

Witness Name: Richard Lappin, Content Policy Director, for and on behalf of Meta Platforms, Inc.

Statement No.: 1

Exhibits: RL/01 – RL/11

Dated: 24 September 2025

## SOUTHPORT INQUIRY

---

### WITNESS STATEMENT OF RICHARD LAPPIN

---

In relation to the issues raised by the Rule 9 request dated 16 September 2025 in connection with the Southport Inquiry, I, Richard Lappin, will say as follows:

#### Introduction

- 1 I provide this statement for and on behalf of Meta Platforms, Inc. in response to a request under Rule 9 of the Inquiry Rules 2006 dated 16 September 2025 issued by the Southport Inquiry (the “**Inquiry**”).
- 2 I am a Content Policy Director in Meta’s Content Policy EMEA Team. I am employed by Meta Platforms Ireland Limited. In my work I lead a team that develops and implements a set of content policies, the Community Standards, which outline what is and what is not allowed on Facebook and Instagram. Prior to joining Meta, I worked at the Organisation for Security and Co-operation in Europe, United Nations and European Union. I hold a PhD from the University of Leuven and an LLM from the University of Oxford. I joined Meta in 2019.
- 3 I understand that Phase 1 of the Inquiry is aimed at establishing an account of the events leading up to the attack in Southport, including AR’s history and interactions with various

state systems. The Inquiry is also considering AR's use of social media. My statement will focus on the period from January 2021 – September 2025 (the "**Relevant Period**"), and what systems, policies, and processes were in place at Meta during this time.

- 4 I am authorised to make this statement on behalf of Meta. In making this statement, I have drawn on my own knowledge and information provided to me by my colleagues at Meta. My expertise is in the development and implementation of Meta's Community Standards. Where this statement provides details about other topics outside of my direct knowledge or expertise, I have relied on information provided by the relevant individuals and teams within Meta.
- 5 Exhibited with this statement are the key supporting materials, which have been drawn from an array of different sources. To assist the Inquiry, I have explained below the format and location of these sources. For example, up-to-date versions of Meta's policies can be found on its website. These also show what changes have been made to each policy over time. To see how a policy changed over the Relevant Period, I refer the Inquiry to the specific policy website.
- 6 On behalf of Meta, I would like to begin by expressing our deepest sympathies to the families and friends of the victims of the appalling attacks in Southport. The loss and suffering caused by these acts are profound, and our thoughts are with everyone affected by this tragedy. Meta is pleased to be able to assist the Inquiry in its important and valuable work and hopes that our participation in this process can help the Inquiry achieve its objectives.

### **Meta's corporate structure**

- 7 Meta Platforms, Inc. is a multinational technology company, headquartered in Menlo Park, California and incorporated in the state of Delaware, USA. Meta Platforms, Inc. is the current provider of the Facebook and Instagram services in the United Kingdom, and has been since 24 April 2023 (including as at July 2024). In January 2021, the provider of Facebook and Instagram services in the United Kingdom was Meta Platforms Ireland Limited (formerly, Facebook Ireland Limited). For the purposes of this statement,

references to “Meta” are to be interpreted as references to the relevant provider, and not to a specific corporate entity unless explicitly stated.

- 8 Meta’s mission is to build the future of human connection and the technology that makes it possible. Meta builds technology that helps people connect, find communities, and grow businesses. Meta’s services enable people to connect and share with friends and family through mobile devices, personal computers, virtual reality (VR) headsets, wearables, and in-home devices. Meta also helps people discover and learn about what is going on in the world around them, enables people to share their opinions, ideas, photos and videos, and other activities with audiences ranging from their closest family members and friends to the public at large, and stay connected everywhere by accessing Meta’s services.
- 9 Meta provides a number of different services and functionalities. For the purposes of this witness statement, I am going to focus on Facebook and Instagram.
- 10 Meta has a range of teams and structures that contribute to users' safety — including both minors and adults — as well as the integrity of its platforms. Oversight of these safety initiatives is provided by Meta’s senior management. There are no discrete individual teams that consider age restrictions and children's safety, or address violent or otherwise harmful content on Meta. Rather, these issues are considered by cross-functional teams that operate across nearly all of the company functions, including Product and Policy subject matter experts, Integrity Governance Risk & Compliance, Engineering, Product Management, Privacy, Operations, Business, Policy, and Legal.

**Meta’s policy on age verification**

- 11 Facebook and Instagram are available to users in the UK aged 13 years and older, subject to the limited exceptions set out in each service’s terms of service (such as where users are prohibited by law from using these services). This has been the approach throughout the Relevant Period.
- 12 Meta has in place mechanisms to prevent, identify and remove users that are potentially under 13 years old. For example, users can report other users they suspect may be under 13, and Meta operates cross platform disablement where a user’s account is disabled for being underage on one Meta platform and Meta identifies that the user has linked accounts on others. Additionally, Meta deploys AI to deliver age-appropriate experiences for its

users. For example, Meta has developed AI classifiers to help detect whether someone is a teen or an adult. Correctly categorising teens is important to help enable Meta to put the appropriate safeguards in place. Correctly categorising adults is important not only because it allows them to access services and features that are appropriate for them, but also because it helps mitigate risks and child safety issues that could arise on platforms where adults and teens are both present [RL/01 - I META000017]

### **Meta's policies on child safety**

- 13 Meta is committed to keeping users, especially teen users, safe on its services. In addition to adhering to applicable relevant legal and regulatory requirements, Meta has established policies that outline what is and is not allowed on Facebook and Instagram. These were the Community Standards (for Facebook) and the Community Guidelines (for Instagram). On 12 November 2024, the Community Standards and Community Guidelines were combined and, since then, are referred to collectively as the Community Standards, and so I refer to them as Community Standards in this statement. These have been in place across the Relevant Period albeit the specific details of particular policies continue to evolve. For example, in September 2024 we introduced Teen Accounts, as set out at paragraph 19 below. The Community Standards apply to all users, globally, and are integral to protecting expression and enhancing personal safety on Meta's services.
- 14 The development of the Community Standards involves an extensive process, often including multi-stakeholder consultations (including active engagement with NGOs, advisory councils, individual experts, and academia) and analysis of internal signals, such as user research, large community surveys, and detailed analysis of what the community is reporting via platform reporting mechanisms.
- 15 The Community Standards incorporate feedback from people and the advice of experts in fields such as technology, gender, public safety and human rights. They also reflect Meta's commitment to freedom of expression while recognising that, at times, this may need to be limited in line with one or more of the following values: authenticity, safety, privacy and dignity. Throughout the Relevant Period, Meta has used a strategy called "remove, reduce and inform" to manage problematic content: this involves removing content that violates Meta's policies, reducing the spread of potentially harmful content that does not violate

Meta's policies and informing people with additional information so they can choose what to click, read or share.

- 16 In relation to child safety specifically, the Community Standards address specific topic areas and explain what content is and is not allowed on Facebook and Instagram. It also explains what content requires additional information or context for Meta to be able to decide whether to take enforcement action, what content is allowed with a warning screen and what content is allowed but can only be viewed by adults aged 18 and over. The full list of policy topics, as well as links to specific policies and how they have developed over time, are available on Meta's website. Certain topics obviously concern children (for example, Child Sexual Exploitation, Abuse and Nudity), while others may indirectly relate more to teen users (for example, Bullying and Harassment or Suicide and Self-Injury).
- 17 To protect young people online, Meta has developed a three-pronged, industry-leading approach: prevent, control, respond. First, Meta focuses on preventing harm from happening in the first place. This is achieved by enforcing policies and developing cutting-edge, preventative tools. Second, Meta makes it easy to report potential harms, and third, Meta responds to take action [RL/02 - **META000018**].
- 18 Meta takes the issues of safety and wellbeing on its platforms very seriously, especially for the youngest people who use the services. Meta employs social psychologists, social scientists and sociologists to help ensure that Meta's policies properly account for the presence of young people on Meta's platforms and, as part of that, Meta has dedicated health and wellbeing experts in its safety policy team. Meta has also consulted a range of external groups in the development of its policies, as well as to build programmes that focus on helping young people with everything from bullying and eating disorders to providing parents with the tools to have conversations with the young people in their lives.
- 19 In September 2024, Meta launched Teen Accounts on Instagram for minors aged 13 - 17 in the UK [RL/03 - **META000019**]. In April 2025, Meta introduced new built-in restrictions for Instagram Teen Accounts and expanded these features to Facebook and Messenger [RL/04 - **META000020**]. Teens under 16 will need their parents' permission to change these settings. Teens over 16 can change these settings themselves unless their account is supervised by a parent or guardian, in which case they will need their parent's permission to change their settings. Teen Accounts now apply to all users of Instagram,

Facebook and Messenger aged 13 - 17. Teen Accounts offer automatic protections to limit inappropriate content and unwanted contact, as well as ways to ensure teens' time is well spent. Some of these built-in protections include content audience settings/content audience controls which limit who can view or tag under 18 users in their posts. Meta continually reviews and enhances the Teen Account protections and child safety features, for example in July 2025 it added new safety features to direct messaging in Teen Accounts to give teens more context about the accounts they are messaging and to help spot potential scammers [RL/05 - **META000021**].

### **Non-user access to content**

- 20 An individual without a Facebook account and/or an Instagram account (a “non-user”) could access limited content on Facebook and Instagram, respectively, throughout the Relevant Period. As well as limits on the amount of content a non-user could access (which is explained further below), limits may have also applied to what types of content they could access. Once accessed, the content may also have been subject to warning labels (as explained further at paragraph 28 below). Meta does not attempt to collect age data from individuals without accounts, and therefore is not able to verify the age of non-users.

### **Access to content on Instagram without an account**

- 21 Throughout the Relevant Period, a non-user could access content on Instagram in the following limited circumstances:
- 21.1 During March 2024 to March 2025, users of the iPhone operating system (iOS) who received a link to an Instagram reel in iMessage could open a limited version of the Instagram app, without logging into their regular Instagram account (the “**app clip**”). Through the app clip, iOS users could then see up to approximately 10 reels before being required to login/register for the full Instagram app in order to access any more content. Individuals could not interact (e.g., like or comment) on the reels unless they were logged into Instagram.
- 21.2 Non-users could also access limited Instagram content if they used a web browser or desktop interface. In particular, at all times throughout the Relevant Period, a non-user could view a limited number of posts/reels on a public Instagram profile. Individuals could

not interact (e.g., like or comment) on the posts/reels unless they were logged into Instagram.

- 22 Other than the app clip scenario described above, an individual without an Instagram account could not access any content on the Instagram app throughout the Relevant Period. For individuals to be able to access content on the Instagram app, they must be logged in.

#### **Access to content on Facebook without an account**

- 23 Throughout the Relevant Period, a non-user could access limited Facebook content if they used a web browser or desktop interface (including, for example, if they conducted a search on a search engine and a Facebook reel was one of the hits). In particular, at all times throughout the Relevant Period, a non-user could view a number of public reels; and posts on public profiles, public pages and public groups. Individuals could not interact (e.g., like or comment) on the posts or reels unless they were logged into Facebook.
- 24 An individual without a Facebook account could not access any content on the Facebook app throughout the Relevant Period. For individuals to be able to access content on the Facebook app, they must be logged in.

#### **Meta's policies on terrorism and serious violence**

- 25 Meta aims to create safe and trusted platforms, where people can feel free to express themselves. Meta's terms and policies do not allow people to post content that is against the law or encourages criminal behaviour. In order to achieve the balance between freedom of expression and protection from harmful and illegal content, Meta takes a multi-faceted approach to addressing potentially criminal or harmful activity on its platforms.
- 26 Many of Meta's policies for specific problem areas within the Community Standards cover content that is or is likely to be illegal in the UK. These address the types of potentially harmful content that are of greatest concern or are seen most commonly on Meta's platforms. In addition, Meta prohibits a wide range of objectionable or harmful content that is likely not illegal in the UK, including content that contains graphic violence, spam, misinformation, bullying or harassment. Meta's relevant policies have evolved during the Relevant Period, and these updates and historic changes are recorded in the Community

Standards available online. To give some examples of how Meta’s policies address terrorism and serious violence in particular:

- 26.1 **Violence and Incitement:** Meta aims to deter potential offline harm that may be related to content on Facebook or Instagram. While Meta understands that people may commonly express disdain or disagreement by threatening or calling for violence in non-serious ways, Meta endeavours to remove language that threatens, incites or facilitates violence or are credible threats to public or personal safety. Meta aims to remove content, disable accounts and work with law enforcement when it believes that there is a genuine risk of physical harm or direct threats to public safety. Meta also tries to consider the language and context in order to distinguish casual statements from content that constitutes a credible threat to public or personal safety. In determining whether a threat is credible, Meta may also consider additional information like a person’s public visibility and the risks to their physical safety. In some cases, there are aspirational or conditional threats directed at terrorists and other violent actors (e.g. “terrorists deserve to be killed”), and Meta deems those non-credible absent specific evidence to the contrary.
- 26.2 **Dangerous Organisations and Individuals:** In an effort to prevent and disrupt real-world harm, Meta’s policies do not allow any organisations or individuals that proclaim a violent mission or are engaged in violence to have a presence on Meta’s services. This includes organisations or individuals involved in the following: terrorist activity, organised hate, mass murder (including attempts) or multiple murder, human trafficking, organised violence or criminal activity. We assess these entities based on their behaviour both online and offline - most significantly, their ties to violence. Under this policy, we designate individuals, organisations and networks of people. Meta also endeavours to remove content that it finds or learns about that represents, expresses support or engages in glorification for groups, leaders, or individuals involved in these activities.
- 27 **Violent and Graphic Content:** Meta understands that people have different levels of sensitivity to graphic and violent imagery. To protect users from such content, Meta removes the most graphic content and adds warning labels to other types of violent content so that people are aware that it may be sensitive before they click through. Meta restricts the ability for younger users to see certain types of violent content that may not be suitable or age-appropriate for them. Some content may be appropriate for adults but too mature for teens under 18. Meta has worked with experts and conducted research across countries to understand what types of content are inappropriate for teens to see, and Meta

hides this content from them. This means, while adults still have access to this content, teens under 18 will not be able to see or interact with it, even if it is shared by an account they follow. By doing so, Meta aims to provide an appropriate user experience, while continuing to provide space for users to express themselves. Meta recognises that users may share violent content in order to shed light on or condemn acts, such as human rights abuses or armed conflict. The Community Standards consider when content is shared in this context and allow room for discussion and awareness raising accordingly.

- 28 Since July 2021, Meta has also launched Sensitive Content Controls in Instagram to give users the ability to decide how much sensitive content shows up in all the main recommendation surfaces on Instagram, such as: Explore (Instagram’s home and search page), Reels (short form, vertical videos designed to be watched on a mobile device), Feed Reels (a carousel of reels), and Hashtag pages (a dynamic digital board that collects and displays all public posts using a specific hashtag) [RL/06 - **META000022**]. Sensitive content includes posts that do not necessarily violate Meta’s Community Standards but could potentially be upsetting to some people — such as posts that may be sexually suggestive or violent. This feature has also been extended to Facebook, and now Meta automatically places teens into the most restricted content control settings on Instagram and Facebook [RL/07 - **META000023**].

### **Identification and removal of violating content**

- 29 Meta deploys a combination of tools, including proactive detection technology that removes the vast majority of violating content before anyone reports it. Engineers, data scientists and review teams work together to update and improve this technology over time. Meanwhile, Meta’s technology helps review teams prioritise content. In addition, user reporting and human review mechanisms help enforce the Community Standards and actions on content that violates Meta’s policies or is illegal content. These mechanisms have developed and iterated over time, including across the Relevant Period, and Meta is continuously evolving its approach. Every day, Meta removes millions of violating pieces of content on Facebook and Instagram globally. In most cases, this happens automatically,

with technology such as AI working behind the scenes to detect and remove violating content.

30 In relation to minors specifically, Meta has developed tools to help users, including teens, have safer, more supportive and age-appropriate experiences online, and to help parents and teen users navigate social media together. Meta removes content completely when it breaks its rules, hides sensitive or mature content from teens, and avoids recommending an even broader set of content. Meta is continuously evolving its approach to help make sure it is providing teens with safe, age-appropriate experiences, and to incorporate the best possible research and expert advice to bring parents peace of mind. This includes reporting and blocking tools, parental resources and supervision tools and referrals to resources.

31 Meta constantly seeks to innovate in this area, and the changes it makes to features and tools on Facebook and Instagram are informed through a collaborative process involving a variety of internal and external stakeholders. Where necessary and appropriate, Meta has implemented further safeguards for its teen users, striking a balance between protecting them and facilitating their connection and development in the digital environment. As the way we operate online continues to evolve, Meta is working to ensure that its measures are reviewed and updated periodically.

**i. User reporting**

32 On Facebook and Instagram, users can report content that they suspect violates the Community Standards or is illegal content. On Facebook and Instagram, users access reporting via the “3 dots” menu. These features are easy to access and use, even for the youngest users. Specific reporting steps and the information provided depend on content type and surface, which are explained in the Facebook and Instagram Help Centres.

33 Meta also provides a legal removal request form, which allows individuals in the UK, including both logged-in and non-logged-in users, to report content they believe violates their personal legal rights or applicable local laws.

34 Where Meta takes action in respect of reported content, Facebook and Instagram users generally have access to an appeals process. Meta uses a combination of human review

and technology to process appeal requests. Meta also provides appeals not just for content actioned, but also for content that was reported but not acted on.

## ii. Technology

35 Meta uses automated content moderation (“**ACM**”) tools to proactively detect violating content. Meta removes millions of violating posts and accounts every day on Facebook and Instagram. Most of this happens automatically, with technology working behind the scenes to remove violating content — often before anyone sees it. The vast majority of violating content Meta actions for violence and incitement content is detected and actioned by ACM, as opposed to reported by users.

36 Meta’s ACM tools can be summarised as follows:

36.1 Meta uses privacy-protective matching technology (sometimes referred to as content hashing or content digital fingerprinting) to identify identical or near identical copies of URLs, text, images, audio and videos which Meta has previously identified as violating the Community Standards. This matching technology can work even if minor modifications have been made to the original content. When Meta matches the content exactly or Meta determines it is near identical to previous violating content, Meta will typically remove the content. The lists of known violating content that Meta uses to power the matching technology are typically created after the same content has been repeatedly labelled as violating content by Meta’s human reviewers. For example, when someone tries to upload a terrorist photo or video, Meta’s systems look for whether the image matches a known terrorism photo or video that violates Meta’s Dangerous Organisations and Individuals policy. This means that if Meta previously removed a propaganda video from a designated terrorist organisation, Meta can work to prevent other accounts from uploading the same video to the site. In many cases, this means that terrorist content intended for upload to Facebook simply never reaches the platform [RL/08 - META000024].

36.2 In addition to matching technology, Meta uses AI and machine learning to proactively detect new violating content on Facebook or Instagram services. As with the matching technology described above, AI operates on URLs, text, images, audio and videos. Meta uses these technologies to more quickly identify this content. Unlike technologies that can only match violations they have seen before, AI has the potential to identify certain violations it has never seen before.

- 36.3 Meta uses AI to analyse text that has already been removed for praising or supporting terrorist organisations. This analysis enables Meta to develop text-based signals that can identify when similar content may be terrorist propaganda. That analysis goes into an algorithm that is in the early stages of learning how to detect similar posts. The machine learning algorithms work on a feedback loop and get better over time.
- 36.4 Meta employs rate limits (speed limits), which restrict the speed at which accounts can take actions on Meta's platforms (e.g. posting content), to help prevent misuse of the services by "bots", software programs that automate content generation attempting to simulate human behaviour. Meta sets its rate limiting thresholds by observing how people use the platform and then setting conservative thresholds designed to allow us to address the worst bot behaviour while only infrequently affecting legitimate behaviour by human users.
- 36.5 AI has become one of the most effective tools for reducing the amount of violating content that people see on Meta's platforms, a measure known as "prevalence". As violating content continues to evolve and people look for new ways to evade Meta's systems, Meta will continue working to build more generalised AI systems that can adapt as needed to keep people safe on its platforms [RL/09 - META000025].
- 36.6 Meta also uses AI to identify content that potentially violates the Community Standards. When AI is confident that content violates the Community Standards, it will typically be removed from Facebook or Instagram. Where there is less certainty, content may be prioritised for human review.

### **iii. Human review**

- 37 In those instances where technology does not automatically remove violating content or needs more input, Meta uses human moderators to help enforce the Community Standards. In 2019, Meta had over 30,000 people working in safety and security, including about 15,000 content reviewers around the world, so teams can review reports across time zones. Today, Meta has around 40,000 people working on safety and security issues globally at Meta, with over \$30 billion invested in teams and technology in this area over

the last decade [RL/10 - **META000026**]. The content review teams operate 24/7/365 and moderate in over 80 languages.

38 Meta’s review teams review both user reports and content surfaced by AI tools. Meta’s technology also supports the review teams by prioritising content to be reviewed, for example based on severity, virality and likelihood of a violation. This helps the human reviewers focus on the most important cases that require human review, which Meta also uses to help train Meta’s technology and strengthen the entire content moderation system.

#### iv. Trusted Partners

39 In addition to the automated moderation and human moderation described above, Meta also works with a network of organisations that assist with reporting potential violations of Meta’s policies (“**Trusted Partners**”).

39.1 Trusted Partners help us detect potentially violating content, analyse harmful content trends, and enhance the contextual understanding needed to enforce the Community Standards.

39.2 Meta’s network of Trusted Partners includes non-governmental organisations, humanitarian agencies, human rights defenders and researchers from around the globe. Meta’s network of partners helps Facebook and Instagram to: (i) learn from local experts across the globe, (ii) identify and address policy, process, or training gaps to improve the standard in-platform report/review process, and (iii) help ensure that Meta’s review of high-priority content and accounts is informed by critical and up-to-date context.

39.3 The Trusted Partner Channel provides Meta’s partner organisations with an expedited mechanism for reporting content to Facebook. This channel is distinct from the in-platform reporting tools which are open to all users of Facebook and Instagram and which routes reported content to Meta’s review centres around the globe. In contrast to standard reporting where users select a series of options in requesting review of problematic content, Trusted Partners are able to provide additional context, which is designed to enable deeper investigation and analysis of the content in question. The same content policies are enforced in both the Trusted Partner Channel and standard in-app reporting. Across reporting channels, Meta prioritises reports related to imminent harm and endeavours to only remove the content and accounts that are in violation of the Community Standards.

39.4 For example, Meta is a founding member of the Global Internet Forum to Counter Terrorism (“**GIFCT**”), an NGO bringing together member companies, governments and civil society organisations to tackle terrorist and violent extremist content online. Member companies of the GIFCT use a hash sharing database to help keep their platforms free of terrorist content. In 2022, Meta launched a new tool called “Hasher – Matcher – Actioner” (HMA) to help platforms identify copies of images or videos and take action against them en masse [RL/11 - **META000027**].

**v. Prevention**

40 Much of Meta’s work has focused on disrupting the type of interactions and behaviours that precede violations. Meta has developed targeted solutions, including tools and policies designed to reduce the sharing of violating content. For example, Meta knows from studies of terrorists that they tend to radicalise and operate in clusters. This offline trend is reflected online as well. When Meta identifies Pages, groups, posts or profiles as supporting terrorism, Meta also uses algorithms to “fan out” to try to identify related material that may also support terrorism. Meta use signals like whether an account is friends with a high number of accounts that have been disabled for terrorism, or whether an account shares the same attributes as a disabled account [RL/08 - **META000024**].

41 Meta has become faster at detecting new fake accounts created by repeat offenders. Through this work, Meta has been able to dramatically reduce the time period that terrorist recidivist accounts are on Facebook. This work is never finished because it is adversarial, and the terrorists are continuously evolving their methods too. Meta is constantly identifying new ways that terrorist actors try to circumvent its systems — and Meta updates its tactics accordingly [RL/08 - **META000024**].

**The Online Safety Act 2023**

42 The Online Safety Act 2023 (“**OSA**”) was enacted into law in the UK in 2023 and imposes a range of duties on user-to-user services — including Facebook and Instagram — concerning illegal content and content that is harmful to children. Although the OSA

became law in 2023, most of its key duties only came into effect in 2025, with the remaining obligations taking effect in the coming months and in 2026.

- 43 Meta engaged with UK policymakers both in the development of the OSA and, since its passage into law, in Ofcom's various calls for evidence, consultations and information gathering to give effect to the OSA's provisions.
- 44 Meta is committed to complying with the OSA and will continue to work with Ofcom as the various elements of the OSA continue to take effect. In line with Meta's obligations under the OSA, during 2025 Meta completed its inaugural illegal content risk assessments and children's risk assessments for Meta's various in-scope services. Meta shares with Ofcom the objective of minimising harm effectively, protecting and empowering people, and upholding their fundamental rights.

### **Recommendations**

- 45 The Chair of the Inquiry has been tasked with making recommendations that are practicable. Meta understands that, as part of this, the Inquiry is seeking to understand if any improvements could be made in respect of the availability of violent material on social media.
- 46 Meta has been vocal that new regulatory frameworks must strike a balance between ensuring users' safety and protecting people's rights, such as freedom of speech. Meta's view is that online platforms need to take their share of the responsibility to ensure this is achieved in practice.
- 47 The OSA is a novel and complicated piece of legislation. We will only know in future years what the impact of the OSA has been. However, Meta is cautiously optimistic that, if

