ICO enforcement and focus on children's privacy

Organisations should ensure they take steps to mitigate risks to children.

By **Nicola Fulford**, **Jabeen Rizvi** and **Kathleen McGrath** of Hogan Lovells.

Around this time two years ago, the new Information Commissioner, John Edwards, began his role. A previous member of OECD's Informal Group of Experts on Children in the Digital Environment, the new Commissioner's opening statement emphasised rights, responsible innovation, and empowering people through privacy[1]. As we reflect on the ICO's actions two years on, their focus on enforcing children's rights at the intersection with modern technologies has gained intensity.

ICO25

The comments of John Edwards in his opening speech were reflected in the ICO's later published strategic plan, 'ICO25'[2]. The plan sets out the purpose, objectives, and values of their new approach, and how the ICO will achieve it by 2025. The ICO specifically outlined four objectives: safeguard and empower people, enable innovation and responsible growth, promote openness and transparency and develop the ICO's culture.

In the plan, the ICO detailed a commitment to empower individuals by focusing on children's privacy and the impact of technology on vulnerable groups such as in the area of AI-driven discrimination. They set out that they would be pressing for further changes on social media platforms, video and music streaming sites and gaming platforms and continue their investigations into any unlawful conduct.

The ICO has actively implemented these commitments through the publication of guidance and the execution of audits. They have published guidance which has clarified the scope of the Age Appropriate Design Code (Children's Code)[3] by including platforms and services that are "likely to be accessed by children"[4]. This reflects the consensus that special rules are required to ensure the protection of children and that their best interests are taken into account. They have also published guidance for the gaming sector[5], with a specific focus on children having the agency to engage in the online gaming environment whilst preserving their privacy.

In their 2022/23 report of the audits conducted[6], the ICO lists the ways in which they have impacted the gaming industry and children's privacy through meaningful engagement with various companies. For example, they have seen specific child privacy risk checkpoints built into the game development process, privacy-preserving options on by default, and guidance for parents and guardians about gaming products and services.

One of the key issues they have been recommending to companies during the audit process is to be providing privacy information for different society groups such as children and vulnerable adults to ensure transparency without discrimination, and that periodic reviews of the privacy information should be standard.

Enforcement action

It is not just in the ICO's approach to guidance that illuminates their focus on children's privacy. Over the past two years, we have seen enforcement action taken by the ICO for the first time on companies unlawfully processing of children's data, notably targeting social media giants.

The ICO has recently issued a provisional enforcement notice to Snap over the processing of children's data in relation to their AI chatbot[7]. In 2023 Snap integrated OpenAI's ChatGPT technology into an AI chatbot on their popular social media application, Snapchat.

The parent company of social media company Snapchat faces the possibility of a series of actions required by the Commissioner to bring their service into compliance. In their provisional enforcement notice, the ICO allege that Snap failed to properly assess privacy risks posed by the chatbot, and in particular to several million child users aged 13-17.

John Edwards has emphasised that this is only a provisional notice, and there should be no assumption that Snap is in breach.

In a more substantive show from the ICO, earlier in 2023 they issued TikTok a £12.7m fine for the unlawful processing of children's data[8]. The ICO found that TikTok were processing the personal data of children unlawfully. What makes this enforcement action particularly divergent from previous GDPR decisions is the emphasis on data protection by design and default principles.

In this case the ICO found that TikTok did not recognise that there were children using its service, and thus did not have the requisite transparency information or parental consent. The ICO stated that TikTok 'ought to have been aware' that children were using the platform.

The ICO also took issue with the age verification mechanism that TikTok relied on to filter out underage users. TikTok relied on self-certification to ensure children did not access their service. Users were asked to state whether they were younger than 13 and users who volunteered the information were barred from creating an account. Users aged under 13 but who did not submit this information were allowed to create an account without further corroboration or verification. The ICO not only found the age verification mechanism to be inadequate, but they also stated that TikTok did not do enough to check and ensure their age verification mechanism as sufficient.

It is worth pointing out that the fine was on the basis of processing that happened between 2018 and 2020, and therefore did not include reference to the Children's Code.

The ICO's continued emphasis on

protecting the rights of vulnerable groups including, and especially, children highlights that large fines and enforcement notices are a real risk to some companies.

Risks and risk assessments

The preliminary enforcement notice against Snap, whether it results in an enforcement notice or not, shows that the ICO is taking risk assessments seriously. This may mean assessing whether the new service or product is likely to result in a high risk to individuals or conducting a full Data Protection Impact Assessment (DPIA). DPIAs should also cover particular risks posed to children and identify appropriate mitigating measures. This is especially important when integrating a new or emerging technology, such as generative AI, into your existing platform.

Age verification

The TikTok enforcement shows that an age verification mechanism is not enough to protect the privacy of children. Companies need to be assessing whether the mechanism is working. The ICO found that there were between 1.1-1.4 million children with accounts on TikTok at the time of the investigation, and the sheer scale of underage users meant that the ICO viewed the breach as significant, and the starting fine amount was higher[9]. Age verification is now inevitable for certain services, similar to the idea of height restrictions for certain amusement park rides. The Commissioner's Opinion on Age Assurance[10] is currently being updated, in particular to take account of Children's Code guidance, technological developments and the introduction of the Online Safety Act, but should be referred to for now.

Use of AI technologies

As AI has become a hot topic across the globe, John Edwards has said the ICO are worried about a 'rush to market' that is liable to happen at the early stages of technological deployment when companies are keen to utilise new and emerging technologies. He said that the ICO wants to ensure that corners are not cut when a new product is launched.

The ICO may have published the provisional enforcement notice against Snap as a way of sending a message to the market that they need to be accountable for the risk assessments that they are doing before deploying new technologies. This should include consideration of the ICO's questions to ask when developing or using generative AI[11] and other AI guidance.

Children's Code

We are yet to see final enforcement on the basis of violations of the Children's Code. The Children's Code was drafted on the basis that children should have agency on the internet i.e. be able to make their own decisions and exercise their rights online. They should be able to use the internet in a safe and secure way, as opposed to being prohibited from it. As such, misleading content and deceptive design patterns can negate children's agency. Addictive model designs are also likely to be an area of increasing focus with many companies engaging advisory panels with experts including child psychologists to consult on product decisions and their impact on children in particular.

Conclusion

The ICO have said publicly that they will continue to focus on enforcing children's privacy rights online, and in particular they will look at the data sharing in child protection and safeguarding areas. It is clear from the intention of the ICO that in areas where vulnerable groups face harm due to non-compliant data protection practices, there is potential for significant enforcement consequences. Controllers should ensure they suitably consider, and take steps to mitigate, risks to children and vulnerable groups, especially when implementing new technology.

AUTHORS

Nicola Fulford is a Partner, Jabeen Rizvi an Associate and Kathleen McGrath a Knowledge Paralegal at Hogan Lovells.
Emails: Nicola.fulford@hoganlovells.com
Jabeen.rizvi@hoganlovells.com
Kathleen.mcgrath@hoganlovells.com

REFERENCES

1 ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/01/new-uk-information-commissioner-begins-term/
2 ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/ico25-strategic-plan/
3 ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/introduction-to-the-childrens-code/
4 ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/likely-to-be-accessed-by-children/
5 ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/top-tips-for-games-designers-how-to-comply-with-the-children-s-code/
6 ico.org.uk/action-weve-taken/audits-and-overview-reports/ico-audit-a-year-in-focus/
7 ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/10/uk-information-commissioner-issues-preliminary-enforcement-notice-against-snap/
8 ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/ico-fines-tiktok-127-million-for-misusing-children-s-data/
9 The original ICO notice of intent for TikTok set the fine at £27 million. Taking into consideration the representations from TikTok, the regulator decided not to pursue the provisional finding related to the unlawful use of special category data. That means this potential infringement was not included in the final amount of the fine set at £12.7 million.
10 ico.org.uk/media/4018659/age-assurance-opinion-202110.pdf
11 ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/generative-ai-eight-questions-that-developers-and-users-need-to-ask/

ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

The ICO's new streamlined approach to UK BCRs

The new system allows for a single version of EU BCR supplemented by a UK Addendum. By **Eduardo Ustaran**, **Katie McMullan** and **Jabeen Rizvi** of Hogan Lovells.

Following a re-think of the process for the authorisation of UK BCR after Brexit, the Information Commissioner's Office (ICO) has devised a new mechanism to significantly streamline approvals. The new process, which was originally suggested by Hogan Lovells in collaboration with *Privacy Laws & Business* (see our memorandum, "Building a common EU and UK BCR framework" of 10 January 2023[1]

Continued on p.3

DPDI Bill moves to the House of Lords for detailed scrutiny

As the government makes a significant number of amendments, there is much to debate. The House of Lords questions the UK's EU adequacy in light of the DPDI Bill. By **Laura Linkomies**.

The government's amendments to the Data Protection and Digital Information Bill (DPDI) Bill,[1] tabled in the House of Commons on 23 November, did not receive proper scrutiny by MPs as there was only limited time available at the Report Stage. Opposition MPs raised concerns over this timetable, but the Bill nevertheless progressed to the House of Lords where it received its second reading on 19 December.

Continued on p.4

Issue 131 **JANUARY 2024**

UNITED KINGDOM
report

ISSUE NO 131 **JANUARY 2024**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Eduardo Ustaran, Nicola Fulford, Katie McMullan, Kathleen McGrath and Jabeen Rizvi
Hogan Lovells

Eleonor Duhs
Bates Wells

Claire Saunders and Jenai Nissim
HelloDPO Law Ltd

Elena Testa
Independent privacy professional

Henry Davies
LLM

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* United Kingdom 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 2047-1479

comment

AI will break through in 2024

Happy New Year to all our readers! 2024 looks to be the year for AI. While we expect to see legislation – the EU AI Act was agreed at a political level in December last year – other developments will affect our lives as consumers in many practical ways.

For example, Microsoft's Copilot, an AI chatbot based on a large language model will soon feature as a separate button on its Windows keyboards, while Google's Bard which transforms Google Search into a conversational bot will be followed by Bard Advanced that could be locked behind a paywall.

Using AI is already common, and will be an everyday experience for most people whether at work or at home. UK Information Commissioner, John Edwards, warned at the end of last year that 2024 cannot be the year consumers lose trust in AI. The UK is not planning to legislate for the time being, but announced last November that it will set up an AI Safety Institute to test emerging types of AI. This global hub will partner with the US AI Safety Institute, and with the government of Singapore.

The ICO says that organisations that outsource the development of their AI systems remain, as data controllers, primarily responsible for ensuring that an AI system they use is capable of producing an explanation for the decisions made. Management cannot abdicate their responsibility. We as privacy professionals have an important role in creating trust with regard to processing personal data within AI applications.

The *PL&B* Roundtable, *Ensuring Fair and Lawful AI Implementation* www.privacylaws.com/ai2024/ including speakers from the ICO and the UK government's Office for AI, will contribute to the debate and seek models for best practice. I hope to see you in London on 23 January.

Meanwhile, the Data Protection and Digital Information Bill has progressed to the House of Lords (p.1). Several tricky issues remain in this Bill, and also more generally on data protection as a fundamental right (p.7).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura.linkomies@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

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

Be alert to privacy and data protection law issues and tech developments that will affect your compliance and your 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 and events. You can then click straight through from the search results into the PDF documents.

3. Electronic Versions
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 in Data Protection, Freedom of Information and related laws.

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

7. Events Documentation
Access UK events documentation such as *PL&B 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.

privacylaws.com/reports

"*Privacy Laws & Business* not only acts as a useful and comprehensive summary of recent key developments in our area of specialism, but also provides excellent, in-depth insight and analysis to drive thought leadership. It's an invaluable source of information."

Emma Erskine-Fox, Managing Associate, TLT LLP

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 37th year. Comprehensive global news, currently on 180+ countries, legal analysis, management guidance and corporate case studies on privacy and data protection, written by expert contributors

Read in more than 50 countries by regulators, managers, lawyers, and academics.

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.