $8.8 billion in lawsuits on day one of GDPR. The Verge, 25 May. bit.ly/2sbG3dH **12** noyb (2018). GDPR: noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook. bit.ly/2H1e8CB **13** UNICEF (2018). Children's online privacy and freedom of expression: Industry toolkit. bit.ly/2JSnTJA **14** Livingstone S, Ólafsson K (2017). Children's commercial media literacy: new evidence relevant to UK policy decisions regarding the General Data Protection Regulation. bit.ly/2tgQXjD **15** Macenaite M (2017). From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. New Media & Society 19 (5): 1–15. **16** Livingstone S, Ólafsson K (2018). When do parents think their child is ready to use the internet independently? Parenting for a Digital Future: Survey Report 2. LSE. eprints.lse.ac.uk/87953 **17** Lievens E et al. (2018). Children's rights and digital technologies. In: Liefaard T, Kilkelly U (Eds.) International Human Rights. International Children's Rights Law. eprints.lse.ac.uk/84871 **18** Acker A, Bowler L (2018). Youth data literacy: Teen perspectives on data created with social media and mobile devices. 51st Hawaii International Conference on System Sciences. bit.ly/2Md6Cr9 **19** Livingstone S, Third A (2017). Children and young people's rights in the digital age: An emerging agenda. New Media & Society, 19 (5): 657–70. eprints.lse.ac.uk/68759