Protecting children's rights in the modern age

Hannah Heilbuth from the University of Nottingham reports on a conference session that considered different approaches to protecting children's data rights.

The protection of children's data and privacy rights could very well be the most meaningful and unified of global priorities in the data protection community. If it takes a village to raise a child then surely, it takes a collective effort to protect our children's data rights.

At *PL&B's* 37th Annual International Conference, *Rachel Masterton* (Deputy Commissioner at the Data Protection Authority of Guernsey), *Paul Lavery* (A partner at the Irish law firm McCann Fitzgerald) and *Timothy Ma* (Co-founder and Chief Legal Officer for the company k-ID) sat down to tackle this topic from three complementary angles.

The session began with panel Chair *Brent Homan* (Commissioner at the Data Protection Authority of Guernsey) reflecting on a recent report from OFCOM which found that a third of children between the ages of five and seven use social media unsupervised and that 24% of that age cohort own a smartphone. He also noted the troubling finding that only one third of parents polled knew the minimum age requirement for most social media. He then handed over to the panellists to discuss the complex topic of children's data rights.

> Many developers struggle to navigate the complex jurisdictional regulatory landscape and keep up with legal developments.

Empowerment through education and outreach

Firstly, Masterton discussed the role of education in protecting children and how the Guernsey authority's education and outreach programmes have helped empower children and defend their rights. She explained that Guernsey law requires that their DPA promotes public awareness of data processing issues particularly when it comes to children and children's data. However, she emphasised that rather than simply talk about children, Guernsey's efforts have focused on bringing children and young people into the conversation and hearing their thoughts and perspective.

It was with this ethos in mind that the Guernsey DPA launched the Bijou Seeds project, a school programme focused on educating children about online safety.

The programme has been designed so that it does not become too intrusive. Rather than bombarding students with one overwhelming session with no follow up, students receive interventions every two years from Year Four through to Year Ten with new concepts and topics introduced based on their age group.

She described the programme's overall aim as focused on teaching young people "how valuable people's personal data is, why it must be protected and why we must treat others well."

The first stage of the programme introduces children aged 8-9 to the world of data through a children's book written by Kirsty Bougourd, an outreach officer for the Guernsey DPA. The book revolves around the adventures of a bear called Warro as she learns about the world of personal data, the challenges and risks children face and the rewards of treating personal information respectfully.

Last year, to celebrate World Children's Day, every child received a copy of the book and thanks to the small size of the jurisdiction, every school got a visit from the author.

When children reach the age of 10-11 years, project Bijou Seeds speaks to them again, this time linking the idea of data protection with the UN Convention of the Rights of the Child (CRC). The focus for this age group is on data sharing and making decisions about people based on personal data.

This is built on again two years later when the children are encouraged to discuss social media. At this point the children are 12-13 years old (the minimum age required for most social media platforms). This is also the stage when deepfakes and images are introduced with discussions about how cyberbullying could impact an individual.

Masterton then discussed the children's views on special category data. In her words "some children are bemused by the fact that something like their care status is not considered to be an item of special category data. To them, the fact that they've been on a care journey with the state and the fact that that could potentially influence decisions made about them in the future is very important." This reveals that what children regard as sensitive data may diverge from the opinion of adults such as regulators and parents. Given how strongly regulation impacts the lives of children, it really highlights the importance of engaging with them.

To further protect children, the DPA of Guernsey is now creating a Children's Framework inspired by the ICO's Children's Code to ensure that all processing of children's data aligns with the legislation and the UN Convention on the Rights of the Child (CRC), and is done in a way that puts the best interests of children at the heart of processing. This allows the Authority to build in messages about high-risk data such as care status which is not currently covered by legislation.

Masterton ended by emphasising that rather than stopping children from engaging with technology

because it's scary, adults must work to make sure technology is a positive, kind and healthy part of young people's experiences growing up.

Enforcement efforts

Next, Lavery discussed enforcement actions and guidance from the Irish Data Protection Commission (DPC) that have focused on protecting children's rights. When considering how to protect children's data, he started by reminding the audience that all of the GDPR obligations that apply when processing the personal data of adults such as privacy by design and default, also apply when processing children's data. In addition, the GDPR also mandates that processors provide specific enhanced protection for children as can be seen in articles 6, 8, 12 and 40.

He then focused on two recent investigations by the Irish DPC.

Firstly, in 2022, the Irish DPC concluded an inquiry into Instagram's processing of personal data relating to child users of the platform. The inquiry focused on the platform's public disclosure of the email addresses and/or phone numbers of children using Instagram's business account feature and the public-by-default setting for the personal Instagram accounts of children.

The Irish DPC determined that Instagram had failed to comply with several of its obligations under the GDPR including articles 5, 6, 12, 13, 24, 25 and 35. As a result, the DPC imposed a fine of €405 million and mandated a range of corrective measures.

Similarly, in 2023, the Irish DPC began an inquiry into how TikTok was processing child users' data. This focused on the public-by-default platform settings, the 'family pairing' feature, TikTok's age verification as part of the registration process and their approach to transparency.

As a result of their findings, the Irish DPC issued a reprimand, an order for TikTok to bring their data processing into compliance within three months of the decision, and a fine of €345 million. This was due to the findings that TikTok was in breach of Articles 5(1)(c), 24 and 25 of the GDPR. In particular, the family pairing feature was found to not be secure as it allowed adults who were not the parent or guardian to link their account to the child user's account.

Although the DPC did acknowledge that age verification is challenging, they found against TikTok because they felt that insufficient attention was being paid to the risk of under 13s trying to access the platform. While a DPIA had been carried out, it did not consider people under 13 and the dangers of them getting access to TikTok.

In parallel with these decisions, the DPC has also issued detailed guidance which Lavery regards just as important as their enforcement decisions. He specifically highlighted the 'Fundamentals for a Child-Oriented Approach to Data Processing' guidance from 2021.

One of the key messages of this guidance was that companies can either opt to provide a floor of protection where all users receive equivalent protection regardless of age or, alternatively, if they intend to differentiate between children and adults then they must engage in appropriate age verification. The guidance also made clear that companies must provide appropriate information to both children and adults even if a parent or child has already consented to data collection.

Furthermore, it emphasised that information must be provided in a concise, intelligible and accessible way that child users can understand. Lavery also pointed out that if a notice can be understood by child users, then it's also likely to meet transparency requirements for adult users.

Much in line with the Guernsey DPC's ethos, this guidance stresses that children should be treated with respect, should be provided with appropriate information, and should be able to exercise their own data protection rights if they have capacity to do so.

Lavery finished by highlighting a key challenge in this area: identifying the circumstances where a child is old enough and mature enough to consent in their own right without the consent of a parent/guardian. He concluded that although these enforcement actions have sent the clear message that there are consequences for breaching GDPR obligations, there are still real challenges in this area about how data controllers can actually make sure they are complying with these decisions and guidance.

Industry's role in protecting children online

Finally, Ma talked about how the Hong Kong company K-ID can help private sector businesses to overcome some of the challenges raised by Lavery. K-ID's aim is to help companies navigate the regulatory landscape of children's privacy protection to provide child users with age appropriate and localised online experiences in the digital world.

Ma discussed the prevalence of children lying during age verification processes to access video games. He explained that often service providers deny children from accessing their services altogether and those that do not, create an ineffective age gate that fails to verify age or location. In some cases, the user flow for a minor to get consent to enter an online video game is so long and complicated that it would require both the parent and child's devoted focus for at least 30 minutes. These overly complicated onboarding processes and barriers do not incentivise children to honestly identify themselves to service providers. This makes it hard for parents and companies to monitor what online risks children are being exposed to on these platforms.

K-ID's highly customisable solution helps companies make these onboarding processes simple and seamless for children. Ma hopes that k-ID's solution will provide children with the benefit of age-appropriate online experiences while minimising potential online harms such as cyber bullying and grooming.

However, he highlighted that many developers struggle to navigate the complex jurisdictional regulatory landscape and keep up with legal developments.

This means that when it comes to developing a strategy to protect child users online, a one-size-fits-all approach is not feasible. K-ID has therefore compiled a database designed to help businesses comply with the complex matrix of privacy and safety regulations impacting kids and teens. This database answers simple questions like "what is a child according to this country's laws?" through to very practical questions like

"what should publishers do if they discover Child Sexual Abuse Material (CSAM) on their platforms?" for more than 200 jurisdictions.

K-ID are also keen to help parents and guardians play an active role in shaping how their kids and teenagers experience the digital world. Through k-ID's family portal, parents can meaningfully engage with their children's online experiences, better understand the risks their children are facing online, and teach their children digital safety skills to help make sure their kids have safe and appropriate experiences online as they grow up.

Conclusions

The panel closed with a question from audience member *Sabrina Salhi* (Chief Privacy Officer and DPO for the EU & UK at Marsh & McLennan) who asked panellists about how they would define an online harm and who should ultimately decide what is harmful for children.

Ma responded that although there are some universally accepted online harms, such as cyberbullying, grooming and CSAM, a significant number of harms are determined subjectively within cultures and jurisdictions. He felt that equipping parents with knowledge of the tools available to them would put them in the position to make the best decision for their own child based on the child's age, maturity, culture and educational level.

Lavery agreed that defining harm is complicated. He felt that "the way to deal with this is through appropriate online safety frameworks and online safety codes. This is already advocated by certain legislation such as the GDPR and the EU Digital Services Act (DSA)." He suggested an approach like the country-specific age classifications of films. In his view, this would allow communities to decide what they feel online harm is, but he still acknowledged the relevance of parents' views in assessing the maturity of their children and that perspectives on harms could change over time.

Masterton worried that with the speed at which new technology is being introduced, it may take some time to fully understand how these products are affecting young people and whether it is damaging them. However, she was also keen to make clear that banning young people from using technology altogether would have significantly worse consequences.

In the face of these daunting challenges, it is clear that any impactful strategy to protect children must have participation from every key stakeholder in the ecosystem. These include regulators, educators, parents, academics, business leaders and most importantly, the children themselves.

Homan, employing the metaphor of an orchestra, suggested that "perhaps we need all parties to grab an instrument and help devise a melodic and harmonious piece of music to protect children's privacy rights."

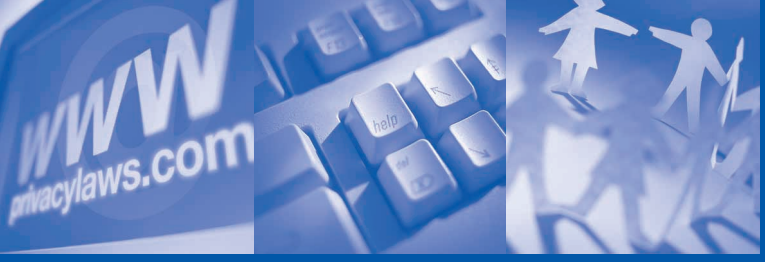
It may be a big responsibility, but deliberate action and investment is essential to protect this planet's most valuable resource - our children.

INFORMATION

ww.ofcom.org.uk/media-use-and-attitudes/media-habits-children/children-and-parents-media-use-and-attitudes-report-2024/
www.odpa.gg/information-hub/children-young-people
www.odpa.gg/childrens-framework
www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-instagram-inquiry
www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok
www.dataprotection.ie/en/dpc-guidance/fundamentals-child-oriented-approach-data-processing

AUTHOR

Hannah Heilbuth is a PhD Student at the University of Nottingham, UK.
Email:
Hannah.Heilbuth@nottingham.ac.uk



ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Uber to appeal Dutch DPA fine of €290m on data transfers to US

The decision could have repercussions for other multinationals transferring personal data between the EU and the US.
By **Laura Linkomies**.

Uber, represented by law firm De Brauw Blackstone Westbroek will be appealing the Netherlands' Data Protection Authority's decision of 26 August.

The decision and fine of €290 million relates to Uber's transfer of personal data of European taxi drivers to the United States[1]. By making the appeal, Uber will not have to pay the fine at this time. Even if the decision was upheld, any fine

Continued on p.3

France: AI is a priority area for CNIL, the data regulator

The CNIL gathers stakeholder feedback on its recommendations and signals that it would be ready to become the AI regulator.
By **Nana Botchorichvili** of IDEA Avocats, France.

With the ever-growing development of artificial intelligence (AI) tools and systems, France aims to position itself among leading countries in the field, in accordance with a national strategy established by the French government since 2018[1]. The strategy is mainly focused on enhancing AI research capabilities, training and attracting the best AI talents, and accelerating the dissemination

Continued on p.5

Issue 191 **OCTOBER 2024**

INTERNATIONAL report

ISSUE NO 191 OCTOBER 2024

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Nana Botchorichvili
IDEA Avocats, France

Graham Greenleaf
Independent Scholar, Australia

Arthit Suriyawongkul
ADAPT Centre, Trinity College Dublin, Ireland

Abigail Dubiniecki
Independent Data Protection Consultant, Canada

Colin J. Bennett
University of Victoria, Canada

Timon Mertens
Bertelsmann, Germany

Hannah Heilbuth
University of Nottingham, UK

Katharine Kemp
University of New South Wales, Australia

Francesca Romana Pesce
University of Milan, Italy

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.
Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

AI guidance begins to emerge

As reported in our lead story, France's CNIL has been active in issuing guidance on Artificial Intelligence (AI) (p.1) to clarify how it should be dealt with from the GDPR perspective, and as we were going to print, Belgium's privacy authority also issued its advice. Other active DPAs in this field include the UK's ICO and Ireland's Data Protection Commission, for example. The European Data Protection Board is of the view that the national DPAs should also become AI authorities (p.19). However, fragmentation will take place as some countries, such as Spain, will appoint a separate entity as their Market Surveillance Authority.

The EU's AI Board, which consists of representatives from each EU Member State and is supported by the AI Office within the European Commission, held its first meeting on 10 September (p.7). It is the key advisory body that was created by the AI Act, and its task is to provide advice and assistance with implementing the AI Act.

The EU has also launched a voluntary AI pledge and now over 100 companies have signed up to it. The signatories include Amazon Europe, Google, Hewlett Packard, Lenovo, Mastercard, Nokia, Orange and Salesforce, to name a few. The Commission is working together with the participants to support them in applying the principles of the AI Act, for example by helping to build internal processes, prepare staff and self-assess AI systems.

What is now of paramount importance is promoting AI awareness and understanding of its use among staff.

Our second lead story is to do with international transfers, a topic that is never away from the headlines as DPAs and companies have different interpretations (p.1). The EU will soon start consultation on a new set of Standard Contractual Clauses aimed at facilitating data transfers to controllers and processors in third parties and directly subject to the GDPR (p.18). As the European Commission is due to issue its report on the functioning of the EU-US Data Privacy Framework by the end of this year, and UK EU adequacy will be evaluated in 2025, this space is still an area that needs international businesses' constant attention.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura@privacylaws.com.

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 180+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 180+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications.

3. Electronic Version
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access *PL&B* events documentation, except for the Annual International Conferences in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

9. Free place at a *PL&B* event
A free place at a *PL&B* organised event when booked at least 10 days in advance. Excludes the Annual Conference. More than one free place with Multiple and Enterprise subscriptions.

privacylaws.com/reports

> *PL&B International Report* is a powerhouse of information that provides impartial and relevant insight across a variety of jurisdictions in a timely manner.
>
> **Mark Keddie, Chief Privacy Officer, SITA**

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the UK GDPR and related regulatory changes, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.