References: 01945198, 01945203, 01945204, 01945234 & 01945237

Information Requests
information.requests@ofcom.org.uk

14 February 2025

Freedom of Information request: Right to know request

Thank you for your requests for information about our recent publications.

We received this request on 17 January 2025 and we have considered your requests under the Freedom of Information Act 2000 ("the FOI Act").

Your requests & our responses

1. *Notes of meetings between Meta/Whats App and Ofcom online safety group staff at which the "technical feasibility" of online safety illegal harms measure 4A (as per 2023 consultation version) was discussed between November 2023-February 2024*

We can neither confirm nor deny whether we hold information in response to this request.

We consider that it is exempt from disclosure under section 44 of the FOI Act. This exemption provides that information is to be withheld if its disclosure is prohibited under other legislation – in this case section 393(1) of the Communications Act 2003 (the Act). Section 393(1) of the Act prevents us from disclosing information about a particular business which we have obtained in the course of exercising a power conferred by, among other legislation, the Act, unless we have the consent of that business or one of the statutory gateways under section 393(2) of the Act is met, neither of which apply here. Section 44 is an absolute exemption under the FOI Act and does not require a public interest test.

2. *Copy of the letter from WhatsApp dated 22 November 2024 referred to in illegal harms statement volume 2 (service design and user choice), page 12, footnote 40*

We can confirm that we hold information in response to this request.

The letter from WhatsApp dated 22 November 2022 was a response to the letter we sent to WhatsApp on 11 November 2024 as part of our standard confidentiality process when we are finalising a publication. We use this process to determine whether stakeholders have any objections to us disclosing information that they have provided to us confidentially. We carefully consider the representations that stakeholders make in response to this process prior to deciding what information we need to disclose, while having regard to section 292(1) and (2) of the Act. It is worth noting that during the confidentiality process, stakeholders from time to time suggest minor changes to the way in which we've summarised evidence they've provided, for accuracy. The letter from WhatsApp constituted its representations.

Section 393(1) of the Act prevents us from disclosing information about a particular business which we have obtained in the course of exercising a power conferred by, among other legislation, the Act,

unless we have the consent of that business or one of the statutory gateways under section 393(2) of the Act is met. A small amount of the information relating to that letter, including the existence of the letter, is information which we have consent from the business to disclose. The majority of that information is published in our statement as you have seen. We received consent to disclose the following extracts, but decided not to include these in the final version of the Statement:

- "Stakeholder(s) to our Call for Evidence flagged the existence and potential of additional 'prompts' that can be served to users as they navigate online services."[1]
- "Stakeholder(s) were of the view that much more is needed to tackle the issue of fraud online. Stakeholder(s) commented on and expressed concerns about several elements of the proposed measure on keyword detection relating to articles for use in fraud including […] the general approach used to address articles of fraud.[2]
- "One service provider noted that standard keyword detection based on mandated standard keywords would have "little to no beneficial effect" on detecting fraud."[3]
- "The views expressed by stakeholder(s) were consistent with our proposal to not expand the measure to cover other fraud types, specifically investment scams, and our conclusion that standard keyword detection is not necessarily the best suited automated content moderation tool for the detection of all fraud types.[4]
- "Stakeholder(s) expressed concern over the costs associated with implementing keyword detection tools. The feedback suggested that these costs may be disproportionate to the limited effectiveness of such tools and may result in diverting resources away from potentially more impactful measures."[5]

We also note that the footnote in question indicates that "WhatsApp have also released similar information publicly" and provides the following link, "About reporting and blocking someone on WhatsApp".

However, we consider that the remaining information, which we do not have consent to disclose, is exempt from disclosure under section 44 of the FOI Act. This exemption provides that information is to be withheld if its disclosure is prohibited under other legislation – in this case section 393(1) of the Communications Act 2003 (the Act). Section 44 is an absolute exemption under the FOI Act and does not require a public interest test.

3. *Confirmation that a child rights impact assessment (CRIA) was carried out on illegal harms code of practice measure ICU C2. If so, please provide a copy of the assessment*

We conducted an impact assessment of all our Codes measures, including (but not limited to) impacts on children.

Our approach to rights assessments is set out in our Statement: context "Our approach to developing Codes measures", paragraphs 1.97 to paragraph 1.103:

[1] Meta response to 2022 Illegal Harms Ofcom Call for Evidence.
[2] Meta response to November 2023 Illegal Harms Consultation, confidential annex, p. 11.
[3] Meta response to November 2023 Illegal Harms Consultation, confidential annex, p.11.
[4] Meta response to November 2023 Illegal Harms Consultation, confidential annex, p.11
[5] Meta response to November 2023 Illegal Harms Consultation, confidential annex, p.11.

In accordance with our obligations under the Human Rights Act 1998, we must consider the impacts that our regulation could have on human rights as set out in the European Convention on Human Rights (ECHR) and ensure that it does not interfere disproportionately with these rights.

We recognise that online safety regulation may also help protect individuals' human rights.

For example, when users feel safe online, they may be more able to exercise their rights to freedom of expression. As set out in 'Introduction, our duties, and navigating the Statement' paragraph 1.21, we start from the position that UK users should be protected from the harms set out in the Online Safety Act and we take account of the evidence of harm set out in our Register of Risks. An important benefit of protecting users from the harms is that their relevant human rights will be protected. We take this benefit into account as part of the assessment of the benefits of the measure which we discuss above.

However, protecting victims' and survivors' human rights is implicit in our duty to carry out our functions so as to secure the adequate protection of citizens from harm presented by content on regulated services. We therefore do not think it is necessary to show that a particular harm to a user infringes their human rights in order to show that the user should be protected from that harm.

Our assessment of human rights in our impact assessment (which is set out throughout our Statement), focuses on whether there is reason to think that a measure which would be effective to address the harm amounts to a disproportionate interference with human rights. In order to assess this, we need to consider the impacts of each measure on the rights that are being interfered with.

Victims' and survivors' human rights may also be engaged in relation to measures we do not recommend, if the harms to which they are exposed both engage their human rights and are sufficiently serious. However, the Online Safety Act does not permit us to make recommendations we have not impact assessed. As set out in paragraphs 1.51 to 1.56 of our Statement: context "Our approach to developing Codes measures", we have adopted an iterative approach to our Codes. Delaying the Codes until we have a fuller set of recommendations would deprive users of such protections as we can put in place now.

Accordingly, although we acknowledge some benefits to human rights of our measures in our thinking, the main focus of our analysis for each measure is on whether their benefits overall justify any possible interferences with human rights.

We have considered the potential human rights implications of each measure, in particular the right to freedom of expression (Article 10 ECHR), the right to freedom of association (Article 11), and the right to privacy (Article 8 ECHR). We have sought to ensure that any interference with adults' and children's relevant rights is proportionate to the legitimate objective of the Act of protecting users from harmful content.

Our rights assessment of measure ICU C1 and C2 is set out in paragraphs 2.75 to 2.102 of Volume 2 of our Statement and covers both adults and children.

4. *Copies of advice from the Ofcom legal directorate to the online safety group on what became illegal harms measure ICU C2 (previously measure 4A) between February 2024 and December 2024*

We can confirm that we hold information in response to this request, however we consider it is exempt from disclosure under section 42 of the FOI Act. This deals with the exemption of information in respect of which a claim to legal professional privilege could be maintained in legal proceedings. In applying this exemption we have had to balance the public interest in withholding the information against the public interest in disclosing the information. The attached annex to this

letter sets out the exemption in full, as well as the factors Ofcom considered when deciding where the public interest lay.

5. *Confirmation of and dates for internal approvals, including Chief Executive, Legal Director, Online Safety Policy Director, Child Safety Policy Director, to adopt the "technical feasibility" change to illegal harms measure ICU C2 prior to publication of the illegal harms statement on 16 December*

There was a process of internal governance. On 12 September 2024, Ofcom's Policy and Management Board formally approved the overall approach to the Illegal Harms Statement and provided approval for key decisions, including the change referred to, with other points of detail left to the Director with delegated authority (Jon Higham).

The delegated authority power was exercised when the document was formally approved for publication on 13 December 2024. Other directors and specialists, including the Legal Director, Technical Director, and Child Safety Policy Director, fed in at appropriate points during the policy development process, including the process for reviewing the detail of the change referred to.

If you have any further queries, then please send them to information.requests@ofcom.org.uk – quoting the reference number above in any future communications.

Yours sincerely,

Information Requests

Request an internal review
If you are unhappy with the response you have received to your request for information, or think that your request was refused without a reason valid under the law, you may ask for an internal review. If you do, it will be subject to an independent review within Ofcom. We will either uphold the original decision, or reverse or modify it.

If you would like to ask us to carry out an internal review, you should get in touch within two months of the date of this letter. There is no statutory deadline for us to complete our internal review, and the time it takes will depend on the complexity of the request. But we will try to complete the review within 20 working days (or no more than 40 working days in exceptional cases) and keep you informed of our progress. Please email the Information Requests team (information.requests@ofcom.org.uk) to request an internal review.

Taking it further
If you are unhappy with the outcome of our internal review, then you have the right to complain to the Information Commissioner's Office.

Annex

<table>
<tr><th colspan="2">Section 42 – Information in respect of which a claim to legal professional privilege could be maintained in legal proceedings is exempt information.</th></tr>
<tr><th>Factors for disclosure</th><th>Factors for withholding</th></tr>
<tr><td>Open policy making and public confidence in regulated activities.</td><td>Ofcom considers the request for Ofcom's internal legal advice is a request for information of which a claim to legal professional privilege could be maintained in legal proceedings. It is advice given by Ofcom's own salaried in-house legal advisers and is connected with the giving or obtaining of legal advice.</td></tr>
<tr><th colspan="2">Reasons why public interest favours withholding information</th></tr>
<tr><td colspan="2">It is in the public interest that policy decisions taken by Ofcom are taken in a fully informed legal context, where relevant. Ofcom therefore needs high quality effectively obtained legal advice for the effective conduct of its business. That advice needs to be given in context, and with a full appreciation of the facts. It needs to be sought and given in a timely fashion to ensure that policy develops in a fully informed way.
Legal advice cannot be effectively obtained unless Ofcom is able to put all the facts before its in-house legal advisers without fear that they may afterwards be disclosed and used to its prejudice. Without such effectively obtained advice, the quality of Ofcom's decision making would be much reduced because it would not be fully informed and this would be contrary to the public interest.</td></tr>
</table>