RESEARCH REPORT

Impact of regulation on children's digital lives

Steve Wood, PrivacyX Consulting

May 2024

Digital Futures For Children

LSE THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

5RIGHTS FOUNDATION

Table of contents

TABLE OF FIGURES

Foreword

A missing piece in the regulation ecosystem is data for independent research and evaluation. Without it the rich community of academics and experts who seek a better digital world are blindfolded. That was the impetus behind commissioning Steve Wood, regulator turned academic, to answer the question: does regulation work? He wrote to 50 companies for evidence of changes they had made in response to regulation – whether in anticipation or following its introduction. One of the starkest numbers in his excellent report is that only eight of the companies bothered to answer, and they only answered partially. Kudos to those eight.

Time will show whether the transparency requirements and data access granted by the EU's Digital Services Act, the information powers given to Ofcom under the Online Safety Act, or the access to data for bereaved parents will together create a more coherent picture of what works and what patently doesn't. In the meantime, we can examine the announcements that tech companies make, check and re-check their digital products and services, and write politely to ask them how they have complied with regulation. The results are illuminating, and the report concludes that regulating tech means change: change to services, governance, moderation strategies, information and tools and, default settings.

The report captures only the tip of the iceberg, as many changes are not made public at all. But it's clear that regulation can bring real benefits to children's lived experience. As the report shows, the most impactful changes are those that are by design and default - changes to product design that take responsibility for aligning digital services with children's rights and development needs. The focus is the UK, but we believe there will be interest from – and lessons for – regulators and governments across the world who are tackling the pressing safety and privacy issues surrounding tech and childhood.

At the DFC we understand that children want and need to participate in the digital world, and we see our role as finding strategies and providing evidence for that to happen in a rights-respecting way that takes account of their evolving capacity. We welcome this report – a snapshot in time – as evidence that regulation can support the goal of building the digital world children and young people deserve. We thank and commend Steve on his forensic work in writing this report, even before his recommendation for independent research access has become a reality.

Baroness Beeban Kidron
Chair, 5Rights Foundation

Professor Sonia Livingstone
London School of Economics and Political Science

1. Executive summary

Context

Recent years have seen significant developments in legislation and regulation covering children's privacy and safety in response to growing public concern and evidence of risks to children online.

The UK Age Appropriate Design Code (AADC) took effect in 2021, and the Online Safety Act (OSA) passed into law in 2023 and is now in a transitional period. The European Union (EU) has passed the Digital Services Act (DSA), which took full effect in 2024. More established legislation such as the General Data Protection Regulation (GDPR) and the US Children's Online Privacy Protection Act (COPPA) also continue to play a role in regulation.

Aims and methods

The project seeks to understand how these new developments in legislation and regulation may benefit children's digital lives. The report examines the impacts of legislative and regulatory measures focused on children's online privacy and safety over the period 2017–24. This is an important step in seeking to generate a baseline of evidence of these impacts, to inform future implementation and development, including in jurisdictions that do not currently have dedicated measures in place to protect children's privacy and safety.

The research collated information about changes companies had publicly announced to improve protections for children's privacy and safety online. This information was recorded from the websites for Meta, Google, TikTok and Snap. These companies were selected based on evidence about their extensive use by children. Each change was then categorised against two sets of criteria: (1) risks in the OECD's typology (contact, conduct, consumer, content and cross-cutting) and (2) four types of change to the design of the service (by default, tools, information and support).

The research project also wrote to 50 companies for information about changes they had made related to child privacy and safety over the relevant period. Only eight responded, providing limited information; some of this information was used alongside research in other sectors, such as gaming, to provide further examples of changes to supplement the publicly announced information for Meta, Google, TikTok and Snap. It is likely that the companies had made other unannounced changes, but this information was not accessible to the project.

Research findings and conclusions

The research made the following findings about the changes announced by Meta, Google, TikTok and Snap:

- 128 changes were recorded during the period 2017–24.
- A peak of 42 changes was recorded in 2021, the year the AADC came into effect.
- Meta was the most active company – announcing 61 changes.
- The highest OECD risk category was content risk – 56 changes – followed by cross-cutting (41), contact (16), consumer (11) and conduct (4).
- The highest category change was 'by default' – 63 changes – followed by tools (37), information (21) and support (7).

It is reasonable to conclude that legislation and regulation is driving the companies to make significant numbers of important child privacy and safety changes. These can provide substantive benefits in protecting children online. However, further research is needed to assess the full extent of the benefits. Further assessment is also needed as the DSA and OSA are fully implemented through 2025 and 2026.

Some of most important changes recorded, linked to legislation and regulation, included social media accounts defaulted to private settings, changes to recommender systems and restrictions on targeted advertising to children.

The research also revealed that companies are significantly relying on tools such as parental controls in response to legislation and regulation. While there is a valid relationship between the use of tools and the requirements in the AADC, GDPR and DSA, there is a risk of over-reliance as a privacy and safety measure. The evidence indicates low levels of use and efficacy for parental controls, plus risks to child autonomy. This therefore presents a risk of reliance to the exclusion of other measures.

The report also notes the risk that changes to age assurance and recommender systems could impact on other rights that children have. The impacts of these changes on rights, such as freedom of expression and non-discrimination, will need to be carefully monitored.

We have observed a significant number of changes. Previously, the question was whether companies were making enough changes. Over time the regulatory questions will focus on whether the solutions are effective. Therefore, regulators will need to be equipped to handle these complex questions.

The research revealed a significant challenge in gathering information about changes made by companies, and highlights a significant transparency gap that regulators and companies should address.

The Digital Futures Commission (DFC) is committed to undertaking a further research project, with the next report to be published in early 2026. This would also draw on evidence from the DSA and OSA's transparency measures, made available over 2024 and 2025.

2. Summary of recommendations

Recommendation 1. Companies subject to the DSA, OSA and AADC should ensure that solutions address the full range of risks, as detailed in the OECD typology of risks, including support measures related to conduct and contact risks.

Recommendation 2. Companies should work across industry to introduce best practice rather than each working separately, to ensure that different solutions don't leave unnecessary gaps in safety provision.

Recommendation 3. The UK Government should update the OSA to introduce mandatory access to data for child safety research, learning from the DSA's approach and implementation by the European Commission.

Recommendation 4. The European Commission and Ofcom should explore how data related to child safety changes could be recorded and logged transparently in a 'child online safety tracking database'.

Recommendation 5. The UK Government, Ofcom, Information Commissioner's Office (ICO) and European Commission should consult on how to assess the outcomes of their child safety regimes, including consideration of children's wider rights under the United Nations (UN) Convention on the Rights of the Child.

Recommendation 6. The ICO, Ofcom and European Commission should provide guidance as to how platforms should record and document changes to the design and governance of their platforms related to child privacy and safety.

Recommendation 7. Companies should provide a single web portal that allows researchers and other stakeholders to see a record of child privacy and safety changes implemented, by date. The changes should also be made available as an API and in machine-readable format. This should initially be developed as regulatory guidance and made into a statutory requirement if evidence indicates formal provision is needed.

Recommendation 8. Companies should provide explicit confirmation of which jurisdiction or region each change applies to, and update this information as it changes.

Recommendation 9. All EU Data Protection Authorities and the ICO should ensure that they assess the risks related to children's online privacy when developing their regulatory strategies, including measures to assess the outcomes achieved. All Data Protection Authorities should also include a section on children in their annual reports, including outcomes of investigations that did not result in formal action.

Recommendation 10. Data protection and online safety regulators should publish their expectations of good practice, require companies to meet or better them, and seek to spread good practice across sectors.

Recommendation 11. Data protection and online safety regulators should work via international cooperation mechanisms, such as the Global Online Safety Regulators Network[1] and Global Privacy Assembly,[2] to agree best practice across jurisdictions with the aim of creating global norms.

1 Global Online Safety Regulators Network https://www.ofcom.org.uk/about-ofcom/international/online-safety/gosrn
2 Global Privacy Assembly https://globalprivacyassembly.org/

3. Introduction

The wider context

Since 2017 a series of legislative and regulatory measures have been proposed, consulted and passed to protect children online – covering data protection, privacy and safety. Legislators and policymakers have recognised that self-regulation has not worked effectively, and that new laws and specific regulatory measures are needed. This report seeks to understand their impact over the period 2017–24.

The legislation and regulations introduced are responding to growing evidence about risks to children online, as well as the online safety of all users. Recent research by Ofcom (2024a) highlighted the pathways for children encountering violent online content, flagging that children describe violent content as 'unavoidable'. It also flagged how recommender algorithms and group messaging enable exposure, and that children's willingness to report harmful content is undermined by a lack of trust in the process.

There is now a public spotlight on how new design features impact on children. In April 2024 Snap switched off a feature dubbed 'Solar System' amid concern it was adding to children's anxiety.[3]

These measures are also framed by the full range of rights under the United Nations' (UN) Convention on the Rights of the Child, which also include freedom of information, freedom of association, and non-discrimination. While not legally binding, the most important and influential international instrument related to children's rights in the digital environment is UN General comment No. 25 (2021).

The UK and EU context

As the UK and EU's legislation and regulation are the most advanced and comprehensive, this report primarily focuses on their impact, while also noting the impact of other jurisdictions, such as the USA. The report then considers global implications in its conclusions (Chapter 11). It considers the impacts on children's rights more broadly, not just data protection, privacy and safety.

The report will primarily consider the UK Age Appropriate Design Code (AADC) (ICO, 2021), a statutory measure issued by the UK Information Commissioner's Office (ICO), and online safety legislation under the EU Digital Services Act (DSA) (2022) and the UK Online Safety Act (OSA) (2023).

3 The ranking system for paid subscribers shows users how close they are to Snap friends by displaying a position in their 'Solar System': https://techcrunch.com/2024/04/05/snapchat-turns-off-controversial-solar-system-feature-by-default-after-bad-press

The UK and EU approach to legislation and regulation seeks to ensure companies' systems and processes embed safety by design and duties of care, to realise the rights of children in relation to the digital environment, so they can learn, explore and play online safely. These new measures aim to hold the companies providing online services accountable, and ensure that concrete and practical steps are taken on an ongoing basis, as part of sustainable risk-based governance for children's safety.

It has been crucial that policymakers recognise that children have a right to be online, freedom to express themselves and to seek assembly with others – it is where they are growing up. Such an approach seeks to ensure a balance of responsibility falls on the companies that design and develop the platforms.

As the AADC, DSA and OSA have all now passed, this is an optimal moment to set out a baseline for monitoring the impact of recently introduced legislation and regulation for children online.

Wider debates

At the time of writing (2024), a wider debate is also growing about 'smartphone bans' as a solution to public concern about the impacts of online services on children.

Professor Jonathan Haidt, a social psychologist at New York University's Stern School of Business, argues that the 'great rewiring of childhood is the single largest reason for the tidal wave of adolescent mental illness that began in the early 2010s'. His book, *The Anxious Generation: How the Great Rewiring of Childhood Is Causing an Epidemic of Mental Illness* (2024), has sought to argue that the evidence of harm to children's mental health from digital technologies means that solutions such as 'no smartphones before high school' and 'no social media before 16' are needed. A significant number of academics have challenged Professor Haidt's analysis as correlation and not causation, and whether the solutions will take account of the full rights of children.[4]

This debate matters to the context of this report as such solutions are contrary to the risk, system and design approach of the AADC, DSA and OSA. Evidence of their impact will be an important part of the policy debate comparing solutions, including the Utah State style approach (2023) that other US States may seek to adopt (covered further in Chapter 4).

4 Academics challenging Haidt's analysis include University of California Professor Candice Odgers and Oxford Internet Institute Professor Andrew Przybylski. An article by Blake Montgomery for *The Guardian* (2024) summarises the debate: www.theguardian.com/books/2024/apr/27/anxious-generation-jonathan-haidt
Professor Odgers published a review of 40 previous studies in 2020 and found no cause and effect relationship between smartphone ownership, social media usage and adolescents' mental health. A 2023 analysis of wellbeing and Facebook adoption in 72 countries cited by Professor Odgers delivered no evidence connecting the spread of social media with mental illness: www.nature.com/articles/d41586-024-00902-2?ref=platformer.news

Research problem

We currently lack good evidence about whether legislation and regulation are effective in protecting children. The Digital Futures for Children (DFC) research centre seeks to understand their role as a key plank of a multistakeholder effort to realise children's rights in relation to the digital environment.

The DFC wants to know: whether and how evidence can inform regulation; the evidence of benefits (or disbenefits) of introducing regulation; and whether these are sufficient to justify advocating for new regulation in other jurisdictions, or updating or changing existing measures.

Many companies 'anticipate' regulatory demands by making changes during the progression or transition of new legislation, either to make the case that they do self-regulate, or sometimes to set the regulatory norms early. This report maps changes made during the passage of regulation, as well as the periods immediately before and after formal compliance is required (e.g., during transitional periods[5]).

The project rationale was informed by prima facie evidence that companies have been making a significant number of changes in relation to children's online safety. They have made announcements about changes,[6] but in different ways and under no formal reporting requirements.

In this research we have chosen to look primarily at the AADC DSA and OSA – all measures that seek to address systemic issues and risks via the design of the online services. We have chosen not to focus on schemes where regulators adjudicate on individual issues or content, such as the German Network Enforcement Act.

Project aim and research questions

The project aims to examine the impacts and benefits of legislative and regulatory measures focused on children's online privacy and safety, over the period 2017–24.

The project has the following research questions:

- **A.** How has recent regulation impacted the design and governance of particular online services likely to be accessed by children, if at all?
- **B.** Which aspects of service design and governance change? Are there specific trends by sector, service or product type? What can be seen as a concrete indicator of change?
- **C.** Are the changes weighted towards specific aspects of privacy, safety or legislation and regulation?

5 A period when legislation or regulation has been agreed but not fully in force, to allow companies to prepare for compliance.
6 See the full details in Annex A.

D. Which regulatory requirements have resulted in which specific benefits to children?
E. What is the impact of regulatory changes on children's rights, viewed holistically? Taking account of other rights children have, have the changes had wider consequences?
F. What can be learned from companies' responses to regulatory changes? How could this inform new regulation or changes to regulation in future?
G. How transparent are companies about changes they make, and how do they explain or promote them?
H. Can the project results inform child rights advocacy, and focus future research questions?

The project proposal recognised that transparency provisions in the EU DSA and UK OSA are yet to be fully implemented by companies. The project seeks to understand the impact of legislation and regulation, but a full study of the effectiveness of the changes made by the companies would require a further, more detailed, study in future.

The research methods are set out in Chapter 5.

Global South

The importance considering regulation from the perspectives of the Global South is recognised. Recent research considering evidence from the perspective of children in the Global South (Global Kids Online, a joint London School of Economics and Political Science [LSE]/UNICEF project) investigated how children benefit from the internet and digital technologies, and how they could be protected from the associated risks (Livingstone, 2021).

Research by Ghai et al. (2022) also illustrates the importance of studying the Global South, as while one in three internet users globally is a child, this proportion is estimated to be higher in the Global South. In Sub-Saharan Africa (specifically Ghana, Malawi and South Africa), children make up most mobile users, even among the poor.

We need to recognise that impacts of online platform business models can be different for children in different regions of the world. Also, jurisdictions and companies may approach regulation differently in the Global South. There are risks of importing regulatory solutions from the Global North, with conversely, children in the Global South having less protection. This is therefore an area that the DFC will consider for future research.

We return to this issue, including global implementation of changes to online services, in our conclusions (Chapter 11).

About the Digital Futures for Children centre (DFC)

The Digital Futures for Children centre (DFC)[7] was founded in 2023 and is a joint research centre between LSE and 5Rights Foundation, which advances understanding of the challenges and opportunities presented by digital technologies for children's rights and needs. The research centre is funded by 5Rights and hosted by LSE.

The DFC facilitates research for a rights-respecting digital world for children. It supports an evidence base for advocacy, facilitates dialogue between academics and policymakers, and amplifies children's voices, following the UN Committee on the Rights of the Child's General comment No. 25 – the authoritative statement in international law of how the UN Convention on the Rights of the Child (UNCRC) should be implemented by states worldwide in relation to all things digital.

About PrivacyX Consulting

Steve Wood is Director and Founder of PrivacyX Consulting,[8] set up in 2022 to provide advice and research services focused on policy issues related to data protection and emerging areas of digital regulation. Steve is also a Visiting Policy Fellow at the Oxford Internet Institute, where he has been conducting research into the impact of social media recommender systems on children.

Previously, Steve worked at the UK data protection regulator, the Information Commissioner's Office (ICO) for 15 years. He was Deputy Information Commissioner, responsible for policy between 2016 and 2022. During this time, he oversaw the development and implementation of the AADC. Steve was Chair of the OECD Working Party on Data Governance and Privacy from 2019 to 2022, overseeing the adoption of the OECD Recommendation on Children in the Digital Environment. He was also the UK representative on the European Data Protection Board from 2018 to 2020.

Acknowledgements

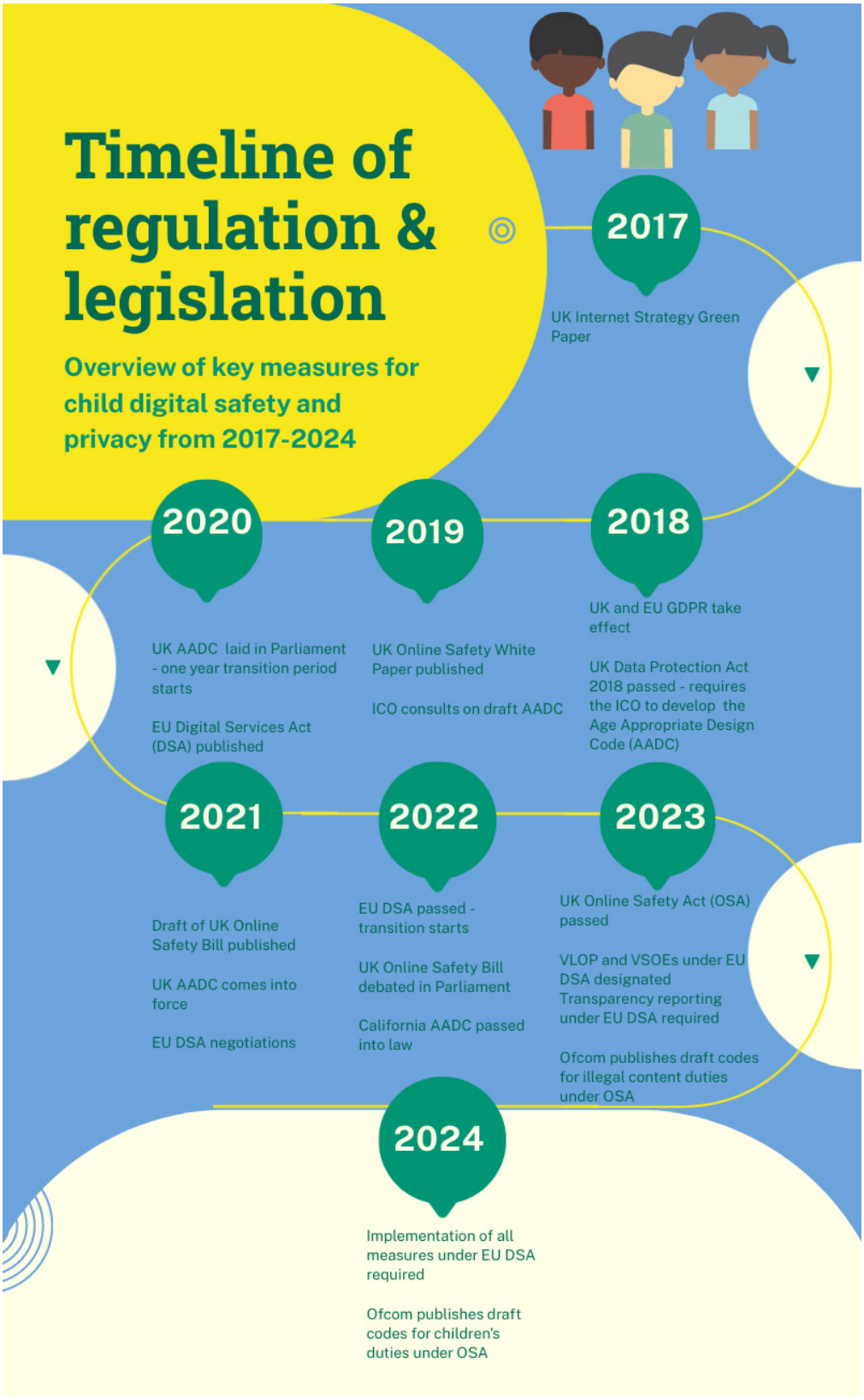
Thanks are extended to Professor Sonia Livingstone from LSE and Baroness Beeban Kidron from 5Rights for providing the vision for the project, and for their expert support and guidance during the research process.

Thanks are also given to Professor Brian O'Neill and Professor Lorna Woods, who peer reviewed the report.

Additional thanks for research support go to Debbie Kent and Gazal Shekhawat.

7 Digital Futures for Children centre: www.digital-futures-for-children.net/home
8 https://privacyx.substack.com

4. Overview of legislation & regulation



This timeline sets out the key milestones in the development of legislation and regulation related to child safety in the digital environment, focused on the UK and EU.

Summary of key legislation and regulation

United Nations General comment No. 25 – wider context of children's rights

Before considering specific legislation, it is important to note the wider international framing provided by the UN Committee on the Convention on the Rights of the Child. In 2021 it agreed General comment No. 25 (GC25) on children's rights in relation to the digital environment. Its development included international consultation with 709 children living in a wide variety of circumstances and in 28 countries.

Although not legally binding, GC25 is an influential international instrument that guides member states in how they should develop legislation and regulation related to children's rights online, to fully implement their obligations under the Convention.

Importantly, GC25 addresses the full range of children's rights, not just data, privacy protection and safety. It takes a holistic approach that reflects the reality and ongoing evolution of children's lives online (UN, 2021).

UK Age Appropriate Design Code (AADC) (also known as the Children's Code)

The requirement for the UK ICO to develop the AADC was contained in the Data Protection Act 2018 (Section 123). It is therefore a regulatory measure focused on protecting children from harms related to use of their data and risks to their privacy. It does not cover issues solely focused on content or general safety. The AADC does cover the intersection between data and content, where profiling is used to target content to children.

The measure was introduced by Baroness Beeban Kidron during the passage of the Data Protection Bill in the House of Lords. It was published for consultation in 2019, was laid in Parliament in 2020 and came into full effect in 2021.The AADC has effect via the powers of the ICO under the UK General Data Protection Regulation (GDPR). It is a statutory code but does not have the direct effect of primary legislation. The Commissioner, Tribunal and Courts must have regard to it.

The AADC covers online services 'likely to be accessed by children', not just services aimed at children. It takes account of the UNCRC and the fact that children have different needs

at different ages. Children are therefore defined as 'under 18'.

It also aims to implement the GDPR's requirement that children require specific protections, given the risks they face online (discussed further below).

The AADC was developed via two stages of public consultation: an initial call for evidence based around a series of questions (2018), and then a consultation on a draft of the code (2019).

The AADC was developed into a set of 15 standards that translate into expectations that online services should follow when designing to protect children from harms related to uses of their personal data. It builds a series of protections for children's personal data using 'data protection by design' standards. Data protection by design is a requirement of Article 25 in the GDPR.

THE 15 AADC STANDARDS:

1. Best interests of the child: The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child.
2. Data protection impact assessments (DPIAs): Undertake a DPIA to assess and mitigate risks to the rights and freedoms of children who are likely to access your service, which arise from your data processing.
3. Age-appropriate application: Take a risk-based approach to recognising the age of individual users and ensure you effectively apply the standards in this code to child users.
4. Transparency: The privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent, and in clear language suited to the age of the child.
5. Detrimental use of data: Do not use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or government advice.
6. Policies and community standards: Uphold your own published terms, policies and community standards (including, but not limited to, privacy policies, age restriction, behaviour rules and content policies).
7. Default settings: Settings must be 'high privacy' by default (unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child).
8. Data minimisation: Collect and retain only the minimum amount of personal data you need to provide the elements of your service in which a child is actively and knowingly engaged.
9. Data sharing: Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child.
10. Geolocation: Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child), and provide an obvious sign for children when location tracking is active.
11. Parental controls: If you provide parental controls, give the child age-appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored.
12. Profiling: Switch options that use profiling 'off' by default (unless you can demonstrate a compelling reason for profiling to be 'on' by default, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing).
13. Nudge techniques: Do not use nudge techniques to lead or encourage children to provide unnecessary personal data or turn off privacy protections.
14. Connected toys and devices: If you provide a connected toy or device, ensure you include effective tools to enable conformance to this code.
15. Online tools: Provide prominent and accessible tools to help children exercise their data protection rights and report concerns.

The first two standards are holistic, requiring companies to consider the best interests of the child when designing services that use children's personal data. A recent report by the DFC on best interests (Livingstone et al., 2024) found that in relation to the digital environment, there is evidence that 'best interests' is being misunderstood, or even misused or abused.

Livingstone et al. (2024) argue that: 'in most cases it is not necessary to evoke best interests but rather to respect, protect and fulfil the full range of rights in the UNCRC; best interests is not a replacement for other or all of children's rights, nor are children's rights a matter of pick and mix' and that 'In certain situations – such as when several of a child's rights are in tension, or where third party claims jeopardize children's rights – a "best interests" determination should be sought. Such a determination informs the standard of expected conduct for digital service providers.'

The ICO also provides an additional tool to support organisations when assessing the best interests of the child and applying Standard 1 (ICO, n.d., a).

The UK Online Safety Act (OSA)

The OSA was preceded by an *Internet safety strategy* Green Paper in 2017 (HM Government, 2017), which was supported by a literature review by the UK Council for Child Internet Safety's Evidence Group (Livingstone et al., 2017). The *Online harms* White Paper then followed in 2019, followed by a consultation and a government response in 2020 (Department for Digital, Culture, Media & Sport, 2020), which set the path for the Bill to be introduced to Parliament in 2021. The OSA was passed into law in 2023.

The OSA covers online safety for all users and contains specific obligations related to children. The overall approach of the legislation is design-focused and risk-based – there is not a right to complain to the regulator about individual matters such as content. The safety duties contained in the OSA are to be considered against other rights, such as freedom of expression. The duties are also framed as a requirement to use proportionate measures.

Further details about how companies should comply with these requirements will be set out in dedicated codes of practice and guidance produced by Ofcom. The codes related to children were published on 7 May 2024 (Ofcom, 2024c), and their impact will also need to be considered in future research. The OSA states that 'service providers which implement measures recommended to them in the children's codes will be treated as complying with the relevant duty or duties to which those measures relate'.

The OSA's key provisions related to children:

- Mitigate and manage the risks of harm to children in different age groups, as identified in a children's risk assessment, and mitigate the impact of harm to children in different age groups presented by content that is harmful to children.
- Companies will need to prevent, detect and remove illegal content (e.g., child sexual abuse content).
- Companies must prevent children from accessing content that is designated as harmful to children (e.g., content depicting self-harm, violence, bullying).
- Companies will need to use age verification or age estimation tools to prevent children from encountering designated content. Otherwise they need to make their service age-appropriate.
- Companies have duties to protect children's online safety, including a duty to take or use proportionate measures relating to the design or operation of the service. This will cover mitigations related to children and harms identified from risk assessments.
- The safety duties related to children also cover safety, policies, terms and other governance matters.
- Larger companies will be required to publish a summary of their risk assessments related to children (further details of the requirements will be contained in the Ofcom codes or guidance).
- Risk assessments must also consider how the design and operation of the service may reduce or increase the risks identified.
- Companies have a duty to ensure that complaints procedures are publicly available and easily accessible (including to children).

Key OSA provisions, Sections 11–13 for user-to-user services, Sections 23–30 for search services, Sections 21 and 32 for complaint procedures duties.

Ofcom has a full range of powers to investigate, fine and enforce the law. It has set out a regulatory approach that will involve supervision and engagement with the platforms that pose the highest risk, and an expectation that the platforms will make changes as a result of these engagements (Ofcom, 2023b). Ofcom has set out four outcomes to achieve under the OSA:

- Stronger safety governance in online firms.
- Online services designed and operated with safety in mind.
- Choice for users so they can have meaningful control over their online experiences.
- Transparency regarding the safety measures services use, and the action Ofcom is taking to improve them, to build trust.

There is now a staged implementation of different requirements:

- Phase one: Illegal harms duties. Obligations will commence following the passage of the relevant codes and guidance in Parliament (the consultation started in late 2023, with commencement likely to be in autumn 2024). The codes and guidance are to be developed by Ofcom, the UK online safety regulator.
- Phase two: Child safety, pornography and the protection of women and girls. Obligations will commence following the passage of the relevant codes and guidance in Parliament (the consultation will be in spring 2024, with commencement likely to be in autumn 2025).
- Phase three: Transparency, user empowerment and other duties on categorised services. Obligations will commence following the passage of the relevant codes and guidance in Parliament (the consultation will be in spring 2024, with commencement likely to be in early 2026).

EU Digital Services Act (DSA)

The DSA was proposed in December 2020. Political agreement was reached in April 2022, and it entered into force in November 2022. The DSA's obligations for all platforms came into effect on 17 February 2024. The Commission designated the first Very Large Online Platforms and Search Engines (VLOPs and VLOSEs) on 25 April 2023 and the second batch on 20 December. Platforms designated as VLOPs or VLOSEs then had four months from designation to comply with DSA rules. As with the OSA, the DSA also takes a design- and risk-based approach.

The DSA contains the following obligations related to children:

- Requirement that online platforms provide terms and conditions on use of the service in a way that children can understand (Article 14).
- Providers of online platforms accessible to children must take appropriate and proportionate measures to ensure a high level of privacy, safety and security of children on their service (Article 28).
- VLOPs and VLOSEs must identify and assess the potential online risks for children using their services, including the design of the service. They will need to conduct a risk assessment annually (at least) (Article 34).
- VLOPs and VLOSEs are required to take reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks, including adapting the design of the platform, testing and adapting their algorithmic systems, including their recommender systems, targeted measures to protect the rights of the child, including age verification and parental control tools (Article 35).
- Complaint systems must be child-friendly for minors to use when they discover illegal or other content that should not be online (Article 20).
- If platforms are reasonably certain that a user is a child, they must not show them any adverts based on profiling (Article 28).
- VLOPs and VLOSEs that use recommender systems must provide at least one option for each of their recommender systems that is not based on profiling as defined by the GDPR. This applies for all users, including children (Article 27).
- The DSA forbids the use of dark patterns for all users, including children (Article 25).
- The DSA also requires the conduct of annual independent audits and their publication, along with details of the risk assessments and mitigations (Article 37).

General Data Protection Regulation (GDPR)

The GDPR came into full effect in 2018 in the EU and UK. Since Brexit, the UK is now subject to the GDPR as a separate law, supplemented by the UK Data Protection Act 2018 for more detailed legal requirements.

The GDPR contains the following provisions relevant to children's online safety:

- The recitals set out the importance of protecting children's data: '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.'
- The recitals also highlight the importance of protecting children's personal data in the context of marketing and profiling.
- The GDPR also requires online services to seek parental consent when consent is used by online services as a lawful basis to process the personal data of children under 16. The GDPR allows member states to choose a different age, down to 13. In the UK the age is set to 13.

Relevant GDPR enforcement actions are also explained in Chapter 9.

EU Audiovisual Media Services Directive (AVMSD)

The EU and UK have also implemented the Audiovisual Media Services Directive (AVMSD) (European Parliament and Council of the European Union, 2018). The Directive extended the previous scope of obligations placed on broadcasters and on-demand services to video-sharing platforms (VSPs) to any commercial service with the principal purpose of providing programmes or user-generated content to the public, but without editorial responsibility for the content that is provided.

The AVMSD requires appropriate measures to protect children 'against content which may impair their physical, mental or moral development'. Appropriate measures will include terms and conditions for users relating to the types of content listed above, age verification systems and mechanisms for reporting harmful or illegal content. While the AVMSD is therefore a much narrower set of safety measures compared to the DSA and OSA, it is also a relevant factor that may be influencing the introduction and design of age verification mechanisms on platforms such as YouTube. Its impact has therefore been briefly noted in the findings that follow.

Legislation in the United States

While the report does not primarily focus on US legislation, it is relevant to note current developments, as some US policymakers will seek to learn from UK and EU approaches. The US base of many major technology companies also mean that US legislation may have a greater global impact than other jurisdictions.

The Children's Online Privacy Protection Act (COPPA) dates to 1998 and is focused on the online protection of children under 13. The COPPA has requirements for transparency, parental or guardian consent and restrictions on how children's data can be used, including a restriction on using children's data for marketing. It is focused on 'websites directed to children', which is a narrower test than the AADC's 'likely to be accessed by children'. The COPPA is enforced by the Federal Trade Commission (FTC), and there have been several

significant enforcement actions since the law was introduced. Some of the more recent actions are covered in Chapter 9.

There have been several proposals for new child safety legislation in the US, including the Kids Online Safety Act (KOSA) (US Senate, 2023) and the COPPA 2.0, both of which would move the USA closer to the EU and UK's standards. While discussions have ongoing for many years, there has been no agreement in Congress on either of these laws. In the meantime, the FTC has proposed a revised COPPA Rule (FTC, 2023a), which covers the detail of interpretation and implementation of the statute. The new Rule is currently out for comment. The changes under the Rule would include further clarification on when a website is directed at a child, require a separate opt-in for targeted advertising, and prohibit use of children's data from educational technology.

The State of California passed the California Age-Appropriate Design Code Act (2022), drawing extensively on the UK code. The Act will be enforced by the State Attorney General's Office, but has not yet come into force due to a legal challenge by a digital industry trade body, Netchoice. An injunction was granted by the California Courts in 2023 and an appeal will be heard in 2024. The Act would be a major milestone in providing a comprehensive regulation to protect children's privacy rights online for the first time in the USA.

CEOs from the large social media platforms have appeared before Congressional Committees several times in recent years, and the threat of introducing the KOSA has been a clear feature of the discussions.

Bills similar to the AADC have also been under consideration in the following States: Minnesota, New Mexico, New York, Connecticut, New Jersey, Nevada, Oregon and Texas (Tech Transparency Project, 2023). In April 2024 the Data of Children (Maryland Kids Code) was passed by the Senate and sent to the Governor for signing (Maryland General Assembly, 2024). The Maryland provisions include safeguards to protect against profiling by default, and requirements to consider the best interests of the child and undertake impact assessments.

Utah's proposed Social Media Regulation Act (SMRA) stood in contrast to the system and design approach of Maryland and others. It required social media companies to verify the age of users and gain parental consent for users under 18 to open a social media account. This is under legal challenge and has raised concerns related to children's access to information and other rights. Utah then repealed and replaced the SMRA in March 2024. The new version of the law instead requires social media companies to implement an age assurance system to determine whether the individual is a minor. Although it does not require that individuals determined to be minors secure parental consent to create or access an account, parental consent would be required before certain functionality could be used. The narrow approach in Utah risks making parents responsible for the harmful design impacts of the social media platforms.

These different approaches highlight the tensions that currently exist on child privacy and safety policy in the USA. An evidence-based approach, learning how different forms of regulation can present benefits and risks for children, should be a key component of the debate.

Other international developments

Other jurisdictions are also in the process of developing and passing new laws. For example, the Online Harms Bill was introduced into the Canadian Parliament in February 2024. Australia already has an Online Safety Act (2021), and plans to introduce an Age Appropriate Design Code (Attorney-General's Department, 2023).

New legislation is also emerging in the Global South; for example the Indian Digital Personal Data Protection Act (2023) contains several key measures related to protecting children online. Rwanda has published an online child protection policy (Ministry of ICT & Innovation, 2019) and more recently a Ministerial Instruction for child online protection (Republic of Rwanda, 2024). In April 2024, Brazil enacted Resolution No. 245, which provides for the rights of children and adolescents in digital environments (Ministry of Human Rights and Citizenship, 2024).

Other international conventions and standards

International organisations have also agreed other relevant, non-binding standards and guidance on protecting children's rights online.

In 2018 the Council of Europe agreed guidelines to respect, protect and fulfil the rights of the child in the digital environment. The guidelines covered the best interests of the child and evolving capacities of the child, the right to non-discrimination and the right to be heard in the digital context. A series of operational principles and measures are also contained in the document.

The OECD Recommendation on protecting children in the digital environment (2021a), and the accompanying typology of risks (2021b), set out an important set of principles and guidelines related to child safety by design. As the OECD is an intergovernmental organisation, the Recommendation also provided direction to national-level legislators and policymakers. The typology of risks (2021b) provides a framework for policymakers to consider the different harms that legislation and regulation may need to address.

5. Methodology

Research design

The research questions listed required evidence of changes that companies had made that could then be categorised and analysed. A decision was therefore made to gather information from company websites and from questions sent to the companies via a letter.

This approach would enable the research team to create data on changes recorded over time, map changes against categories, make comparisons and test for connections (a descriptive and correlational design). The dataset would also be supplemented by case studies and further examples from companies where less data was available.

Companies would be selected based on evidence that their services were extensively used by children.

As the research design involved collection of data from publicly available sources or from the companies themselves, this did not pose any significant ethical considerations, including data collection from children.

Strategic focus on four large online platforms widely used by children

Following a limited response from the initial information gathering phase, a decision was made to undertake detailed analysis of four companies' services:

- Meta (including Instagram, Facebook, Messenger and Quest)
- Google (including YouTube)
- TikTok
- Snap

These four companies' services repeatedly feature in statistics of the top 10 online platforms used by children.[9] All four are subject to the AADC, OSA and DSA.

These companies had made a significant number of announcements, and would provide an effective set of data for quantitative analysis. The websites for all four companies were searched using terms such as 'children', 'safety', 'privacy'. Internet searches were also used to identify media articles that reported changes.

9 Such as Ofcom's *Children and parents: Media use and attitudes report* (2023) (www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2023); Pew Centre's *Teens, social media and technology 2023* (www.pewresearch.org/wp-content/uploads/sites/20/2023/12/PI_2023.12.11-Teens-Social-Media-Tech_FINAL.pdf); and YPulse's 'These are European Gen Z's top social media platforms' (www.ypulse.com/article/2023/06/13/we-these-are-european-gen-zs-top-social-media-platforms).

By 'announcement' we mean company blog, press release, safety policy updates and privacy and safety centre updates.

When using the term 'change', we mean any change made to the design, operation or governance of an online service, with the intention of improving children's privacy and online safety.

Each change announced was then recorded on a spreadsheet, along with the URL, date, OECD risk category and category of the type of change. Where a company had several services (e.g., Meta – Instagram), the service was also recorded. When an announcement, such as a press release, covered several different changes, these were all recorded and categorised separately. When an announcement referenced a specific piece of legislation or regulation, this was also recorded.

Close to the completion of the research project the Children and Screens project at the Institute of Digital Media and Child Development (IDMCD) published a report on the impact of the AADC (Mootz & Blocker, 2024). This report assessed changes across Google, Amazon, Meta, Snap and TikTok against the AADC. The changes listed in the IDMCD report were checked against the evidence logged for our report to check whether any further changes could be logged. This identified a small number of changes to be added to the dataset.

OECD risk categories

Each change was categorised against the four categories in the OECD typology of risk for children in the digital environment, plus cross-cutting risks (OECD, 2021b):

Risks for children in the digital environment				
Risk categories	Content risks	Conduct risks	Contact risks	Consumer risks
Cross-cutting risks*	Privacy risks (interpersonal, institutional & commercial)			
	Advanced technology risks (e.g. AI, IoT, predictive analytics, biometrics)			
	Risks on health & wellbeing			
Risk manifestation	Hateful content	Hateful behaviour	Hateful encounters	Marketing risks
	Harmful content	Harmful behaviour	Harmful encounters	Commercial profiling risks
	Illegal content	Illegal behaviour	Illegal encounters	Financial risks
	Disinformation	User-generated problematic behaviour	Other problematic encounters	Security risks

Source: Reproduced from OECD (2021b, p. 7[10])

10 www.oecd.org/termsandconditions, under non-commercial use terms.

These categories were used as they are an internationally recognised approach to risk. They would provide an indication of which risks the changes were addressing. Collectively, the AADC, DSA and OSA address all these risks.

Categories of privacy and safety changes

Four categories were derived from assessing the key features of the AADC, DSA and OSA and from initial observations from the types of changes collected. The categories were then applied to each of the changes recorded from Meta, Google, TikTok and Snap.
Some changes logged were available to all users, not just children, but it was clear that children could be a key beneficiary – for example, changes that allowed users to use controls to filter hateful comments or a chronological content feed.

Wider focus on 50 companies

The research plan also focused on 50 companies providing online services (listed in Annex B). The companies were selected from a range of sectors drawing on research evidence that children are likely to be accessing the services. Criteria for selecting the 50 companies were based on the following:

- Data from surveys such as Ofcom's Children and Parents Media Use and Attitudes survey (2023a), that indicated which services were most used by children.
- Sectors subject to formal regulator action or priority, indicating a level of risk posed.

The services included social media, messaging, video and audio-streaming platforms, online games and generative AI.

A letter was sent in late 2023 seeking information about the changes the companies had made to the design and governance of their online services related to children's privacy and safety in the period 2017–24. Information was also sought about the legal or regulatory reasons why the changes had been made. The letters were sent to individuals with responsibility for trust and safety or data protection and privacy, depending on how the organisation had structured its responsibilities. If no contacts were available, the letters were sent to the press or media email contacts listed on the company's website.

It was recognised that the letters could have a limited response rate, due to legal caution, lack of willingness or resources available in the companies to respond. To provide a further source of insight, company websites were also assessed for announcements about child safety changes. A web alert tracker was added for the most relevant pages, so that changes could be tracked during the project.[11]

For some services no responses were received to the letters and no information was

11 Wachete: www.wachete.com

Category	Description	Examples	AADC	DSA	OSA
By default	Changes made to the design of the service that provide default protections by settings or new permanent design features	• User accounts private by default • Geolocation off by default • Recommender system settings • Age assurance requirements • Content filtering settings • Targeted advertising switched off for children	Standards 3, 5, 7, 8, 9, 10	Articles 25, 28, 35	Section 12
Information	The provision of new information that provides additional clarity to children or parents about the online service and steps that can be taken to enhance privacy and safety	• New or updated privacy notices designed to be accessible by children • Positive nudges such as screen time reminders	Standards 4, 6, 13	Article 14	Section 12
Privacy and online safety tools	Changes that provide new controls and mechanisms for users or parents to control how certain platform features work. These are user-initiated rather than set by default	• Options to use chronological content feeds • Parental controls • Controls used by children e.g., comment filters	Standards 10, 14, 15	Articles 27, 35	Section 12
Support	Changes to mechanisms that provide support for children	• Reporting concerns about content or other users • Complaint procedures • Automated or human help for when things go wrong for children on the service	Standard 15	Article 20	Section 12, 21

clearly available about changes that had been made. This is not to say that these services did not have child safety measures in places, or had not made changes, but that it was not possible to discern when they had been introduced and therefore as a possible impact of legislation and regulation. Indeed, the research team had been told of changes that had been made and not publicly stated, including some major changes.

Parliamentary evidence

In addition, searches were made for public 'on the record' statements made by the companies about legislation and regulation related to child online privacy and safety. These were undertaken on the websites for the UK and EU Parliaments and the US Congress. This evidence was then analysed to consider how the statements of support or concern about regulation compared with practical actions taken on the ground.

Challenges

We discuss the challenges of conducting the research and recommendations related to transparency in Chapter 11.

6. Findings: Analysis of child privacy and safety changes made by Meta, Google, TikTok and Snap

To inform the research questions, the analysis here seeks to address the following:

- Is there evidence of linkages between the number and type of changes and key milestones in the introduction of legislation and regulation?
- How do the number of changes for each company compare over time?
- Which features of service design have been the subject of most development or updates?
- Which of the online risks, as classified in the OECD typology of risks, are the changes addressing?
- What impact can we see from the legislation and regulation?
- Are there wider trends and impacts beyond individual service changes?

All the changes made by Meta, Google, TikTok and Snap are listed in Annex A, with a hyperlink to the announcement of each change.

Initial findings

Across the four companies' services, between 2017 and 2024 we logged **128 changes** that were relevant to child privacy and safety.

Most of the announcements assessed did not reference a specific piece of legislation or regulation as the reason for the change. Only **five references to legislation** were found. There were four references to the DSA and one to the EU Audiovisual Media Services Directive (AVMSD). This indicates that transparency is currently run on the companies' own terms.

It was therefore not possible to link some of the changes to a single piece of legislation or regulation with absolute certainty. In some cases, the impact may also be due to the cumulation of legislation and regulation.

However, factors such as the timing and nature of the change announced can provide an indicator of link. For illustration, 'by default' changes made during the summer of 2021, ahead of the AADC coming into full effect in September, have a likelihood of linkage. Therefore plausible linkages are drawn out in the narrative analysis that follows. Overall, this analysis does indicate significant impacts from the AADC, DSA and OSA.

The four companies all promote the changes as proactive measures and investments they have taken to protect children online. This approach has also included advertisements in newspapers and on public billboards by Meta (Sutcliffe, 2023).

Companies will often not see incentives to talk about the benefits of new legislation and regulation, as they can perceive this could lead to more. This therefore creates important questions about evidence, accountability and the need for a multistakeholder discussion about impacts and benefits.

Where they do publicly mention specific legislation, it is very often in parliamentary evidence sessions where they refer to legislation that has been implemented rather than new legislation. This is analysed further in Chapter 7.

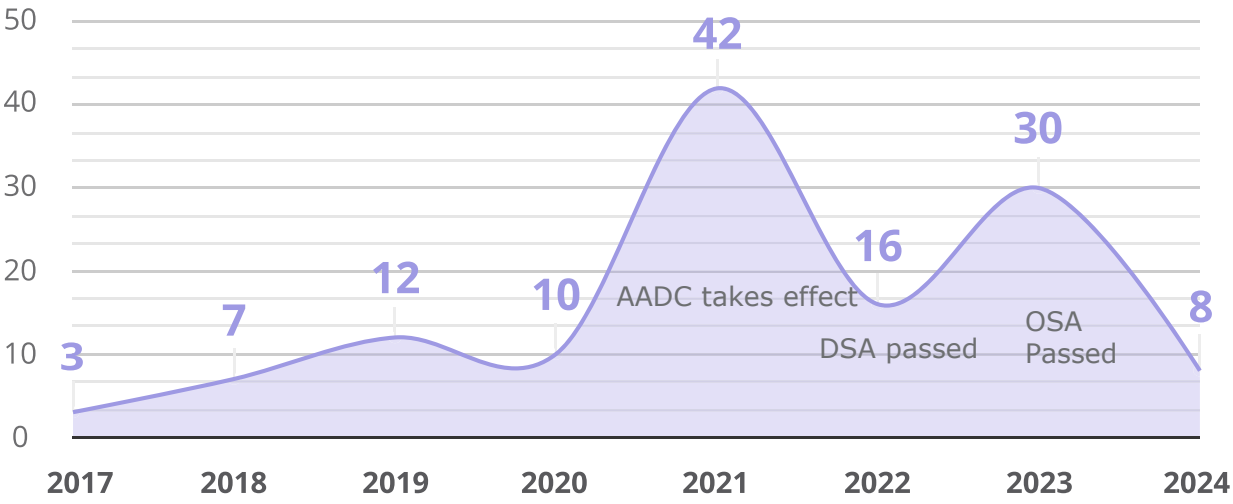
Is there evidence of linkages between the number and type of changes and key milestones in the introduction of legislation and regulation?

Graph 1 illustrates a highly significant step-change in activity in 2021, as the AADC comes into full effect. This led to a peak of 42 changes, the highest during the 2017–24 period studied. The changes then continue at a higher rate in the subsequent years.

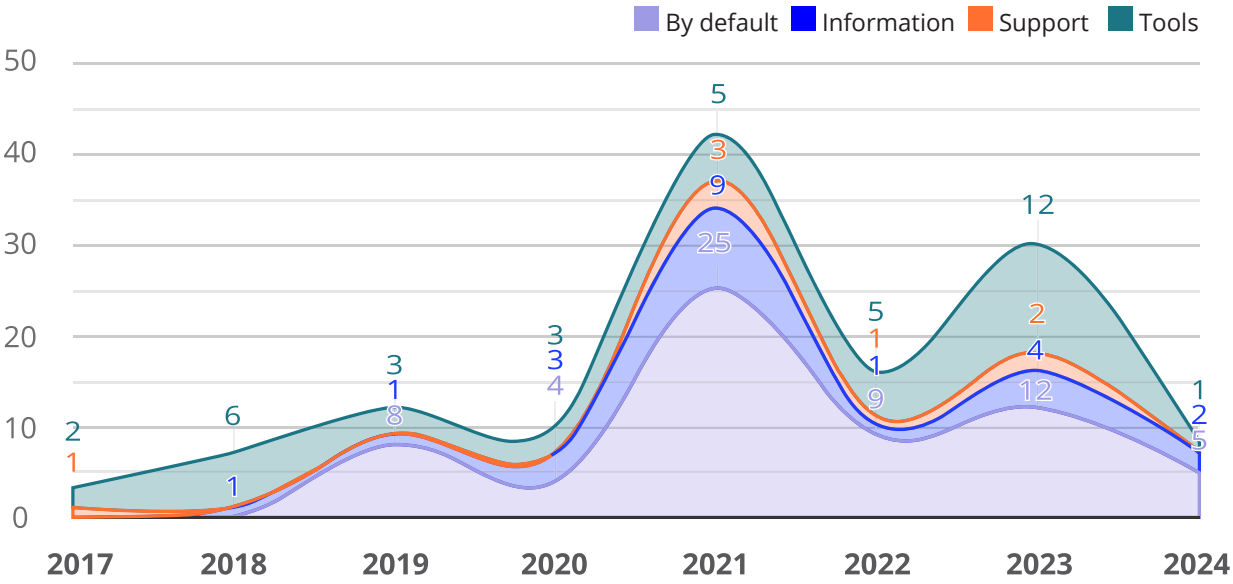
We can also discern a further significant rise in 2023 as the DSA comes into effect and the OSA was passed. The data for 2024 is incomplete as the research was completed in Q1 of that year, so no conclusions can be drawn about whether there is an upward trajectory. This also highlights the need to undertake this research later in 2025.

Graph 2 illustrates how the categories of change developed over time. The changes made between 2017 and 2020 are more focused on provision of tools to end users rather than design and system changes such as default settings. After 2020 the links become stronger and more direct; even if the companies do not explicitly recognise the legislation or regulation, the changes themselves comply with the legislation. For example, the peak of 25 changes under the 'by default' category in 2021 appear to have a clear link to the AADC.

Graph 1 - Count of changes for all four companies by year



Graph 2 - Categories of changes by year

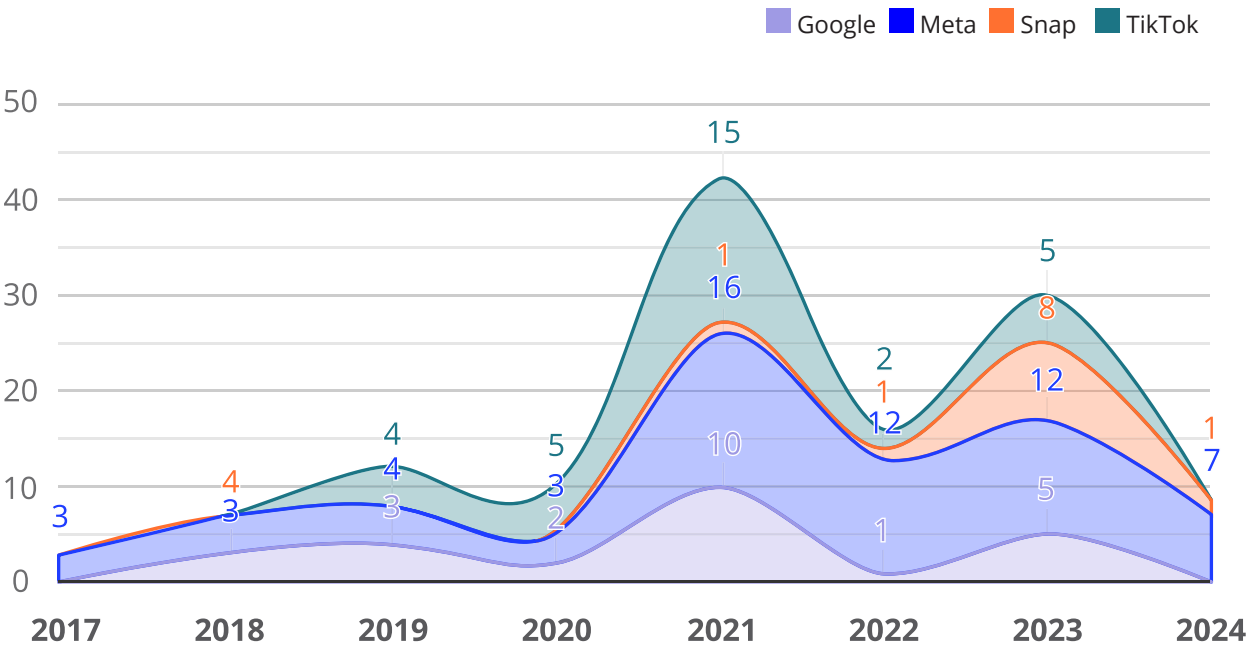


How do the number of changes for each company compare over time?

Graph 3 illustrates that Meta was the most visibly active company in terms of announcements, making 61 changes in total, followed by Google with 25, TikTok with 31, and Snap with 11.

The graph also shows that Meta, Google and TikTok all made a peak of changes in 2021, indicating the linkage with the AADC. Snap's peak of changes came in 2023, which may indicate a stronger reaction to the incoming DSA and OSA legislation and a later reaction to the AADC.

Graph 3: Number of changes by year for each company



Meta is currently the only platform with a published timeline of child privacy and safety-related updates, although it did not cover all the links we logged for this study and found elsewhere on its website (Meta, 2024). This highlights the importance of a consistent and regulated approach, to avoid selective presentations of information.

The fact that companies have announced more or less changes is not a direct indication of their compliance or the level of safety or privacy for children on their platform. It depends on the nature of the changes made, the range of different features the services have, the

starting point of the platform before they made the changes, and whether the changes are effective. It is also the case that an announcement may cover both large and smaller updates, so it depends on the granularity of what is covered in each case.

It cannot be assumed that all changes are captured, given the lack of access to companies' data for researchers, and there is an overdependence on companies themselves to record what they have done.

None the less, the data recorded for this project provides a valuable indication of how the companies approach transparency. It also highlights the importance of the risk reporting requirements in the DSA and OSA in ensuring that the largest platforms take a consistent approach to recording design changes. Publication of the risk assessments can enable researchers to better track how changes are linked to compliance risks and how the platforms perform over time. Also, the DSA (Article 40) is the only piece of legislation that has binding requirements on the largest platforms to provide vetted researchers access to data.

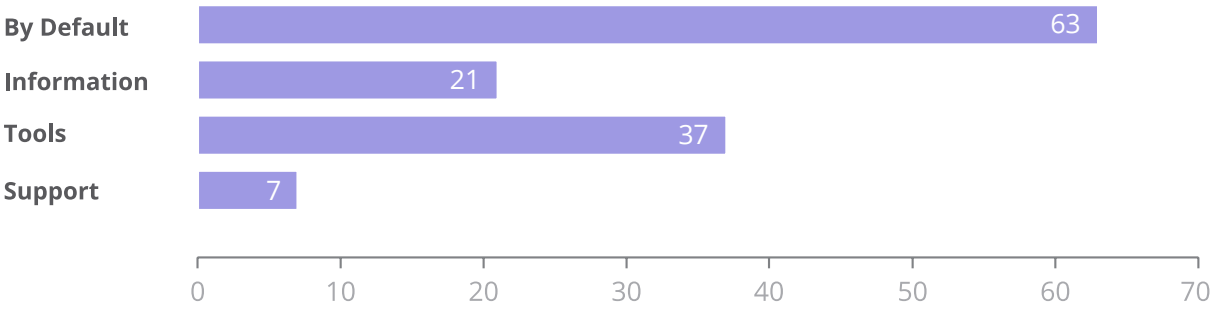
Which features of service design have been the subject of most development or updates?

Graph 4 illustrates that the 'by default' category was the most active area of change, followed by tools, information and then support. This highlights the significant impact of the 'by default' design concept as a regulatory measure. The low number of changes related to support is also an important area to highlight, and it is an area that was highlighted by children as ineffective in Ofcom's 2024 research, for example, reporting content concerns.

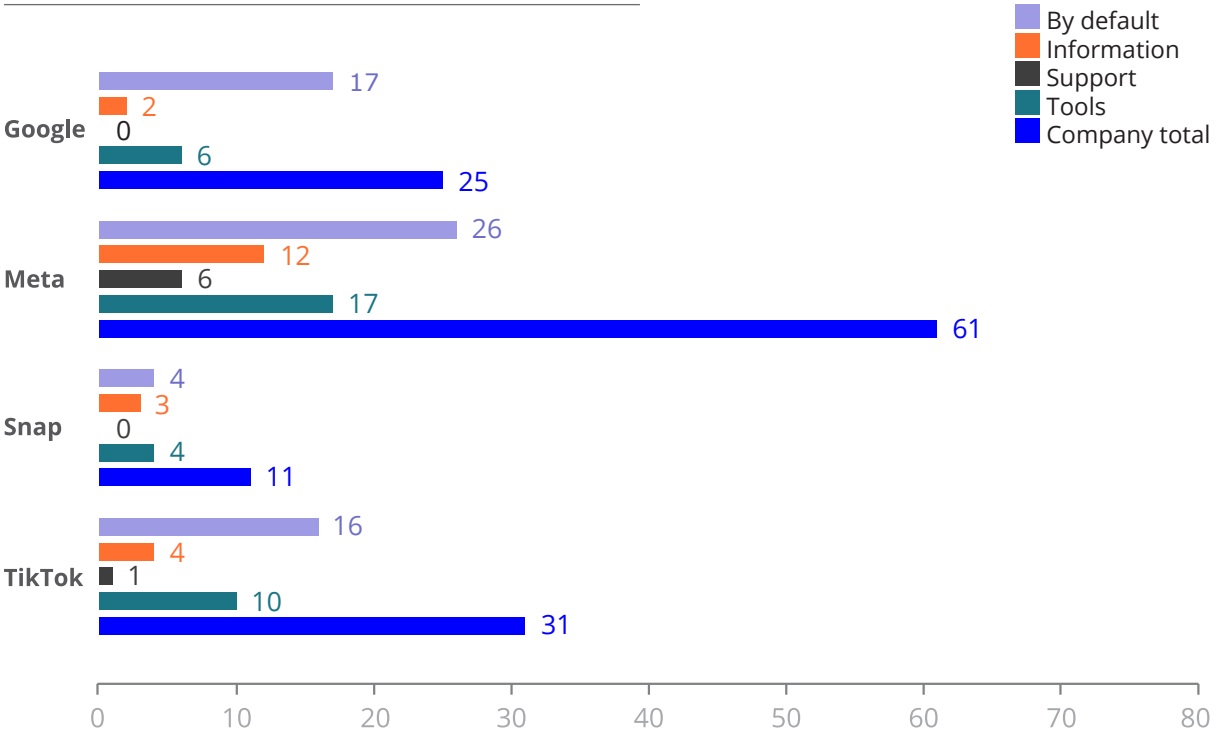
Graph 5 illustrates that Meta has provided the most changes in relation to 'by default' and tools. TikTok has also focused on both areas. This compares with Google that has focused most on 'by default'. Snap's changes are evenly distributed.

While noting that there will be differences in how the companies' online services operate and are provided to children, it is notable that there is a not a common approach emerging in terms of priorities for privacy and safety design changes.

Graph 4: Categories of changes across all four companies



Graph 5: Categories of changes by each company



Which of the online risks, as classified in the OECD typology of risks, are the changes addressing?

Graph 6 illustrates that, overall, all five of the OECD risk categories have been addressed – indicating the breadth of the changes now being made and the likely impact of legislation and regulation across a range of risk categories.

That content is the most prevalent risk category is also important as measures to address this area of risk are a feature of the OSA and DSA (although recognising the companies will have had longstanding obligations related to illegal content).

There is also clear evidence that content risks are being primarily addressed by changes that are by design and default, illustrating the impact of this concept from the AADC, DSA and OSA. It is notable that content risks are addressed by all four types of change.

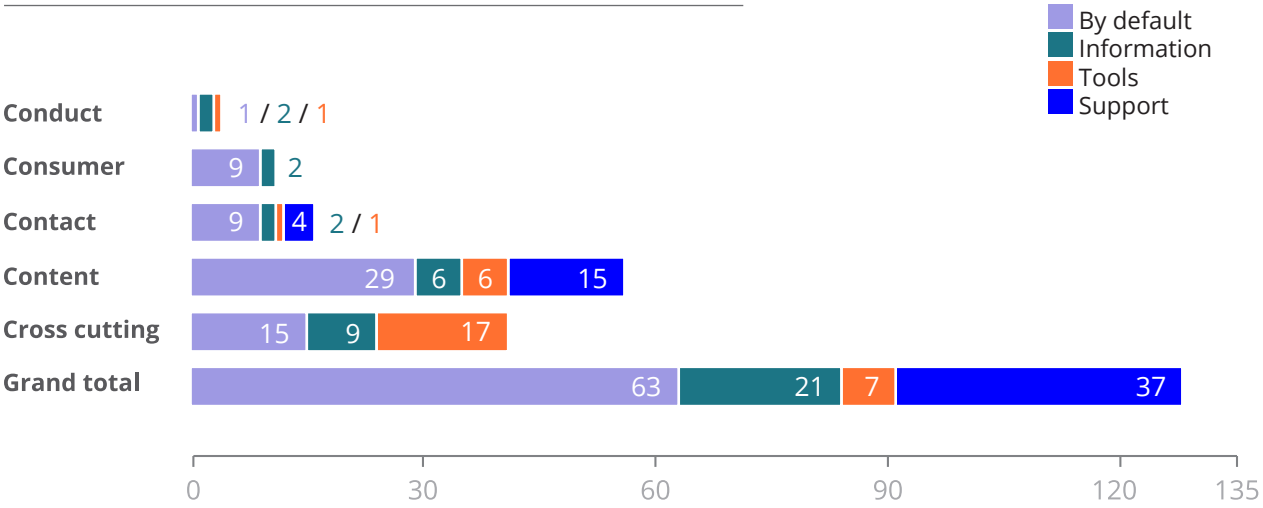
Cross-cutting risks were the second highest in the OECD categorisation; this includes privacy risks, highlighting the relevance of the AADC.

The changes related to consumer risks are significantly related to changes in targeted and behavioural advertising to children. Key drivers of this change are the AADC's focus on default settings and the DSA's prohibition on advertising to children based on profiling.

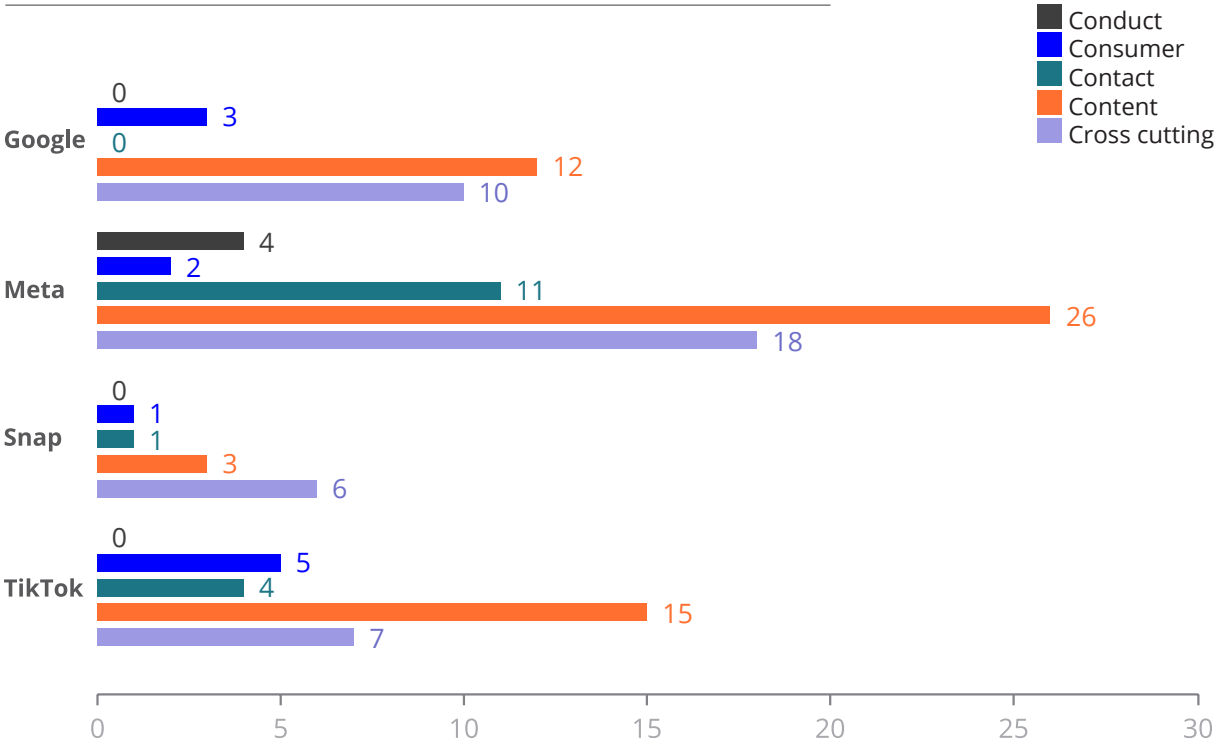
Changes categorised as addressing contact and conduct risk are considerably lower in prevalence. Companies have also announced a small number of changes of support measures for these areas, when support is often an important component of assisting children to address these risks.

Graph 7 illustrates that Meta, Google and TikTok have focused most on content risks in their announced changes, while Snap has focused on cross-cutting risks. Some of the differences can be explained by the differences in the companies' services – for example, Snap is often characterised as a social media messaging service, while Meta's Instagram and Facebook services, Google's YouTube service and TikTok all have a greater focus on user-generated content and algorithmic recommendations.

Graph 6: OECD risk category against categories of change



Graph 7: OECD risk categorisation of changes for each company



Detailed analysis of change categories

- What impact can we see from the legislation and regulation?
- Are there wider trends and impacts beyond individual service changes?

Category 1: By default

Key findings:

- Across the four companies, 63 changes were recorded under the 'by default' category.
- 2021 saw the highest number of changes, which was also the year the AADC came into effect.
- Meta announced the highest number of changes in this category. 'By default' changes were the highest category for all four companies.
- It is possible to discern an impact of the AADC, DSA and OSA, with the AADC's impact strongly apparent in 2021.
- Changes include a wide range of features, spanning messages, recommender systems, ad settings, content and age assurance.
- The evidence points towards legislation and regulation driving the four companies towards significant design changes that can provide substantive protections for children's privacy and safety.
- Further research would be required to discern the detail of practical benefits for children. Research would also need to consider whether children are evading these features by creating adult accounts, and how children change and update any settings.

Examples of changes:

- In July 2021 Instagram changed their default settings so that everyone under 16 (or under 18 in certain countries) is defaulted into a private account when they join.
- In 2022 Tik Tok announced new systems to help prevent content with overtly mature themes from reaching children.
- In 2023 Google introduced age restrictions on certain content about eating disorders.
- In November 2023 Google announced that YouTube was limiting repeated recommendations of videos related to certain topics for teens, e.g., content that idealises certain body weights.
- In November 2023 Google also announced safeguards for Bard, its generative AI tool. The safeguards seek to prevent unsafe content, such as illegal or age-gated substances, from appearing in its responses to teens.
- In September 2023 Snap made changes to require a greater number of friends in common before they can be recommended.
- All four companies have prohibited advertising to children based on profiling, starting with some restrictions in 2021 in response to the AADC moving to full implementation in 2023, in response to the DSA.

Standard 7 in the UK AADC is clear in its expectations of design privacy protections by default: 'Settings must be "high privacy" by default (unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child).' Standard 12 (profiling) in the AADC also states, 'Ensure features that rely on profiling are switched off by default (unless there is a compelling reason to do otherwise).' Changes 'by default' have significant potential to effectively protect children's safety and privacy as they focus on proactive measures that design in protections rather than safety after the event.

Of the 63 'by default' changes recorded, only 12 took place before 2021. A significant number of these changes (25) took place in 2021. It seems clear that this was a major area of implementation for these companies before the AADC took full effect in 2021. Twenty-one of the changes were also announced in the summer/early autumn, noting that the AADC took full effect in September 2021.

It is therefore likely that the initial driver in this area has been the UK AADC, but the OSA and DSA have reinforced the importance of settings as a protective safety design feature and pushed other new requirements, such as advertising restrictions.

A similar pattern is emerging in relation to the DSA and OSA, with a flurry of changes emerging in the immediate aftermath of the scope of the legislation being settled. One example would be a change that Meta made in January 2024, turning off teens' ability to receive DMs from anyone they don't follow or aren't connected to on Instagram, including other teens, by default.

In some examples default settings were updated so that they were permanently off; for example Google made this change for location history for under-18s.

The companies made changes to default settings across a range of features and services, including for video uploads and sharing, messaging, autoplay, virtual reality, comment filtering and search services. This illustrates that benefits to children's privacy and safety are accruing across a range of online scenarios.

By default: recommender systems

The AADC, OSA and DSA all require platforms to assess the risks caused by recommender systems, although the AADC's scope is on data and profiling. The focus the OSA and DSA place on algorithms and recommender systems is an important component of child safety regulation given the risk of accelerating children's exposure to harmful content. It is a priority area in Ofcom's draft codes and guidance (Ofcom, 2024c).

The design and engineering solutions used by the companies are essential in mitigating risk.

More of the changes made to recommender systems have occurred in 2022 and 2023, indicating that the explicit focus of the DSA and OSA may be the key driver. The changes made by the platforms sought to reduce the risk of the recommender systems promoting harmful content to children. This is therefore a positive impact, but the extent and effectiveness of these changes needs to be assessed.

Concerns about recommender systems are focused on how recommender feeds and search can narrow the information children see, and quickly aggregate large volumes of harmful or illegal content. Certain items of content may not be harmful in isolation but risk becoming harmful in repeated and rapid exposure (e.g., content related to body image). There is also a concern that recommender systems can draw children into the 'attention economy' at an early age when they struggle to find mechanisms to disengage or assess. Recommender systems can also suggest user accounts that children should follow or connect with, introducing contact risks.

Recommender systems can also enable children to find and engage with content that helps them in different life situations. As recommender systems intersect with content

availability, it is therefore important to recognise the freedom of expression implications as children's recommender system use is regulated.

The European Commission (2024a) has opened formal proceedings to assess whether TikTok may have breached the DSA in areas linked to the protection of minors, advertising transparency, data access for researchers, as well as the risk management of addictive design and harmful content. Their press release indicates that algorithms will be a key feature of the investigation (2024a).

The announcements also indicate that companies are starting to become more transparent about how recommender systems work, when previously this has been a closely protected area of commercial importance. The academic research community has highlighted the need to access data to understand the impact of recommender systems. Access is still inconsistent and often subject to restriction on use and publication (Davidson et al., 2023). The European Commission published a study on researchers' access to platform data in April 2024, with a view to informing the effective implementation of the DSA's requirement for vetted researcher access to data (European Commission, 2024d).

Studies have been conducted by NGOs to assess how recommender systems serve content to child users (CCDH, 2022; Reset Australia, 2021; Revealing Reality, 2021). These studies have been primarily conducted using avatars to replicate child users through profile characteristics and online behaviour, such as search and 'likes'. An exploratory research paper published by Ofcom in 2023 (Revealing Reality, 2023) also highted how avatars were exposed to potentially harmful and age-inappropriate content, and the value of using this research method. Further research of this type will be needed to fully assess the impact of the changes being made by the companies.

By default: age assurance

The companies made four announcements about age assurance mechanisms during the period surveyed. The DSA and OSA both make clear that age assurance is one of the mitigation mechanisms that platforms will need to use to prevent children from encountering harmful content and other risks. It is also a measure to ensure age limits in the terms and conditions are upheld. A report by 5Rights (2021) highlights that 'age assurance should not be mistaken for a silver bullet or a short cut to making the digital world fit for children … and its value lies not simply in the act of verifying or estimating age but in the enormous opportunity it brings once children have been recognised.'

The AADC also sets a standard for 'age-appropriate application' and a requirement that the platforms understand the age of users, proportionate to the risks, so that the relevant protections for children's personal data can be in place. The AADC provides an option for platforms to provide AADC standards for all users, which would negate the need for age assurance.

Age assurance can include age estimation as well as age verification (and may include behavioural detection to assess an individual is in the age range they claim).

It is also important to note that age assurance can have different purposes online:

- To verify whether someone is an adult (over 18).
- To verify whether someone is a teenager (over 13).
- To understand the age of the use to tailor an age-appropriate experience.

Age assurance is not necessary where a service is designed for all its users, including children. The AADC and OSA aim to give a child an age-appropriate experience and provide a clear message that this is possible without age assurance. It is notable that the last strategy has significant support from the child rights community and is supported by the UN General comment No. 25, which is sometimes overlooked.

The different age assurance purposes have challenges in terms of accuracy as you move down the list, and potential data protection risks in terms of excessive and intrusive data collection.

In relation to the DSA, the European Commission published a study on age assurance that assessed the benefits and risks of 10 different methods, and highlighted their position that 'age assurance is not a one-size-fits-all solution, it is an important tool for safeguarding children online' (European Commission, 2024e). This indicates the importance of assessing the impact of assurance methods in the context of each individual online service. The risks and benefits to children (and adult users) will need to be considered alongside the proportionality of the solution proposed. The fact that this study has just been released by the Commission also indicates that regulators and policymakers are still working to provide greater clarity.

It is important that age assurance is not used as a single solution aimed at blocking access, and the overall outcome of child safety regulation will be most beneficial for children if they are able to use and explore platforms in a way that takes account of their age and development capacity, not simply reducing their level of access.

The ICO also fined TikTok (currently under appeal) £12.7 million for GDPR breaches for the processing of personal data of children under 13 (2023a). In its action the ICO estimated that TikTok allowed up to 1.4 million UK children under 13 to use its platform in 2020. Ofcom's research indicates that it is common for 8- to 11-year-olds to have profiles on social media (Ofcom, 2023). This indicates that age assurance is clearly on the radar of regulators for future investigation.

For video-based platforms such as YouTube there are additional age assurance requirements from the AVMSD. In 2020, YouTube announced that if their systems are unable to

establish that a viewer is above the age of 18, they will request that they provide a valid ID or credit card to verify their age.

The only other announcements have come from Meta. This has included a change to ensure that all Instagram users enter a birthdate, and this was added as a sign-up requirement in 2019. In 2022 Instagram announced a test of a new system to verify ages when users attempt to amend their birth date. There are three options: upload their ID, record a video selfie or ask mutual friends to verify their age. The video selfie will use age estimation technology from Yoti. This is the first example of a major platform using a third-party age estimation tool and the use of facial biometric patterns. This is also a limited change as it does not yet cover new users signing up. The test pilot was expanded to more countries during 2023, but no results have been published.

This an area where there are a range of children's rights to be balanced – age assurance mechanisms, such as age verification using hard identifiers or biometrics, could unfairly discriminate and prevent children using platforms, reduce access to information that empowers children, or create privacy risks. There is also limited research on how age assurance is managed in the domestic context, for example, the situation for children with disabilities or refugees who lack government IDs, or those whose parents are in conflict about their digital activities.[12]

The ICO's formal opinion on age assurance for the AADC provides guidance on how platforms should use these technologies in compliance with data protection law (ICO, 2024a). The DSA also makes clear that online platforms are not obliged to process additional personal data to assess whether the recipient of the service is a minor. Ofcom, in its draft guidance (2024c), also stresses the right to privacy and the need to have effective 'effective' age assurance for primary priority harms, but to provide age-appropriate services in other less extreme circumstances.

There is also a question about the effectiveness of age assurance methods and how children can evade them, including with parental assistance. The companies could be concerned about making major changes to age assurance that immediately deny a significant number of younger users access to the platform. Facebook, Instagram, Snap, TikTok, X (formerly Twitter) and YouTube collectively derived nearly US$11 billion in advertising revenue from US-based users younger than 18 in 2022, according to a new study led by Harvard T.H. Chan School of Public Health (Raffoul et al., 2023). Given these incentives to retain younger users, this highlights the importance of independent regulation and oversight.

This is an area where legislation and regulation are likely to have a significant impact in the future, but from the announcements reviewed for this study there is evidence of evolutionary change in how the platforms are approaching age assurance. Future guidance from Ofcom and the European Commission will also be key in driving the direction. The

12 Further assessment of the impact on children's rights will be published as 'Children's rights and online age assurance systems: The way forward' by Sonia Livingstone, Abhilash Nair, Mariya Stoilova, Simone van der Hof and Cansu Caglar in the *International Journal of Children's Rights*: https://brill.com/view/journals/chil/chil-overview.xml?language=en

forthcoming ISO and IEEE (ISO/IEC 27566 and P2089.1) standards will also provide further direction. It will also be important for researchers to assess evidence from the tests undertaken by Instagram.

By default: illegal and harmful content

Both the DSA and OSA require platforms to take steps to assess the risks of illegal content being present on their platforms, and to ensure they have proactive measures in place to remove such content. The DSA and OSA do not expect platforms to remove legal but harmful content for all users, but both pieces of legislation expect platforms to take measures to protect children from the risks of harmful content. The OSA is focused in large part on risks to children from content that should be prevented (primary priority content) and that which should be age-appropriate (priority content). It also made it a requirement that no children should normally be able to access pornography.

All four companies have longstanding processes to detect and remove illegal content, including the use of AI as well human moderation. Effective and swift removal of child sexual abuse material (CSAM) images relies on industry-wide standards that enable platforms to share information. Google and Meta have been the most active in terms of explaining their approach. From the changes announced, it appears that the OSA and DSA are likely to be creating a renewed focus on risk mitigations, particularly for CSAM.

Further research and evidence will be required to see how effective the measures introduced by the platforms are, although it seems likely that legislation and regulation are moving the platforms to more tangible steps and with a greater degree of transparency. Further evidence from future transparency reporting under the DSA and OSA can also inform a more detailed analysis of this area in future research.

All four platforms already have content moderation policies as longstanding practices, and use AI to moderate and remove content that violates their terms and conditions, alongside changes to their recommender systems to make content less available.
In the UK Ofcom will provide further guidance about risk assessment and mitigations related to content that is likely to be harmful to children. We can therefore expect further steps to be taken and announced in due course.

From the evidence recorded, it appears that the companies are taking an incremental approach to harmful content in combination with their approach to recommender systems.

Changes have also been made to filter certain comments made on social media posts. This is a further indication of different ways that content harms can impact children and the various steps companies need to take.

The topic of harmful content is complex as it also intersects with freedom of expression and the right for children to also receive information; for example, information related to self-harm and body image may also include educational and supportive content. Companies will need to clearly set out how they address all full range of risks in their risk assessments.

By default: advertising changes

The DSA has the most explicit requirements related to advertising as it prohibits children receiving adverts based on profiling, if the platforms have a reasonable degree of certainty the user is a child. All four companies have now announced changes to comply with this provision in the DSA, in advance of it coming into force. The OSA does not cover advertising to children.

The AADC requires profiling for children to be switched off by default, unless there is a compelling reason in the best interests of the child. This includes use of children's personal data for targeted advertising. As some changes were also made in 2021, we can also discern an impact from the AADC in this area as well. For example, in 2021 Instagram, Facebook and Messenger changed their systems to only allow advertisers to target ads to those under 18 (or older in certain countries) based on their age, gender and location (not on their interests or other profiling).

Legislation and regulation have had a defined impact on children's exposure to targeted advertising. There are also several factors that will vary its impact, such as whether the platform accurately knows which users are children.

Rossi and Nairn (2024) conducted an online experiment with over 650 participants aged 11–78 to investigate whether consumers of all or any age could recognise social media content marketing as advertising. They found that children show significantly lower recognition rates for social media ads compared with adults. They also highlight that, irrespective of age, content marketing is universally challenging to identify compared to conventional ads. They also highlight the importance of these findings for gambling ads. This study illustrates the importance of safeguards for children related to advertising.

The changes made to ad settings in response to the AADC and DSA can play a role in reducing risk exposure from targeted advertising, although recognising that children will continue to be exposed to some forms of advertising online.

By default: overall observations

Overall, the move towards 'by default' changes can be seen as an area where legislation and regulation have had a significant impact on child privacy and safety. The default settings provide a safer space for children to connect, explore and learn online without the immediate pressures of widespread or unwanted contacts or exposure to certain forms of content. The default settings introduced can help reduce risks across the OECD categories. There is some evidence (Ng, 2019) that only a small percentage of users change settings from default, although dedicated research is needed with child users. Deceptive designs that suggest a service only works with less protective settings are also a risk.

Further research will be needed to measure the overall impact of these changes; it will also need to consider whether the companies' implementation of default settings impact children's ability to connect and engage with peers or receive information about important topics for their exploration and development, for example information related to mental health. Companies should also monitor whether default settings should be made permanent if evidence indicates there are significant risks from settings being changed to less protective options.

Category 2: Tools

Key findings:

- The research recorded 37 changes made related to tools across the four companies.
- 2023 saw the highest number of changes. The peak in 2023 may indicate that the companies sought to announce changes to tools as a response to the coming impact of the DSA and OSA.
- Meta announced the highest number of changes in this category.
- The driver of the changes to tools is likely to be a cumulative impact of legislation and regulation, as only the DSA specifically requires their consideration as a risk mitigation.
- The DSA's requirement for users to have an option for a recommender system not based on profiling has led to new tools being introduced. These tools are available to all users.
- Tools introduced include parental controls and tools that children can use themselves.
- Despite this being the second ranked area of change, the benefits of the tools are less clear, as there is no data available from the companies about how the tools are used, and academic research indicates that parental controls may be ineffective. Risks to child autonomy also require further research.
- The GDPR requirement for parental consent may also be a factor in the use of parental controls. The US COPPA may also have an influence on the use of parental controls globally.

Examples include:

- In 2020 Instagram introduced a tool to help users control who can tag and mention them (all users).
- In 2021 Google announced that parents can allow their children to access YouTube through a supervised Google Account.
- In 2021 TikTok introduced a 'filter all comments' feature.
- In 2022 Instagram announced a tool that allows users to see their feeds in chronological order.
- In 2023 TikTok announced that they were introducing a tool that allowed users to switch off personalisation. This was in response to the DSA requirement that this option be available to all users (although the DSA is silent on what the default should be).
- In 2023 Snap announced a similar change to TikTok that would allow users to opt out of a personalised Discover and Spotlight content experience.
- In 2024, Snap expanded their in-app parental tools and Visibility into Their Teens' Settings.

Tools: parental controls

All four companies offer a feature so that parents can set controls for their children's accounts. The announcements indicate a growing granularity and sophistication in how the controls can work, and they are also added to products with different types of interaction, such as Google's voice assistant and Meta's virtual reality products.

It is possible that companies continue to enhance and develop parental controls in response to legislation and regulation. The driver of the changes to tools is likely to be a cumulative impact of legislation and regulation, as only the DSA specifically requires their consideration as a risk mitigation.

The AADC does not require the use of parental controls, but does cover the use in Standard 11, although from the perspective of achieving balance with a child's autonomy: 'If you provide parental controls, give the child age-appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored.'

Parental controls can be viewed as a measure to enable parents and children to agree boundaries and ways to progressively explore the features and information available on the platforms. But there are also risks in their use, such as false security, controlling be-

haviour by family members or others, and children not taking responsibility for some aspects of their learning and life necessary to mature.

Parental controls may be viewed as an attempt to transfer responsibility to parents regarding the child's use and potential exposure to risks. Many campaigners for children's rights see a risk that companies are outsourcing the responsibility for their services, and see a design of service approach with default measures as the key priority (and not parental controls).

There is considerable concern that parental controls give a false sense of security, particularly those related to GPS tracking, and that the 'over-surveillance' of children might impact on their own development as regards risk.

Finally, there is concern that it shifts responsibility for safety from the company to the parent who may not be able to make meaningful changes to the service other than binary decisions about access or not. The benefits, as children get older, become less clear.

Stoilova et al. (2024) conducted a rapid evidence review to identify which families use parental controls and why, and the outcomes of such use, beneficial or otherwise. The research indicated the following:

> *The available research revealed that the use of parental controls depends on the age of the parents and children, their digital skills, parental involvement, and the motivation to reduce exposure to online risk. However, the consequences of use were mixed, with evidence of parental controls having both beneficial and adverse outcomes, limiting other outcomes or simply having no outcomes. While the review found little support for advocating parental controls as a stand-alone strategy, parents valued them when embedded in a broader approach to parental mediation and parent – child relations.*

A report in *The Washington Post* (Nix, 2024) quoted internal company sources from Meta about parental controls: 'fewer than 10 percent of teens on Meta's Instagram had enabled the parental supervision setting, according to people familiar with the matter who spoke on the condition of anonymity to discuss private company matters; of those who did, only a single-digit percentage of parents had adjusted their kids' settings.'

While this news report is unverified and may not reveal a full picture of evidence, it illustrates the importance of further research, and transparency from the companies, to better assess the effectiveness of parental controls and what role they should play as a risk mitigation measure in response to legislation and regulation. Further research should also explore how controls can impact on children's autonomy, particularly as they move from tween to teen.

There are a range of settings with the controls offered by all four companies, from paren-

tal restriction to parental accompaniment.

It is also relevant to note that several parental controls do recognise the autonomy and privacy of the child in some features. For example, on Snap's Family Centre parents can also see who their child has communicated with over the last seven days (but not the content of those conversations) – although children will have to agree before their parent can begin monitoring. The parental tools are becoming more sophisticated, and we can see an evolution of the more traditional filtering or restrictive approach to also offering a paired or linked service that provides certain conditions under which an access or feature request is put through a dialogue process.

Parental controls have a long and varied history, and this suggests a more indirect relationship to legislation. They have been promoted as a self-regulatory measure that has featured prominently in the use of mobile devices and social media services over several years, including by bodies such as the Global System for Mobile Communications (GMSA), CEO Coalition and Alliance for a Better Internet.

Overall, it seems likely that a complex range of factors are driving the use of parental controls. The DSA also makes references to controls as a mitigating measure to risk, while the OSA does not directly mention them. The US COPPA and the EU GDPR, which both have requirements related to parental consent, will also play a role. The EU AVMSD also requires parental controls.

Tools: user controls

Companies are also making privacy and safety controls available for children (or in some cases, all users) that enable them to make their own choices about safety online.

The DSA requires non-personalised content feeds to be available to users, but doesn't specify that they should be set as a default setting. This is a requirement for all users rather than just children, although children can use it. This DSA requirement has now been addressed by all four platforms as a tool that users can use to set a preference.

This DSA requirement is an area that will require further research, to see how many users, including children, select the option for non-personalised feeds. Research should also consider how prominent and easy it is for children to make a change. This may also raise questions as to whether default settings should be used in this area, rather than a tool that a user has to proactively seek out.

Other tools that have been introduced provide opportunities for children to control risks themselves. Several changes related to comment filtering tools (Meta and TikTok), for example.

There are also questions about the effectiveness of content controls. Research by Ofcom (2024b) covered a nationally representative sample (those aged 16+) of social media/video-sharing platform users (thus including some older children). The findings indicated that: 'about a quarter of users (26%) said they have used content controls at least once. After using content controls, only 38% said their experience improved, while 44% said their experience didn't change, 2% said it got worse and 16% said they didn't know.' Ofcom defines content tools as 'personalised settings provided by social media and video-sharing platforms. These controls enable users to manage the content they see online and avoid encountering harmful or upsetting content.'

Tools: overall observations

Legislation and regulation have played a role in cumulatively driving changes to tools, the DSA and AADC having had the most notable influence. The OSA will have greater influence in future when Ofcom addresses the issue in their code of practice and guidance on children's safety duties. The other driver is that companies are seeking to use tools as a proactive response to legislation and regulation, even if they are not a primary requirement. The relationship between legislation and regulation and parental controls is more complex. Further research is needed about their effectiveness and consideration from regulators about how they should feature in codes and guidance.

Category 3: Information

Key findings:

- The research recorded 21 changes made related to information provision across the four companies.
- 2021 saw the highest number of changes, which was also the year the AADC came into effect.
- Meta announced the highest number of changes in this category.
- It is possible to discern an impact of the AADC, DSA and OSA, with the AADC's impact clearly discernible in 2021.
- The information provided covers a range of scenarios – safety, privacy and wellbeing.
- The provision of information and further transparency may have benefits in empowering some children and parents, in conjunction with other safety measures, such as default settings.
- There is a risk that companies over-promote the value of information measures as an empowerment tool without evidence to support the tangible impact.

Examples of changes:

- In 2021 Instagram introduced safety notices in DMs for suspicious behaviour.
- In 2018 Google created a new Safety Center.
- In 2023 Snap introduced a pop-up warning for teens if someone tries to add them as a friend when they don't share mutual contacts or the person isn't in their contacts. They also introduced in-app education about common online risks.
- In 2020 TikTok produced an age-appropriate summary of their privacy policy, called 'privacy highlights'.

Throughout the period studied, the companies have continued to improve the provision of information to children and parents. These mechanisms can allow users to make informed decisions about how they use the platform and how to use settings and other features. They can also nudge or guide vulnerable users to help.

Standard 4 of the AADC focuses on transparency. It has been a particular criticism of the sector that terms of service, privacy notices and community rules have been written in complex legal language that is far beyond the reading age of the children they are engaged with.

Standard 13 of the AADC highlights the importance of positive nudges for children, and makes clear that nudges that lead to poor privacy choices are likely to be unfair under the GDPR. The requirements in the DSA and OSA for platforms to take measures to reduce the risk of harm from the design of the platforms can also include proactive measures that provide information to children related to safety and wellbeing.

Linked to these information and controls, the platforms have introduced screen time nudges as a positive mechanism to change screen time behaviour. The changes that have been announced seek to address concerns about how social media use may affect sleep and other areas of child development. One example is the night-time nudges announced for Instagram in 2024 – the nudges show up when teens have spent more than 10 minutes on Instagram late at night.

The impact of time that children spend on online has been the subject of considerable debate and concern, including from parents, but there is still no definitive evidence that screen time is negative for children's cognitive development and wellbeing (see Miller et al., 2022). Any research into the impact of screen time nudges will need to be considered in this context.

It therefore seems likely that the AADC, DSA and OSA have promoted and encouraged platforms to use nudges that are positive in intent related to child safety, but further research is needed into the specific nudges the platforms have started to use.

A key consideration for further research will be whether the information provided by these changes is provided at an effective point of the child's online experience and whether there is engagement – the 'right information at the right time'.

Category 4: Support

Key findings:

- The research recorded seven changes made related to support across the four companies. This relatively low number introduces an important question about whether the companies are focusing enough on developing and updating their support features.
- 2021 saw the highest number of changes, and they continued after this period.
- Meta announced the highest number of changes in this category.
- The number of changes in 2021 may be due to the platforms reacting to political scrutiny and the emergence of daft legislation on safety.
- The most likely drivers in this area are the DSA and OSA, as the tools introduced relate to content reporting or reporting other users.
- Support measures can be a valuable mechanism to children to empower them to act against risks they see online.
- Future transparency reporting under the DSA and OSA may provide further evidence on how these features are used and to what extent children use them.

Examples of changes:

- In 2022 Facebook and Instagram introduced a new mechanism to prompt children to report accounts to the service after they block someone.
- In 2021 TikTok launched a feature that gives users the ability to delete multiple comments at once or report them for potentially violating community guidelines.
- In 2023 Meta joined Take It Down, a new platform designed to proactively prevent young people's intimate images from spreading online. Take It Down allows people to only submit a hash value, rather than the intimate image or video itself, to the National Center for Missing & Exploited Children (NCMEC).

A requirement for platforms to offer tools to enable users, including children, to report concerns, including content or other users, is a feature of both the DSA and OSA.

The DSA and OSA are likely to place greater emphasis on the accessibility, usability and responsiveness of reporting mechanisms, particularly for children. These changes can be seen as anticipating the expectations of the DSA and OSA.

7. Findings: How do the companies' actions compare to their statements about legislation and regulation to Parliaments?

This section analyses statements by the companies during the passage of the legislation and other parliamentary inquiries, and compares this with their actions.

Key findings:

- The companies raised concerns about the OSA during its passage, about age assurance and how to deliver age-appropriate services.
- This indicates a likely area of tension between regulators and companies, and platforms may be less likely to explain the detail of changes they make.
- Although the companies made public commitments to implementing the AADC, the Netchoice case in California indicates that the companies have not accepted the full requirements of the AADC.
- Positive statements have been made about the AADC, but there is less specific detail about what steps companies take to conform in practice.
- Evidence submitted to US Senate Committee hearings indicates inconsistencies in transparency across the companies and the impact of the measures they take, including parental controls.

Research was conducted on the websites for the UK and EU Parliaments and the US Congress during the period 2017–24 (sources referenced at the end of the report).

Formal records of hearings and written evidence submitted were reviewed, to identify any statements the four companies had made about regulation related to children's safety. The research covered inquiries on the general topic of children's safety and specific evidence submitted related to draft legislation. The most valuable evidence was found in that provided to the UK Parliament and US Congress, which is detailed below. This evidence provides context for their approach to compliance and engagement with the AADC, OSA and DSA.

UK Parliament, passage of the OSA (also includes comments about the AADC)

In evidence to the UK Parliament the companies made similar points in relation to the Online Safety Bill:

- Concerns about whether the Bill was sufficiently reflective of its intention to be risk-based and outcome-focused.
- While the platforms had previously voiced concerns about the AADC (ICO, 2019), in the evidence on the Bill the platforms were more positive about the AADC and the steps they had taken to implement it. Their concerns were that the Bill was not sufficiently aligned with the AADC in relation to aspects such as age assurance.
- They raised concerns about implementing the Bill's child-focused content provisions, as they argued it required them to implement age assurance methods that could create tensions with the AADC and the collection of additional data about children.

In evidence to the UK Parliament (Draft Online Safety Bill Committee, September 2021), written evidence submitted by Google UK highlighted their commitment to the AADC:

> *Over the years, we've been significantly investing in the policies, products and practices to help us protect kids and their privacy. This includes implementing additional protections for children and teens on our platforms to comply with the ICO Age-Appropriate Design Code.*

The evidence called the Online Safety Bill complex and requested clarification on:

> *Ensuring that the Bill will not lead to widespread automated monitoring of content, which would result in the over-removal of legal content that users should have access to... Ensuring that Ofcom's assessment of proportionality protects UK users' privacy and rights to share/access information.*

Meta's submission to the Online Safety Bill Committee (September 2021) recommended the following:

> *The Committee should advocate for a proportionate and risk-based approach to age assurance. Age assurance should not be a single-step process, but rather a collection of ongoing efforts that work dynamically to provide effective solutions, jointly with safety and privacy safeguards. The UK Online Safety Bill should allow for the age verification space to evolve and to foster innovation by adopting a technology agnostic, 'future proof' approach, Government should encourage a broad collaboration among all stakeholders who must be involved, including regulators, experts, industry, parents and children.*

At the Department for Digital, Culture, Media & Sport (DCMS) Select Committee (House of Commons, September 2020), Theo Bertram from TikTok addressed a question about the impact of the AADC: *'It is already changing our business operations. I think it is one of the most forward looking, interesting pieces of legislation. It is very interesting to see child safety being driven by a data protection authority in those terms.'*

US Senate hearing, 'Protecting Kids Online: Snap, TikTok, and YouTube' (comments about the AADC)

In the USA, Michael Beckerman (2021), TikTok's Head of Public Policy for the Americas, told the US Senate Subcommittee on Consumer Protection, Product Safety and Data Security:

> *We have voluntarily implemented much of the Age-Appropriate Design Code here in the United States. I agree that companies can do more … and that is the approach we are trying to take, to do more and go above and beyond and to be a place where we are putting wellness of teenagers and safety of teenagers ahead of other platforms… We strongly and enthusiastically support that kind of child safety law.*

At the same hearing, Jennifer Stout, Vice President of Global Public Policy at Snap, said:

> *We of course complied with the Code as it's come into force this year and I mentioned we are looking actively at that Code to see how we can apply it to outside the UK market and apply it to many of our other markets.*

The Netchoice v. Bonta court case in California, where Netchoice (2022) sought an injunction against the California AADC on first amendment grounds, offers a counterpoint against these statements. As Meta, Google, TikTok and Snap are all Netchoice members, this indicates a potentially contradictory position against the positive engagement the companies have presented about the AADC in a UK context.

US Senate hearing on Big Tech and the online child sexual exploitation crisis

The US Senate Committee on the Judiciary held a hearing in January 2024, with witnesses from Meta, Snap, TikTok, X and Discord. The witnesses also submitted written evidence in response to questions after the hearing. In March the Committee published the companies' responses. A detailed analysis is beyond the scope of this report, but there are some relevant points to draw from the written evidence submitted.[13]

There are significant differences in transparency between the responses. One important area to highlight is in the use of parental controls. TikTok did not supply this information to the Committee, citing commercial confidentiality. Snap did supply this information, indicating that 400,000 children use parental controls out of 60 million users under 18. This indicates a usage rate of 0.67%, which is an interesting contrast to the prominence that parental controls have in the announcements analysed in the Chapter 6. Snap's global revenue in 2023 from minors was approximately US$437 million, which was also a question that TikTok did not answer (US Senate Committee on the Judiciary, 2024).

It is relevant to note the lack of tangible evidence the companies submitted in response to questions about the effectiveness of the measures they use to protect children. The companies' responses only referenced transparency reports published that cover quantitative data on issues such as accounts removed for being underage, but little substantive evidence on efficacy. We return to this area in Chapter 11.

13 Note that Meta had not submitted full responses to all the questions at time of writing this report.

8. Findings: What privacy and online safety changes have been made on other services?

In this section we explore how legislation and regulation have impacted child privacy and safety protections in other social media companies and in the gaming sector. This is based on information supplied in response to the letters sent to 50 companies as well as other information from public announcements and updates on company websites.

These examples do not have the volume of data compared to the four companies covered in Chapter 6, but do provide further insight as to changes being made and the impact of legislation and regulations.

Key findings:

- There are further examples of social media companies implementing changes by default, information and tools.
- The evidence of changes made by Pinterest indicate a focus on 'by default'. These changes suggest significant impact from the AADC and DSA.
- Yubo provides an example of a social media company going further with age assurance than others in the market.
- There is also significant evidence of child privacy and safety changes being made across the gaming industry.
- These changes span all four categories: by default, tools, information and support.
- It highlights the importance of the legislation and regulation spanning a wide range of sectors and not just social media.
- In the gaming industry there is evidence of responses to the AADC (high default privacy settings) and DSA (changes to ad targeting for children).

Other social media companies

Pinterest

The research study has also considered changes that have been introduced by Pinterest, a social media platform that is regularly listed in the top 10 used by children. In 2023 Pinterest made the following changes to relevant to child safety.[14]

By default

- For users under the age of 16, followers will be removed so that they can decide who gets to follow them.
- Users under 16 will only be able to send and receive messages from mutual followers who have been accepted through a unique profile link that expires, or when they get five new followers with a shareable link.
- Private by default accounts, including for those aged 16–17.
- An updated age verification process – if birth dates are edited, a user will have to confirm with a third-party system.
- No targeted paid advertising to users between the ages of 13 and 17 in the UK and EU. The timing also indicates the impact of the DSA.

Tools

- Parental passcode feature added.

Yubo

The social media platform Yubo has implemented the following child safety features:

By default

- Every new user is required to pass an age estimation solution (powered by Yoti).[15]
- Age gates are in place to separate adults from minors on the platform where possible (depending on the features and age difference).

Information

- Pop-up alerts before users share their personal data (phone number or address), to make them confirm before sharing data and raise their awareness on privacy.
- Warnings to users to make them aware of inappropriate behaviours, requiring them to stop before any harm is done (e.g., in case of bullying).

14 https://newsroom.pinterest.com/en-gb/news/new-features-enhance-teen-safety-on-pinterest
15 www.yubo.live/blog/goal-100-age-verified-users-on-yubo

Tools

- User settings to manage their privacy preferences: option to turn off geolocation, push notifications, discovery features and cookies. Users can also download a file containing their data and permanently delete their profile at any time.
- An option to block users, mute words they don't want to see, and report any inappropriate content, profile or ad.

Gaming sector

Information about changes introduced by several major gaming companies was sourced from announcements on their websites. They also process significant personal data about children, and many services contain social interaction functions and messaging.

The companies are all subject to the GDPR and AADC, and their functions related to user-generated content will be caught by the OSA. The DSA will also apply to content moderation and online advertising on gaming platforms (Ng, 2024). The information gathering is not exhaustive across the sector, but provides further examples to illustrate the changes being made.

The companies covered in this section (from online research) are:

- PlayStation (Sony Interactive Entertainment)
- Xbox (Microsoft)
- Roblox
- Epic Games

By default

- In 2023 Microsoft announced an updated account creation process, which now requires players to first identify date of birth, and if under 13, to obtain verified parental consent, before providing any information such as phone number or email address.
- In 2023 Roblox announced that advertisers will no longer be able to select gender when creating ads that reach users aged 13–17 in Europe – as part of an announcement explaining how they are complying with the DSA.
- In 2023 Roblox implemented new policies, disallowing advertising in experiences accessible to under-13s (going further than the legal requirements).[16]
- In 2023 Roblox implemented new 'experiences' for those verified as aged 17+.[17]
- In 2022 Epic Games introduced 'Cabined Accounts', which allow under-13s to play before they obtain parental consent. This means that Epic doesn't collect any personal data. In practice, this means certain features (including voice chat and pur-

16 https://kidscreen.com/2022/10/26/roblox-removes-ads-and-sponsored-opps-for-non-teens
17 https://blog.roblox.com/2023/06/introducing-experiences-for-people-17-and-older

chasing) are switched off. Full accounts are subject to verified parental consent.[18]
- In 2022 Epic Games implemented high privacy default settings for players under 18. Chat defaults to 'Nobody', profile details default to 'Hidden', parties default to 'Invite Only', and personalised recommendations are defaulted 'off'. Players under 16 also have the mature language filter defaulted to 'on' for text chat.[19]

Tools

- In 2021 PlayStation announced personalised settings to control interaction with others, including friend requests.[20]
- In 2022 Roblox upgraded parental controls that allow parents to choose between '13+', '9+', or 'All Ages'.
- In 2019 Epic Games introduced in-game parental controls.[21]

Information

- In 2022 PlayStation introduced a privacy account, security and online safety web-page.[22]
- In 2023 (as part of an FTC settlement – see Chapter 8) Microsoft updated their privacy statement for Xbox, including a new explanation on how data is processed.[23]
- In 2023 Microsoft updated Xbox Family Hub with information about creating a family group and managing child accounts, to help parents and caregivers understand the safety measures.[24]
- In 2023 Microsoft released Minecraft's Privacy Prodigy, aimed at teaching young people about privacy and how to safeguard their sensitive personal information.[25]
- In 2024 Roblox announced additional transparency measures about ads, recommendations, ranking and content moderation.[26]
- In 2022 Roblox launched age recommendations for each experience; this indicates which age group an experience is suitable for: 'All Ages', 'Ages 9+', or 'Ages 13+'.[27]

Support

- In 2021 PlayStation introduced a new Voice Chat reporting function, to help in the reporting of inappropriate behaviour, including Community Code of Conduct violations.[28]
- In 2023 Epic Games introduced voice reporting, including audio evidence submission.[29]

18 www.epicgames.com/site/en-US/news/introducing-cabined-accounts-a-new-way-for-kids-to-join-the-metaverse
19 www.epicgames.com/site/en-US/news/epic-ftc-settlement-and-moving-beyond-long-standing-industry-practices
20 https://sonyinteractive.com/en/news/blog/continuous-enhancements-to-ensure-a-positive-experience-for-all-players
21 www.fortnite.com/news/parental-controls-have-arrived?lang=en-US
22 https://sonyinteractive.com/en/news/blog/playstations-new-privacy-account-security-and-online-safety-webpage
23 https://privacy.microsoft.com/privacystatement
24 www.xbox.com/community/for-everyone/responsible-gaming
25 https://news.xbox.com/en-us/2023/02/06/xbox-safer-internet-day-2023
26 https://devforum.roblox.com/t/changes-we%E2%80%99re-making-as-the-digital-services-act-dsa-takes-effect/2837088/1
27 https://devforum.roblox.com/t/experience-guidelines-age-recommendations-parental-controls/1982517
28 https://blog.playstation.com/2020/10/16/details-on-new-voice-chat-functionality-coming-to-ps5
29 www.epicgames.com/site/en-US/news/introducing-voice-reporting-in-fortnite

9. Findings: How have changes in privacy and safety for children been driven by regulators' actions?

This section explores whether changes have been driven by regulators, and what legislation has been most influential. It also recognises the role of other legislation, such as the GDPR and COPPA.

Key findings:

- The importance of regulatory oversight and enforcement action is an important factor in driving changes to the design of platforms to protect children's privacy and safety.
- The evidence so far primarily relates to the AADC, GDPR and US COPPA as the OSA and DSA are still at earlier stages of implementation, but also serve as an illustration of the importance of regulatory action for safety regulation.
- There have been important actions under the GDPR and US COPPA, which indicates this legislation will play a role alongside the DSA and OSA.
- The ICO is yet to take formal action related to the AADC, although the latest strategy in 2024 indicates the ongoing priorities, and the ICO should evidence how the strategy has been effective.
- The importance of a clear 'end to end' regulatory strategy, with published enforcement priorities, can also be a relevant factor in driving change.

UK AADC and GDPR, ICO action

The ICO has taken a proactive approach to implementation, writing to 55 companies asking for information about how their online services accessed by children conform to the

code (ICO, 2021). This has resulted in 11 audits[30] and the assessment of 44 companies, and some investigations are ongoing at the time of writing.

The ICO has also provided additional resources and tools to support implementation, such as a harms framework, age assurance guidance and sample data protection impact assessments (ICO, n.d., b).

Civil society groups, including 5Rights, have also submitted complaints.

In April 2024 the ICO published a new strategy with their priorities for protecting children online 2024–25. The strategy contains four priorities (ICO, 2024b):

1. Default privacy and geolocation settings.
2. Profiling children for targeted advertisements.
3. Using children's information in recommender systems.
4. Using information of children under 13.

These priorities indicate that the ICO sees further areas where online services need to improve their conformity with the AADC. The ICO will need to evidence how this strategy can deliver further change and impact, including use of enforcement action for systemic breaches of the law.

The ICO issued a preliminary GDPR enforcement notice against Snap (2023b) over a potential failure to properly assess the privacy risks posed by its generative AI chatbot 'My AI'. The ICO's investigation provisionally found that Snap failed to adequately identify and assess the risks to several million 'My AI' users in the UK, including children aged 13–17. Although this announcement was made in October 2023, the full notice has not yet been published, and it expected that the ICO will make a further announcement about the conclusion of the case later in 2024. The announcement illustrates the importance of AADC Standard 2 (data protection impact assessments, DPIAs).

EU GDPR, guidance and enforcement

One of the most important Data Protection Authorities under the EU GDPR is Ireland, as many online platforms have their EU headquarters there. Ireland is therefore the lead authority for investigations and enforcement for these companies under the GDPR's one-stop shop system for cross-border cases. The fines and sanctions reflect that cross-border context. The Data Protection Commission in Ireland has produced specific guidance: *The fundamentals for a child-oriented approach to data processing* (2021). While not binding, the guidelines contain similar elements to the UK AADC.

The Irish Data Protection Commission fined TikTok €345 million for breaches of GDPR related to processing of children's personal data (2023). The fine related to TikTok's platform

30 For example, ICO's voluntary audit of Mediatonic Games: https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/4021238/mediatonic-audit-20220803.pdf

settings, including public-by-default settings as well as the settings associated with the Family Pairing feature. The breaches also covered the fairness principle, the use of dark patterns and nudging towards privacy intrusive options.

The Italian Data Protection Authority (GPDP) acted against the AI chatbot Replika on the grounds that it did not contain any age assurance mechanism to ensure that safeguards for protection of children's personal data were being applied (GPDP, 2023a). The US-based developer, Luka Inc., was ordered to terminate processing of data relating to Italian users and to inform GPDP within 20 days on any measures taken to implement the orders.

The GPDP also took similar action against OpenAI, the developer of ChatGPT, on the grounds that it did not verify the age of its users (GPDP, 2023b).

In March 2024 the Spanish Data Protection Authority (AEPD) took out an injunction that prevented Worldcoin (a digital ID and cryptocurrency service) from continuing to process personal data in Spain for three months. The order cited breaches of the GDPR related to children's personal data (AEPD, 2024b).

The GDPR therefore also plays an important role in protecting children online, while we recognise its focus on data rather than content or wider harms from digital design.

Initial DSA enforcement

While still at an early stage of implementation, the European Commission has already had an impact with its investigations. In April 2024 it commenced an investigation into the Tik-Tok Lite app under the DSA (European Commission, 2024f). The app offers rewards such as gift vouchers for watching videos.

The Commission said it was minded to impose interim measures that could force the company to suspend access to the TikTok Lite app in the EU while it investigated concerns the app posed mental health risks to users, including children. Tik Tok then wrote to Digital Commissioner Thierry Breton to announce it would pre-emptively suspend the service.

While the Commission's claims that the app could be addictive to children will need to be substantiated with valid evidence, it is a further example of the DSA having an impact on a service that was deemed a possible risk to children. The investigation will focus on whether TikTok undertook an effective risk assessment and mitigation measures prior to its launch.

US FTC enforcement action under the COPPA and consumer protection laws

In December 2022 the FTC secured agreements requiring Epic Games, Inc., creator of video game Fortnite, to pay a total of US$520 million in relief over allegations the company had violated the COPPA and deployed design tricks, known as dark patterns, to dupe millions of players into making unintentional purchases. The FTC findings also alleged that Epic collected personal data from children without first obtaining parents' verifiable consent. They also included a finding related to default settings that live on-by-default text and voice communications for users caused harm to children. Epic has subsequently made changes to their platform, as covered in Chapter 8, illustrating the impact of regulatory action on issues such as default settings (FTC, 2022).

In 2023 the FTC acted against Microsoft via an order filed by the Department of Justice. Microsoft was required to take several steps to improve privacy protections for child users of its Xbox system. For example, the order extended COPPA protections to third-party gaming publishers with whom Microsoft shares children's data. The order also found that avatars generated from a child's image, and biometric and health information, are covered by the COPPA Rule when collected with other personal data (FTC, 2023b).

10. Findings: What role has civil society played in driving changes to children's privacy and safety?

Key findings:

- The important role of civil society organisations in bringing cases about children's safety and privacy is highlighted.
- The case study illustrates how changes for all users can be used to provide protection for children and avoid the use of age assurance.
- Civil society cases will be important under the OSA, which contains provisions that allow for 'super-complaints'.

UK AADC, Poki: an example of changes made following civil society engagement

The 5Rights Foundation published a case study that explained how Poki,[31] a free gaming platform with more than 60 million users worldwide, has changed its UK service to comply with the AADC (5Rights Foundation, 2024).

5Rights approached Poki with evidence that its platform was not conforming to the AADC:

- Tracking children by default.
- Embedding monitoring technology without the consent or knowledge of the user.
- Sharing children's data with third parties, often for 'unspecified purposes'.
- Nudging and misleading children into lowering their privacy protections.

31 https://poki.com

After eight months of engagement, the changes made include:

- Changing default settings to high privacy.
- Restricting cookies.
- Switching out advertising based on profiling for contextual ads.
- Ending precise location tracking.
- Making the privacy policies more intelligible and accessible.

5Rights also highlight that Poki chose to implement the changes for all UK users, meaning that adults benefit from the changes required for children by the Code. That Poki chose only to implement its changes in the UK market underlines the impact of the AADC being on a statutory basis in the UK.

11. Conclusions and recommendations

These conclusions are structured around the research questions posed at the start of the report. They inform recommendations for companies, governments, researchers and regulators.

The limitations of the research are acknowledged in that it was significantly based on published announcements and additional information supplied by the companies themselves. From our own conversations with the companies and with the regulators, it seems likely that the published announcements are only a certain percentage of the impact that recent regulation has had.

How has recent regulation impacted the design and governance of particular online services likely to be accessed by children, if at all?

The report provides significant evidence that legislation and regulation are driving important and substantive changes, increasing protections for children's privacy and safety, in the design and operation of online services.

The high spike of changes in 2021, across the main four companies, is a significant indicator that the AADC drove significant design changes for child safety.

The impacts are clearest for the AADC and DSA due to their earlier implementation, but there is also clear evidence of safety changes being relevant to the OSA as well.

The number of changes identified, and how they have increased since 2021, indicates that these measures in legislation and regulation may have created a cumulative momentum towards substantive changes being made.

Other legislation, such as the GDPR and COPPA, has also had an impact, particularly through enforcement actions.

The research provides evidence of changes being made during transitional periods, after commencement and also after enforcement actions.

Which aspects of service design and governance change? Are there specific trends by sector, service or product type? What can be seen as a concrete indicator of change?

The research provides the most significant evidence for Meta, Google, TikTok and Snap, but also valid evidence from other social media platforms and in the gaming industry.

The most significant changes are those that have been made by design and default. These changes have significant potential benefits to children in providing a safe environment where children can explore and enjoy their online experience. Substantive changes included social media accounts defaulted to private settings, changes to recommender systems and restrictions on targeted advertising to children.

There is evidence to suggest that parental controls are being over promoted as a solution to address risks about children's privacy and safety. There are concerns about their effectiveness and impacts on children's autonomy.

Tools, information and support measures are being introduced, and their benefit is likely to be as part of a range of measures rather than in isolation. While these changes alone are not pivotal in their impact, they can be seen as positive outcomes from regulation if they are part of a holistic design and governance programme, guided to mitigate evidenced risks. There should also be scrutiny of their effectiveness, alongside the prominence platforms give them as a safeguard.

Are the changes weighted towards specific aspects of privacy, safety or legislation and regulation?

There was considerable weighting towards default settings. Given the AADC's earlier adoption, this had a significant impact. We can also see a clear impact of the DSA and OSA's focus on recommender systems. There was a clear response from companies to the DSA requirement to prohibit advertising based on profiling, while the AADC had had an earlier impact in reducing the types of targeting undertaken. There was a strong focus on content risks, linked to the OSA and DSA's focus on this area.

We can see evidence that both legislation (DSA and OSA) and regulation (AADC) are having an impact. Future research may need to consider whether the combination of these measures is an important factor.

In general, the data protection and privacy-focused requirements of AADC can be seen to complement the DSA and OSA's safety requirements, although tensions are most likely on the age assurance requirements of the DSA and OSA.

Which regulatory requirements have resulted in which specific benefits to children?

The changes platforms are making to default settings are the greatest area of visible benefit and have been applied across a range of features and different services. In many respects, privacy equals safety for children – it allows them to have greater autonomy online as well as a safe space to develop and explore.

Regulators should also refine guidance on default settings as evidence emerges about which design changes and practices are most effective to ensure best practice in one company – for example, high privacy or no direct messaging becomes a norm across sectors. The AADC, which is the most established, has had the greatest impact, and has had, retrospectively, most support from industry.

The DSA has already had a clearly defined impact in two key areas: (1) prohibition of targeted advertising to children and (2) the requirement to provide feeds that don't use algorithms to suggest content. This should provide benefits to some children's online experience in terms of less profiling and choice over recommender systems, but it is difficult to know the extent of this.

What is the impact of regulatory changes on children's rights, viewed holistically? Taking account of other rights children have, have the changes had wider consequences?

In general, the evidence indicates significant impacts of enhanced protections for children's privacy and safety online. Risks to their wider rights are still emerging and will need to be assessed in future research. Therefore, at present, the impacts appear net positive, and are in line with the kinds of recommendations young people ask for (5Rights, 2022).

Legislation and regulation are also driving changes to age assurance, but these changes are evolving slowly, given the wider concerns about impacts on other rights, such as privacy, freedom of expression and non-discrimination. The industry's desire to keep children on their services is also leading to questions about proportionality and effectiveness.

It is important that companies consider whether they provide an age-appropriate service without the need for age assurance. It is also important to recognise that age assurance is not a single solution to children's online safety.

What can be learned from companies' responses to regulatory changes? How could this inform new regulation or changes to regulation in future?

We have observed a significant number of changes. Previously the question was whether companies were making enough changes. Over time, the regulatory questions will focus on whether the solutions are effective. Therefore, regulators will need to be equipped to handle both these questions. Recommender systems will be a key area where the focus on effectiveness will be needed – in this report we have observed that companies are starting to make potentially important changes but whether they are reducing repeated exposure to harmful content is unclear.

Future regulation can learn from the implementations of 'by default' changes, and companies have provided evidence that they can be integrated into their design process. Regulators will need request detailed information from the companies about their implementation and how their effectiveness is assessed.

When requirements in legislation have been explicit, for example advertising prohibitions, companies have responded in clear terms. While prohibitions may not be suitable for some parts of the legislative framework, and this is a risk-based approach, it illustrates that it can be an effective measure when required.

There is a risk that companies are deprioritising or staging implementation when they see a lack of clarity in regulatory guidance (e.g., age assurance). They may also seek to promote their own preferred solutions (e.g., parental controls). For the DSA and OSA this highlights the importance of clarification via additional codes and guidance from regulators, which is adjusted in response to consultation and evidence on how regulation is working in practice. Regulators need to ensure that codes meet the ambition of legislation rather than muddy or water it down.

The importance of strategic regulatory supervision and enforcement is also highlighted – creating momentum for change during this transitional and early period through regulatory engagement and guidance while enforcing against the systemic breaches that create significant risk and harm.

How transparent are companies about changes they make, and how do they explain or promote them?

Gathering consistent evidence for the research has been a considerable challenge, and steps should be taken to address the gap in transparency. This is a risk for accountability of the systems of regulation. Companies rarely acknowledge the role of legislation or regulation in announcing the changes they make. It is likely, therefore, that the impact of

legislation is significantly greater than this report has been able to illustrate.

It has proved challenging to gather information to conduct this study, as only 8 out of 50 online services we wrote to replied. Responses received varied in detail. The research study therefore had to rely on extensive research via company websites and other information gathered from 5Rights advocacy work. It is difficult to identify the changes companies are making related to child safety, why they are making them, and tracking them over time. We also encountered some practical challenges, such as company announcements or policy updates lacking a date. Independent access to company data, which is anticipated by the DSA, will bring vast benefit to researchers.

Can the project results inform child rights advocacy, and focus future research questions?

This research highlights the value of building a regime that creates responsibilities to design protections for privacy and safety by default, and to evolve these requirements over time in response to evidence. The importance of formal transparency requirements and researcher access should also be a core part of the regime.

This report does not suggest that the changes introduced by companies are enough to protect children online and uphold their rights. It indicates that a direction towards change is now apparent. The challenge is ongoing, and regulators such as Ofcom are just starting their work.

Therefore, we see considerable value in repeating the study, probably in late 2025, when there will be significant amounts of additional information from transparency measures under the DSA and OSA. There should also be further impacts from further codes and guidance under both pieces of legislation and from enforcement action.

Our study was also limited in the sectors it could cover due to resource constraints and lack of information available. Future studies should seek to cover a broader range of companies and sectors, including gaming and generative AI tools.

Further research is needed to assess these initial conclusions, particularly to assess how the child's experience online is really impacted by design changes. The child's voice in the evidence will be crucial. For example, a study could assess how children interact with default privacy settings for their social media accounts, and how their experiences were shaped by more protective or open settings.

Legislation and regulation related to child privacy and safety will be continually tested by new technologies over the coming years. Children's experience online (and offline) will be increasingly shaped by AI. Services are starting to introduce changes – Google, for exam-

ple, has announced safeguards for children using Bard. Future research will also need to place greater emphasis on this dimension of children's experience online.

As these regimes have been rolled out in the Global North, it is important that future research also focuses on the Global South, to inform what regulatory measures may work most effectively in that context. Such a research project could explore the following: the extent to which design changes for child users in the Global South are driven by legislation and regulation in the Global North, how privacy and safety risks differ for children in the Global South, and evidence of regulatory interventions in the Global South.

Recommendations

How companies approach compliance and best practice

While companies are clearly taking steps to address the requirements of legislation and regulation, the process of compliance is ongoing, and more evidence is needed about the effectiveness of the solutions they deploy, and how they balance tensions between rights.

Recommendation 1. Companies subject to the DSA, OSA and AADC should ensure that solutions address the full range of risks, as detailed in the OECD typology of risks, including support measures related to conduct and contact risks.

Recommendation 2. Companies should work across industry to introduce best practice rather than each working separately, to ensure that different solutions don't leave unnecessary gaps in safety provision.

Transparency

The EU is currently providing the leading examples of transparency. The DSA requires providers of hosting services to inform their users of the content moderation decisions they take and to explain the reasons behind those decisions in so-called statements of reasons. These statements must be submitted to the DSA Transparency Database, hosted by the European Commission (2024c). The Digital Services Terms and Conditions Database (European Commission, 2024b) also provides a further example of a standardised approach, this time for terms and conditions in machine-readable formats. Both databases can also allow APIs to utilise re-use of the information.

The companies' failure to publicly record the impact of design strategies or default settings that benefit children has created a perverse world in which companies, and governments, cite lack of evidence as a reason to take no action. Formal statutory requirements for record keeping, research access and transparency must be central to regulatory regimes. There is also uncertainty about the geographical scope and application of the changes made; companies will sometimes reference jurisdiction and other times there is not mention, leaving the reader unsure whether the changes are global or not.

Recommendation 3. The UK Government should update the OSA to introduce mandatory access to data for child safety research, learning from the DSA's approach and implementation by the European Commission.

Recommendation 4. The European Commission and Ofcom should explore how data related to child safety changes could be recorded and logged transparently in a 'child online safety tracking database'.

Recommendation 5. The UK Government, Ofcom, Information Commissioner's Office (ICO) and European Commission should consult on how to assess the outcomes of their child safety regimes, including consideration of children's wider rights under the United Nations Convention on the Rights of the Child.

Recommendation 6. The ICO, Ofcom and European Commission should provide guidance as to how platforms should record and document changes to the design and governance of their platforms related to child privacy and safety.

Recommendation 7. Companies should provide a single web portal that allows researchers and other stakeholders to see a record of child privacy and safety changes implemented, by date. The changes should also be made available as API and in machine-readable format. This should initially be developed as regulatory guidance and made into a statutory requirement if evidence indicates formal provision is needed.

Recommendation 8. Companies should provide explicit confirmation of which jurisdiction or region each change applies to, and update this information as it changes.

Approach of regulators

In this report we have noted examples of interventions and enforcement actions from the data protection regulators and emerging action from the European Commission under the DSA.

These actions play an important role in clarifying grey areas, and the actions provide clear lines and dissuasive messages for those who ignore the requirements of the law.

The Spanish Data Protection Agency published its *Global strategy on children, digital health and privacy* in January 2024 (AEPD, 2024a), and this is serves as a useful example to other Data Protection Authorities in setting priorities for proactive engagement and enforcement.

Regulators' actions may not always involve formal use of fining or enforcement order powers. Online services will often make changes following supervision and intervention. It is therefore important that regulators consider how they record and publish information about child safety changes they observe following their action. But regulators must take decisive action to address systemic non-compliance. There is a risk that lack of implementation by companies is directly linked to lack of action by regulators. Regulators should be given adequate resources, and the expectations of legislators should be incorporated into regulatory systems.

Recommendation 9. All EU Data Protection Authorities and the ICO should ensure that they assess the risks related to children's online privacy when developing their regulatory strategies, including measures to assess the outcomes achieved. All Data Protection Authorities should also include a section on children in their annual reports, including outcomes of investigations that did not result in formal action.

Recommendation 10. Data protection and online safety regulators should publish their expectations of good practice, requiring companies to meet or better them, and seek to spread practice across sectors.

Recommendation 11. Data protection and online safety regulators should work via international cooperation mechanisms, such as the Global Online Safety Regulators Network1 and Global Privacy Assembly, 2 to agree best practice across jurisdictions with the aim of creating global norms.

1 Global Online Safety Regulators Network: www.ofcom.org.uk/about-ofcom/international/online-safety/gosrn
2 Global Privacy Assembly: https://globalprivacyassembly.org

12. References

5Rights Foundation (2021). *But how do they know it is a child? Age assurance in the digital world*. October. https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf

5Rights Foundation (2022). *Making child online safety a reality: Child online safety toolkit*. https://childonlinesafetytoolkit.org/wp-content/uploads/2022/05/5Rights-Child-Online-Safety-Toolkit-English.pdf

5Rights Foundation (2024). Poki: A case study in service redesign for children. 24 March. https://5rightsfoundation.com/uploads/pr-poki-a-case-study-in-service-redesign-for-children-5rights-21-03-2024.pdf

AEPD (La Agencia Española de Protección de Datos) [Spanish Data Protection Agency] (2024a). *Estrategia global sobre menores, salud digital y privacidad* [*Global strategy on children, digital health and privacy*]. January 29. www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-agencia-presenta-su-estrategia-global-sobre-menores-salud-digital-y-privacidad [in Spanish].

AEPD (2024b). The Agency orders a precautionary measure which prevents Worldcoin from continuing to process personal data in Spain. Press releases, March. www.aepd.es/en/press-and-communication/press-releases/agency-orders-precautionary-measure-which-prevents-Worldcoin-from-continuing-toprocess-personal-data-in-spain

Attorney-General's Department (2023). Privacy Act Review. Report 2022. Australian Government. www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf

Beckerman, M (2021). Testimony of Michael Beckerman, Vice President and Head of Public Policy, Americas, TikTok – Hearing on Protecting Kids Online: Snap, TikTok, and YouTube – to the United States Senate Subcommittee on Consumer Protection, Product Safety and Data Security. 26 October. www.commerce.senate.gov/services/files/8C751FF4-A1FD-4FCA-80F6-C84BEB04C2F9

California Age-Appropriate Design Code Act 2022 (USA). https://legiscan.com/CA/text/AB2273/id/2606836

CCDH (Center for Countering Digital Hate) (2022). *Deadly by design: TikTok pushes harmful content promoting eating disorders and self-harm into young users' feeds*. https://counterhate.com/research/deadly-by-design

Children's Online Privacy Protection Act 1998 (USA). S.2326. www.congress.gov/bill/105th-congress/senate-bill/2326

Council of Europe (2018). Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment. July. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016808b79f7

Data Protection Act 2018 (UK). C12. www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Data Protection Commission (Ireland) (2021). *The fundamentals for a child-oriented approach to data processing*. Guidance. www.dataprotection.ie/en/dpc-guidance/fundamentals-child-oriented-approach-data-processing

Data Protection Commission (Ireland) (2023). Irish Data Protection Commission announces €345 million fine of TikTok. Press release, 15 September. www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok

Davidson, B.I., Hinds, J., & Racek, D. (2023). Shifting landscapes of social media data for research. *Times Higher Education*, 4 August. www.timeshighereducation.com/campus/shifting-landscapes-social-media-data-research

DCMS (Department for Digital, Culture, Media & Sport) (2020). *Online harms White Paper: Full government response to the consultation*. www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response

Digital Personal Data Protection Act 2023 (India). No. 22 of 2023. Section 9 – Processing of personal data of children. www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

Draft Online Safety Bill Joint Committee (2021). Written evidence submitted by Google. https://committees.parliament.uk/writtenevidence/39457/html/

European Commission (2024a). Commission opens formal proceedings against TikTok under the Digital Services Act. Press release, 19 February. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_926

European Commission (2024b). Digital Services Terms and Conditions Database. https://platform-contracts.digital-strategy.ec.europa.eu

European Commission (2024c). Digital Services Act Transparency Database. https://transparency.dsa.ec.europa.eu

European Commission (2024d). *Status report: Mechanisms for researcher access to online platform data*. 4 April. https://digital-strategy.ec.europa.eu/en/library/status-report-mechanisms-researcher-access-online-platform-data

European Commission (2024e). *Research report: Mapping age assurance typologies and requirements*. 19 April. https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements

European Commission (2024f). Commission opens proceedings against TikTok under the DSA regarding the launch of TikTok Lite in France and Spain, and communicates its intention to suspend the reward programme in the EU. Press release, 22 April. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2227

European Parliament and Council of the European Union (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

European Parliament and Council of the European Union (2018). Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L1808

European Parliament and the Council of Europe (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2022%3A277%3ATOC&uri=uriserv%3AOJ.L_.2022.277.01.0001.01.ENG

FTC (Federal Trade Commission) (2022). Fortnite video game maker Epic Games to pay more than half a billion dollars over FTC allegations of privacy violations and unwanted charges. Press release, 19 December. www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations

FTC (2023a). 16 CFR Part 312: Children's Online Privacy Protection Rule (NPRM). 20 December. www.ftc.gov/legal-library/browse/federal-register-notices/16-cfr-part-312-childrens-online-privacy-protection-rule-nprm

FTC (2023b). FTC will require Microsoft to pay $20 million over charges it illegally collected personal information from children without their parents' consent. Press release, 5 June. www.ftc.gov/news-events/news/press-releases/2023/06/ftc-will-require-microsoft-pay-20-million-over-charges-it-illegally-collected-personal-information

Ghai, S., Weinberg, L., Stoilova, M., Livingstone, S., & Orben, A. (2022). Social media and adolescent well-being in the Global South. *Current Opinion in Psychology*, 46(4), 101318. www.researchgate.net/publication/359155442_Social_Media_and_Adolescent_Well-being_in_the_Global_South

GPDP (Garante per la protezione dei dati personali) [Italian Data Protection Authority] (2023a). Intelligenza artificiale, dal Garante privacy stop al chatbot "Replika". Troppi i rischi per i minori e le persone emotivamente fragili. [Artificial intelligence: Italian SA clamps down on 'Replika' chatbot.] 3 February. www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9852506 [in Italian].

GPDP (2023b). Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'età dei minori. [Artificial intelligence: The guarantor blocks ChatGPT. Unlawful collection of personal data. Absence of systems for verifying the age of minors.] 3 February. www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870847

Haidt, J. (2024). *The anxious generation: How the great rewiring of childhood is causing an epidemic of mental illness*. Penguin Books.

HM Government (UK) (2017). *Internet safety strategy – Green paper*. October. https://assets.publishing.service.gov.uk/media/5a8222f2e5274a2e8ab57aed/Internet_Safety_Strategy_green_paper.pdf

House of Commons (UK) (2020). Digital, Culture, Media and Sport Sub-committee on Online Harms and Disinformation. Oral evidence: Online harms and the ethics of data, HC 646. https://committees.parliament.uk/oralevidence/906/html/

ICO (Information Commissioner's Office) (no date, a). *Children's code: Best interests framework*. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/how-to-use-our-guidance-for-standard-one-best-interests-of-the-child/best-interests-framework/#:~:text=The%20concept%20of%20the%20best,they%20hold%20under%20the%20UNCRC

ICO (no date, b). *Children's code guidance and resources*. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources

ICO (2019). *Responses to the consultation on age appropriate design: A code of practice for online services*. https://ico.org.uk/about-the-ico/responses-to-the-consultation-on-age-appropriate-design

ICO (2021). *Age appropriate design: A code of practice for online services*. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services

ICO (2023a). ICO fines TikTok £12.7 million for misusing children's data. News and blogs, 4 April. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/ico-fines-tiktok-127-million-for-misusing-children-s-data

ICO (2023). UK Information Commissioner issues preliminary enforcement notice against Snap. 6 October. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/10/uk-information-commissioner-issues-preliminary-enforcement-notice-against-snap

ICO (2024a). *Age assurance for the Children's code*. January. https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code

ICO (2024b). *Protecting children's privacy online: Our Children's code strategy*. April. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/protecting-childrens-privacy-online-our-childrens-code-strategy

Livingstone, S. (2021). *Realising children's rights in a digital world*. Impact Case Study. London School of Economics and Political Science. www.lse.ac.uk/Research/research-impact-case-studies/2021/realising-childrens-rights-in-a-digital-world

Livingstone, S., Davidson, J., Bryce, J., with Batool, S. (2017). *Children's online activities, risks and safety: A literature review by the UKCCIS Evidence Group*. UK Council for Child Internet Safety, October. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759005/Literature_Review_Final_October_2017.pdf

Livingstone, S., Cantwell, N., Özkul, D., Shekhawat, G., & Kidron, B. (2024) *The best interests of the child in the digital environment*. March. Digital Futures for Children. https://5rightsfoundation.com/uploads/dfc-report-best-interests-of-the-child.pdf

Maryland General Assembly (USA) (2024). Consumer Protection – Online Products and Services – Data of Children (Maryland Kids Code). https://mgaleg.maryland.gov/2024RS/bills/sb/sb0571T.pdf

Meta (2024). Our tools, features and resources to help support teens and parents. www.meta.com/en-gb/help/policies/safety/tools-support-teens-parents

Miller, J., Mills, K.L, Vuorre, M., Orben, A., & Przybylski, A.K. (2022). Impact of digital screen media activity on functional brain organization in late childhood: Evidence from the ABCD study, *Cortex*, 169 290-308. https://doi.org/10.1016/j.cortex.2023.09.009

Ministry of Human Rights and Citizenship (Brazil) (2024) Resolution no. 245, of April 5, 2024. Provides for the rights of children and adolescents in the digital environment. https://in.gov.br/en/web/dou/-/resolucao-n-245-de-5-de-abril-de-2024-552695799 [in Portuguese].

Ministry of ICT & Innovation (Republic of Rwanda) (2019). *Child online protection policy*. June. https://rura.rw/fileadmin/Documents/ICT/Laws/Rwanda_Child_Online_Protection_Policy.pdf

Mootz, J., & Blocker, K. (2024). *UK Age-Appropriate Design Code: Impact assessment*. Children and Screens, Institute of Digital Media and Child Development. www.childrenandscreens.org/wp-content/uploads/2024/03/Children-and-Screens-UK-AADC-Impact-Assessment.pdf

Netchoice, LLC v. Rob Bonta, Attorney General of California (2022). Complaint for declaratory and injunctive relief. https://netchoice.org/wp-content/uploads/2022/12/NetChoice-v-Bonta_-Official-AB-2273-Complaint-final.pdf

Ng, A. (2019). Default settings for privacy – we need to talk. CNET, 21 December. www.cnet.com/tech/tech-industry/default-settings-for-privacy-we-need-to-talk

Ng, G (2024). Navigating the Digital Services Act: A guide for game developers. Forbes, 25 January. www.forbes.com/sites/forbestechcouncil/2024/01/25/navigating-the-digital-services-act-a-guide-for-game-developers/?sh=38d9824619d2

Nix, N. (2024). Meta says its parental controls protect kids. But hardly anyone uses them. *The Washington Post*, 30 January. www.washingtonpost.com/technology/2024/01/30/parental-controls-tiktok-instagram-use

OECD (Organisation for Economic Co-operation and Development) (2021a). Recommendation of the Council on children in the digital environment. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389

OECD (2021b). *Children in the digital environment: Revised typology of risks*. OECD Digital Economy Papers, No. 302. https://doi.org/10.1787/9b8f222e-en

Ofcom (2023a). *Children and parents: Media use and attitudes report 2023*. 29 March. www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2023

Ofcom (2023b). *Ofcom's approach to implementing the Online Safety Act*. 26 October. www.ofcom.org.uk/__data/assets/pdf_file/0017/270215/10-23-approach-os-implementation.pdf

Ofcom (2024a). *Understanding pathways to online violent content among children*. Qualitative Research Report, 15 March. www.ofcom.org.uk/__data/assets/pdf_file/0026/280655/Understanding-Pathways-to-Online-Violent-Content-Among-Children.pdf

Ofcom (2024b). *Survey: Online platform terms & conditions (T&Cs) and content controls*. 28 February. www.ofcom.org.uk/__data/assets/pdf_file/0028/279091/content-controls-technical-report.pdf

Ofcom (2024c). Consultation: Protecting children from harms online. 8 May. www.ofcom.org.uk/consultations-and-statements/category-1/protecting-children-from-harms-online

Online Safety Act 2021 (Australia). Act no. 77. www.legislation.gov.au/C2021A00076/latest/text

Online Safety Act 2023 (UK). Chapter 50. www.legislation.gov.uk/ukpga/2023/50/enacted

Parliament of Canada (2024). Online Harms Bill C-63. www.parl.ca/DocumentViewer/en/44-1/bill/C-63/first-reading

Raffoul, A., Ward, Z., Santoso, M., Kavanaugh, J., & Austin, S. (2023). Social media platforms generate billions of dollars in revenue from US youth: Findings from a simulated revenue model. *PLoS ONE*, 18(12), e0295337. https://doi.org/10.1371/journal.pone.0295337

Republic of Rwanda (2024). Ministerial Instructions n° 001/minict/2024 of 22/03/2012 on child online protection. www.minijust.gov.rw/index.php?eID=dumpFile&t=f&f=91546&token=d5eb7096a06042554606ab1c4fac9b87b9de3c2e

Reset Australia (2021). Surveilling young people online: An investigation into TikTok's data processing practices. 1 August. http://au.reset.tech/news/surveilling-young-people-online-an-investigation-into-tiktok-s-data-processing-practices

Revealing Reality – commissioned by 5Rights (2021). *Pathways: How digital design puts children at risk*. 5Rights. https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf

Revealing Reality (2023). *Avatar methodology: Pilot study. A report for Ofcom*. www.ofcom.org.uk/__data/assets/pdf_file/0025/263167/Avatar-Methodology-A-pilot-study.pdf

Rossi, R., & Nairn, A. (2024). Clearly (not) identifiable – The recognisability of gambling content marketing. 16 March (Preprint). https://doi.org/10.31219/osf.io/8ybgv

Stoilova, M., Bulger, M., & Livingstone, S. (2024). Do parental control tools fulfil family expectations for child protection? A rapid evidence review of the contexts and outcomes of use, *Journal of Children and Media*, 18(1), 29-49, doi: 10.1080/17482798.2023.226551.

Stout, J (2021). Testimony of Jennifer Stout, Vice President of Global Public Policy, Snap Inc. Hearing before the United States Senate Committee on Science, Commerce, and Transportation, Subcommittee on Consumer Protection, Product Safety, and Data Security. 26 October. www.commerce.senate.gov/services/files/0AACA9BA-49C8-4AC3-8C2E-E62ACC3F73BC

Sutcliffe, C. (2023). Meta's latest campaign highlights child safety features – will it satisfy critics? The Drum, 10 May. www.thedrum.com/news/2023/05/10/meta-s-latest-campaign-highlights-child-safety-features-will-it-satisfy-critics

Tech Transparency Project (2023). Big Tech's scramble to stop child safety laws. 3 May. www.techtransparencyproject.org/articles/big-techs-scramble-to-stop-child-safety-laws

UN (United Nations) (2021). General comment No. 25 (2021) on children's rights in relation to the digital environment. www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

US Congress (2022). Children and Teens' Online Privacy Protection Act. S.1628. www.congress.gov/bill/117th-congress/senate-bill/1628

US Senate (2023) Kids Online Safety Act. S.1409. www.congress.gov/bill/118th-congress/senate-bill/1409/text

US Senate (2024). The American Privacy Rights Act of 2024. www.commerce.senate.gov/services/files/3F5EEA76-5B18-4B40-ABD9-F2F681AA965F

US Senate Committee on Commerce, Science, & Transportation (2021). Subcommittee: Protecting Kids Online: Snap, TikTok, and YouTube. www.commerce.senate.gov/2021/10/protecting-kids-online-snapchat-tiktok-and-youtube

US Senate Committee on the Judiciary (2024). Big Tech and the online child sexual exploitation crisis. Responses to questions for the record. 31 January. www.judiciary.senate.gov/committee-activity/hearings/big-tech-and-the-online-child-sexual-exploitation-crisis

Utah State (2023). Protecting Minors Online. https://socialmedia.utah.gov

13. Annex A List of changes announced by Meta, Google, TikTok and Snap

This includes a hyperlink for each announcement, ordered by year (most recent first), 2024-17

CHANGE DETAIL	YEAR	OECD 5 'Cs'	TYPE
META			
Instagram and Facebook – stricter private messaging	2024	Contact	By default
Instagram and Facebook – detect images in messages	2024	Content	By default
Instagram – night-time nudges	2024	Cross-cutting	Information
Instagram and Facebook – automatically placing teens into the most restrictive content control setting	2024	Content	By default
Instagram and Facebook – hiding more results in Instagram search related to suicide, self-harm and eating disorders	2024	Content	By default
Instagram and Facebook – changed teen content policy for recommendations e.g., self harm	2024	Content	By default
Instagram and Facebook – prompting teens to easily update their privacy settings	2024	Cross-cutting	Information
Facebook – parental supervision tools on Messenger	2023	Contact	Tools
Instagram – testing new messaging privacy features	2023	Contact	By default
Instagram – additional tools to parental supervision	2023	Contact	Tools
Instagram and Facebook – Take a Break	2023	Conduct	Information
Metaquest – parents and guardians manage what their teens can access and view in the Meta Quest Browser	2023	Content	Tools
Horizon Worlds – giving teens customised controls with age-appropriate settings	2023	Cross-cutting	Tools
Horizon Worlds – giving parents supervision tools	2023	Cross-cutting	Tools
Facebook and Instagram – Take It Down launched to prevent the spread of young people's intimate images online	2023	Content	Support

Instagram and Facebook – Take It Down – intimate images expanded to more languages	2023	Content	Support
Instagram – new Quiet Mode to help people focus and prompt teens to turn it on	2023	Conduct	Tools
Instagram – New ways to manage recommendations	2023	Content	Tools
Facebook and Instagram – removing gender as an option and app engagement won't inform ads, further ad controls	2023	Consumer	By default
Facebook dating – age verification	2022	Cross-cutting	By default
Facebook and Instagram – users under 16/18 will be defaulted into more private settings (encourage teens already on the app)	2022	Cross-cutting	By default
Facebook and Instagram – prompting teens to report accounts to us after they block someone	2022	Contact	Support
Instagram – when you block someone, you'll have the option to block other accounts they may already have	2022	Contact	Tools
Quest – new tools that allow parents to enable and disable social features for teens they're supervising	2022	Cross-cutting	Tools
Instagram – sensitive content control has only two options for teens: 'standard' and 'less'. New teens under 16 will be defaulted into the 'less' state. For teens already on Instagram send a prompt encouraging them to select the 'less' experience	2022	Content	By default
Instagram – new options for people to verify their age on Instagram	2022	Cross-cutting	By default
Instagram – sensitive content control will cover all surfaces where recommendations are made	2022	Content	By default
Instagram – option to see their feeds in chronological order	2022	Content	Tools
Instagram and VR – family centre, a new place for parents and guardians to access supervision tools and resources	2022	Cross-cutting	Information
Horizon – introduced personal boundary for Horizon Worlds and Horizon Venues	2022	Contact	By default
Instagram – show certain content (e.g., regulated products, nudity, sexual) lower in Feed and Stories	2022	Content	By default
Instagram – restricting people from tagging or mentioning teens who don't follow teens	2021	Conduct	By default
Instagram – remove 'allow' option for under-18s in sensitive content control	2021	Content	By default
Instagram – Take a Break feature	2021	Conduct	Information
Instagram – nudging teens towards different topics if they've been dwelling on one topic for a while	2021	Content	Information

Instagram – asking people for their birthday on Instagram	2021	Cross-cutting	By default
Instagram – hidden Words and limit comments	2021	Content	By default
Instagram – sensitive control – teens defaulted to 'less'	2021	Content	By default
Instagram – default teens into private accounts when they join Instagram	2021	Cross-cutting	By default
Instagram – stopping suspicious behaviour from interacting with teen accounts	2021	Contact	By default
Instagram – only allow advertisers to target ads to those under 18 based on their age, gender and location	2021	Consumer	By default
Instagram – restrict people over 19 from sending private messages to teens who don't follow them	2021	Contact	By default
Instagram – safety notices in DMs for suspicious behaviour	2021	Contact	Information
Instagram – expert-backed resources when someone searches for eating disorders or body image-related content	2021	Cross-cutting	Information
Instagram – dedicated reporting option for eating disorder posts	2021	Content	Support
Instagram and Facebook – reporting using Google's content safety API	2021	Content	Support
Instagram and Facebook – pop-up that is shown to people who search for terms on apps associated with child exploitation	2021	Content	Information
Instagram – added a message at the top of all search results for searches related to suicide or self-injury	2020	Content	Information
Instagram – choosing who can tag and mention you	2020	Contact	Tools
Messenger Kids – giving parents even more control	2020	Cross-cutting	Tools
Instagram – caption warnings for content that may be considered offensive	2019	Content	Information
Instagram – asking for date of birth when creating an account on Instagram	2019	Cross-cutting	By default
Instagram – restrict – comments on posts from that person will only be visible to that person	2019	Content	By default
Instagram – not allow any graphic images of self-harm, such as cutting	2019	Content	By default
Instagram – new anti-bullying tools	2018	Cross-cutting	Tools
Messenger Kids – introduction of kindness stickers	2018	Cross-cutting	Information
Instagram – comments filter – bullying filter	2018	Cross-cutting	Tools
Messenger Kids – sleep mode – giving parents more control	2018	Cross-cutting	Tools

Instagram – choose who can comment on your posts	2017	Content	Tools
Instagram – anonymous reporting for live video	2017	Content	Support
Instagram – filter to block certain offensive comments	2017	Content	Tools

GOOGLE

YouTube additional safeguards for content recommendations for teens	2023	Content	By default
YouTube – Updated Take a Break and Bedtime reminders	2023	Cross-cutting	Information
Bard safety features for teens	2023	Cross-cutting	By default
Expand content safety API to video	2023	Content	By default
YouTube – Introducing age restrictions on certain content about eating disorders	2023	Content	By default
Google Assistant – new parental controls	2022	Cross-cutting	Tools
Removal tool for images from search for under-18s and parents	2021	Content	Tools
Default upload setting to the most private option available for users ages 13–17 on YouTube	2021	Content	By default
YouTube – Take a Break and Bedtime reminders on by default	2021	Cross-cutting	By default
Removal of overly commercial content from YouTube Kids	2021	Consumer	By default
Turn SafeSearch on for existing users under 18 and make this the default setting for teens setting up new accounts	2021	Content	By default
Location history will remain off for under-18s (without the option to turn it on)	2021	Cross-cutting	By default
YouTube Autoplay off by default	2021	Content	By default
Play – new safety section	2021	Consumer	Information
Ad targeting and age-sensitive ad changes	2021	Consumer	By default
Parents can allow their children to access YouTube through a supervised Google Account	2021	Cross-cutting	Tools
YouTube – age verification added	2020	Cross-cutting	By default
YouTube – all creators will be required to designate their content as made for kids or not made for kids in YouTube Studio	2020	Content	By default
YouTube – changes to use of data for children's content on YouTube	2019	Cross-cutting	By default
YouTube – potentially inappropriate comments now automatically held for creators to review	2019	Content	By default

YouTube – updated enforcement of our live streaming policy to specifically disallow younger minors from live streaming unless they are clearly accompanied by an adult	2019	Content	By default
YouTube – disabling comments on videos featuring minors	2019	Content	By default
Expanded Safety Center	2018	Cross-cutting	Tools
Family Link expanded to teens	2018	Cross-cutting	Tools
YouTube Kids – parent-approved content	2018	Content	Tools

TIKTOK

Allow users to turn off personalisation	2023	Content	Tools
EU users 13–17 no longer see personalised ads based on their activities on or off TikTok	2023	Consumer	By default
New feature that enables people to refresh their 'for you' feed if their recommendations no longer feel relevant	2023	Content	Tools
Under-18 users will automatically be set to a 60-minute daily screen time limit	2023	Cross-cutting	By default
New features to Family Pairing – mute notifications for teens	2023	Cross-cutting	Tools
New systems to help prevent content with overtly mature themes from reaching younger audiences under the age of 18	2022	Content	By default
Updates to Community Guidelines – dangerous acts and challenges, eating disorders, hateful ideologies	2022	Content	By default
Self-harm hoaxes – changes to warning labels and detection	2021	Content	Information
Expanding search interventions (e.g., suicide) and strengthening notices on search results	2021	Content	Information
For those 16–17 joining TikTok, their direct messaging setting will now be set to 'No One' by default	2021	Contact	By default
Video publishing choice for under-16s	2021	Content	Tools
Choose who downloads video	2021	Content	Tools
Changed content moderation policy and violation approach	2021	Content	By default
Ability to delete multiple comments at once or report them for potentially violating Community Guidelines	2021	Content	Support
New filter all comments feature	2021	Content	Tools
Default privacy setting for all registered accounts ages 13–15 to private	2021	Cross-cutting	By default
Tightening the options for commenting on videos created by those aged 13–15	2021	Content	By default

Changing Duet and Stitch settings for those aged 13–15, default off for 16 and over	2021	Content	By default
Allowing downloads of videos that have been created by users 16 and over only, default off for 16 and over	2021	Content	By default
Setting 'Suggest your account to others' to off by default for users aged 13–15	2021	Contact	By default
Restricting direct messaging and hosting live streams to accounts of those 16 and over	2021	Contact	By default
Restricting the buying, sending and receiving of virtual gifts to users below the age of 18	2021	Consumer	By default
New ad policies that ban ads for fasting apps and weight loss supplements, and increasing restrictions on ads that promote a harmful or negative body image	2020	Consumer	By default
EEA/UK users under 18 age-appropriate summary of TikTok privacy policy, called privacy highlights	2020	Consumer	Information
Launch of TikTok youth portal	2020	Cross-cutting	Information
Family Pairing introduced	2020	Cross-cutting	Tools
Automatically disabling DMs for registered accounts of those under 16	2020	Contact	By default
Updating gifting policies – only allow those aged 18 and over to purchase, send or receive virtual gifts	2019	Consumer	By default
Filter comments – remove comments that contain keywords users perceive as hurtful	2019	Content	Tools
More options for Screen Time Management	2019	Cross-cutting	Tools
Upgraded restricted mode feature	2019	Cross-cutting	Tools

SNAP

Expanding in-app parental tools, Visibility into Their Teens' Settings	2024	Cross-cutting	Tools
In-app warnings for risk contacts	2023	Contact	Information
Require a greater number of friends in common before they can be recommended	2023	Cross-cutting	By default
New strike system for accounts promoting age-inappropriate content	2023	Content	By default
In-app education about common online risks	2023	Cross-cutting	Information
Opt out of a personalised Discover and Spotlight content experience	2023	Content	Tools
Restricting personalised advertising to users aged 13–17 in the EU and UK	2023	Consumer	By default
My AI utilising a user's birthdate and age-appropriate experiences	2023	Cross-cutting	By default

Content controls on Family Centre	2023	Content	Tools
Family Centre launched	2022	Cross-cutting	Tools
New 'safety snapshot', a new safety and privacy-focused channel on the Discover platform	2021	Cross-cutting	Information

14. Annex B Companies contacted for this research project

The letters were sent via email to a known contact in a relevant trust and safety, privacy or public policy team (December–January 2023). If an email address was not available, a request was sent via a general enquiry or press email, or a message was sent to a relevant trust and safety or privacy contact via LinkedIn. Follow-up emails were also sent if no response was received.

Companies that responded

The following companies responded and provided information in response to the letter. However, none of the companies responded with a detailed breakdown of changes by legislation:

Google / TikTok / Pinterest / Yubo / LEGO® / Niantic, Inc. / Tencent / ClassDojo

No response received

The following companies either declined to take part or no response was received:

Meta (Instagram, Facebook and WhatsApp) / X / Snap Inc. / Discord / Tumblr / Wizz / Reddit / Wink / BeReal / Telegram / Viber / JusTalk Kids / Roblox / Microsoft / Supercell / Twitch / EA / Activision Blizzard / Nintendo / Epic / Kitka Games / Sony / Rockstar Games / Steam / Square Enix / NetEase / Take-Two Interactive / Ubisoft / Netflix / Disney / Zoom / BBC / Apple / OpenAI (ChatGPT & DALL-E) / Replika / Midjourney / Amazon / Spotify

Digital Futures For Children

digital-futures-for-children.net
info@dfc-centre.net

@5RightsFound @MediaLSE @Livingstone_S
#DFC #DigitalFutures4Children

LSE THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

5RIGHTS FOUNDATION

The Digital Futures for Children centre acknowledges funding from the 5Rights Foundation.
This joint LSE and 5Rights research centre supports an evidence base for advocacy, facilitates dialogue between academics and policymakers and amplifies children's voices, following the UN Committee on the Rights of the Child's General comment No. 25.

Please cite this report as: Wood, S. (2024). Impact of regulation on children's digital lives. Digital Futures for Children centre, LSE and 5Rights Foundation.