5RIGHTS FOUNDATION

Ofcom: Researcher Access to Regulated Online Services Information

5Rights Foundation
Call for Evidence response
January 2025

Summary

5Rights welcomes the opportunity to feed into Ofcom's research on researchers' access to data from online services.

Facilitating access to data for independent researchers is crucial to understanding how digital products and services operate and the impact they have on society. Access to such data will play a central role in the transparency and accountability of digital services, which is crucial to the success of, and compliance with, the UK's online safety regime.

This access will address the current asymmetry of power and information between independent researchers and the world's largest companies, who are rich in the currency of our age - data. Outside of information released by whistleblowers,[1][2][3] everything we know about how these systems operate is entirely controlled by industry, whose stakeholder-produced reports have a vested interest in making the company look the best it can, which obscures problems that can and should be fixed. This was a key point raised in the discussion of the provisions during the passage of the Online Safety Act. As noted by Lord Bethell, "*... only the companies themselves can see the full picture of what goes on the internet. That puts society at a massive disadvantage and makes policymaking virtually impossible.*"[4]

This call for evidence is an essential first step in understanding the challenges researchers currently face and how this situation can be made easier. The evidence in our response is drawn from our own experience and that of our academic colleagues from the LSE Digital Futures for Children Centre (DFC). To support regime and the new powers set out in the Data (Use and Access) Bill we recommend that:

- The range of data and pool of researchers provided access be drawn as broadly as possible (Annex 1 provides examples of what could be relevant).

[1] Béjar, A. (2023) Written Testimony of Arturo Bejar before the Subcommittee on Privacy, Technology, and the Law, November 7, 2023

[2] Haugen, F. (2021) Statement to the United States Sub-Committee on Consumer Protection, Product Safety, and Data Security

[3] The Wall Street Journal (2021) *The Facebook Files: Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*

[4] Lord Bethell (22 June 2023) Online Safety Bill, Committee Stage (Day 10), cols. 390-391

- A focus is placed on facilitating access to granular and exact data to support researchers analysing systemic risks to society stemming from the design or functioning of a service and its related systems (including algorithmic systems).
- Any perceived limitations in responding to a request for data must be justified by tech companies.

Current experiences of research and data access

1. How, and to what extent, are persons carrying out independent research into online safety related issues currently able to obtain information from providers of regulated services to inform their research?

    a. What kind of online safety research does the current level of access to information enable?

There are several ways researchers currently access data from digital services, including:[5]

- **Web scraping/crawling**: extracting data from a website (scraping) or using a type of bot to index links (crawling).
- **Research application programming interfaces (APIs)**: tools tied to online services (e.g. Google, TikTok, Meta) where researchers can access data sets.
- **Data donations**: directly partnering with individuals interested in donating their digital traces for research purposes.
- **Integrated data service:** cross-sector government initiatives providing a platform for accredited researchers to access data and analytical tools.
- **Purchasing data sets:** purchase of specific datasets online.
- **Data repositories:** databases specialising in the collection of sensitive data.
- **Data sharing programmes:** UKRI funded programmes[6] that streamline access to data from online spaces.
- **Avatars and simulations:** research experiments designed to replicate the experiences of specific users.

These methods have been drawn on to collect a wealth of research particularly in relation to occurrence of specific harm, harms to specific groups and/or society, design-based risks, content-based risks and threats to public safety. Below we list some examples:

- 5Rights *Pathways* research[7] illustrates how the commercial interests and business models of tech companies drive design choices that lead children to

[5] The British Academy (2024) *Data as a Tool for Researching the Digital World: Summary Brief*, p. 7

[6] See: UK Research and Innovation (UKRI) (ND) *What we've funded*

[7] 5Rights Foundation (2021) *Pathways: How digital design puts children at risk*

harm. Revealing Reality researchers used child avatars, based on the interests of and interviews with children, to replicate their experiences on social media.

- Amnesty International's *Driven into the Darkness* research[8] examined how TikTok's recommender system created "rabbit holes" of harmful content targeted towards children. The research used an "automated algorithmic audit" of its recommender system using research accounts, simulating a 13-year-olds' activity.
- A Wall Street Journal investigation[9] into Instagram's content recommender system found it connected accounts to 'vast' networks of child sexual abuse material. The research used newly set up accounts to monitor how suggestions changed after viewing CSAM-hosted accounts.
- Center for Countering Digital Hate has drawn on a number of these methods to undertake research into how content is pushed towards vulnerable users. In December 2024, the NGO published research based on 100 simulations of how YouTube promoted eating disorder and weight loss content to vulnerable young people.[10]
- Revealing Reality research on Snapchat interviewed children and child support professionals to detail the experiences of children's experiences on the service: the content they saw and the features and functionalities that pushed it.[11]
- DFC research examining the impact of digital regulations[12] used publicly announced information to assess changes made to the services. In gathering this information, researchers "wrote to 50 companies for information about changes they had made", however only 8 responded with limited evidence.

b. Are there types of information that researchers are currently unable to access that may be relevant to the study of online safety matters?

Data-driven recommender systems, which can personalise content based on known or inferred characteristics to extend children's use and engagement, are at the heart of the largest digital services – geared towards revenue generation and the benefit of the wider tech sector business model.[13]

[8] Amnesty International (2023) *Driven into Darkness: How TikTok's 'For You' Feed Encourages Self-Harm and Suicidal Ideation*

[9] Wall Street Journal (2023) *Instagram Connects Vast Pedophile Network*

[10] Center for Countering Digital Hate (2024) *YouTube's Anorexia Algorithm: How YouTube Recommends Eating Disorder Videos to Young Girls*

[11] Revealing Reality (2023) *Anti-social Media: The violent, sexual and illegal content children are viewing on one of their most popular apps*

[12] Wood, S. (2024) *Impact of regulation on children's digital lives*, Digital Futures for Children Centre, 5Rights Foundation, LSE

[13] *Pathways: How digital design puts children at risk*

As a result, tech companies are opaque about how their recommender systems work. Indeed, these systems often subject children to profiling and automated processing with no adequate transparency or accountability, including from researchers who may wish to know more about these systems.[14]

Current challenges and risks for researchers

2. What are the challenges that currently constrain the sharing of information for the purpose of research into online safety related issues?
    a. What are the legal challenges/risks to sharing information from online services with independent researchers?
    b. What are the security challenges relating to sharing information from online services with independent researchers?

Despite the current pathways available to researchers, and the excellent analysis and work published, many still encounter challenges when gathering data from online services, which risks compromising the utility, integrity and creativity of their research.[15] Below we highlight some of the most significant barriers to access.

Increasing difficulty in accessing reliable data

In recent years, it has become more difficult to access data held by tech companies.[16] This poses a serious challenge to researchers investigating behavioural patterns that inform the impact digital technologies have. Existing avenues that allow researchers to access datasets within legal and ethical frameworks are closing, or becoming increasingly unreliable.

Access to APIs – which offer researchers access to large, rich datasets and provide flexible and customisable access – are being blocked or limited by tech companies.[17] For example, in 2023, Twitter (now X) cut access to its free API and began charging for access – its enterprise packages costing between $42,000 and $210,000 per month.[18] This is unaffordable for researchers and deprives them of high quality data needed to conduct impactful, real-time research.[19]

Historically, tech companies have been unwilling to share information in cases where there are known harms that are not sufficiently mitigated. Instead, the testimony of whistleblowers and/or internal document leaks have been heavily relied upon to bring to

[14] See: Livingstone, S. & Sylwander, K. R. (2024) *Children's rights and the global digital compact*

[15] *Data as a Tool for Researching the Digital World*, pp. 8-9

[16] Ibid.

[17] See: McDonnell, D. (2020) "Web-scraping for Social Science Research: APIs as a Source of Data", *UK Data Service*

[18] Binder, M. (2023) "Twitter's new API plan costs up to $2.5 million per year", *Mashable*

[19] Coalition for Independent Technology Research (2023) *Letter: Twitter's New API Plans Will Devastate Public Interest Research*

light these concerns. For example, whistleblowers Frances Haugen[20] and Arturo Béjar[21] exposed Meta's knowledge of the harms their services were causing – in particular to girls; and leaked internal communications at TikTok revealed executives knew proposed time management tools would have negligible impacts on children's compulsive use of the service – but still released these features anyway and promoted them as 'wins'.[22]

The failure of tech companies to be honest in their knowledge of how their services cause harm creates a disproportionate burden on academia and civil society organisations' resources, who have less much less funding but the need to uncover metrics that already exist through their own labour-intensive investigations.

Legal risks

Certain data gathering methods also put researchers at legal risk. Data scraping can lead to violations of terms of service and tech companies have previously taken action against researchers using these methods. For example, a group of New York University (NYU) researchers investigating political ad targeting on Facebook had their accounts suspended and access blocked to the service, citing privacy concerns.[23]

Security implications

Some researchers have concerns about companies engaging in revenge-seeking behaviour, which is more feasible if they are leaving a 'footprint' of their research and there is not sufficient protection in place for these researchers.[24]

Models for solutions

3. How might greater access to information for the purpose of research into online safety issues be achieved?

Examples of data that could be requested

For researchers – both academic and civil society – seeking to understand how features and functionalities impact users, it is important that a researcher access provision allows for access to the widest possible range of data, including supporting documents.

Accompanying documentation, such as risk assessments or product testing results, is critical in understanding the choices as to *why* a certain feature or functionality has been implemented or rolled out – as well as understanding if there were internal concerns

[20] Statement to the United States Sub-Committee on Consumer Protection, Product Safety, and Data Security

[21] Written Testimony of Arturo Bejar before the Subcommittee on Privacy, Technology, and the Law

[22] 5Rights Foundation (2024) *TikTok knows it is harming children*. See also: NPR (2024) *TikTok executives know about app's effect on teens, lawsuit documents allege*

[23] See: Edelman, G. (2021) "Facebook's Reason for Banning Researchers Doesn't Hold Up", *WIRED*

[24] Raji, I & Buolamwini, J. (2019) *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products*, Conference on Artificial Intelligence, Ethics, and Society

beforehand. It is also key to identifying what, if any, KPIs were prioritised in the design, development, deployment and evaluation of a feature.[25]

Access to source code would be the most complete and direct way to understand and analyse service features and functionality – but this is met with a number of legal, commercial and practical constraints. Access to data should allow for comparable knowledge of a service or feature.

We set out examples of data that could be requested relating to analysis of service and feature design in Annex 1.

Format of data

Data should be provided in a format that is accessible to researchers and is easy to understand. Formats that allow for purposeful use of the data by the organisation or researcher accessing it (e.g. through use of APIs, data vaults or other machine-readable data exchange formats). Formatting of data that makes accessibility, analysis and interpretation of data more difficult should be avoided and, where such formats are used, should not be regarded as having fulfilled a data access request.

The format of data is particularly important, given previous attempts by tech companies to "dump" data in legal cases with the intention of delaying the process. For example, during the Molly Russell inquest, Meta handed over its first disclosure of information the night before the pre-inquest hearing and it could not "be reviewed in a long sitting and certainly not late at night"[26] owing to the thousands of data points received at short notice.

Breakdown of data should also be relevant to the research request. For example, for the purpose of investigating systems and service design as they impact children, where the service has a significant number of children (any user under the age of 18) or if it is likely to be accessed by children then it should break down data by age or age groups, taking any age-specific requirements specified by law (e.g. processing of personal data) or by a company's terms and conditions, as well as other markers used for age-appropriate design.

Researcher accreditation

Given the differential of resources and power between tech companies, academics and civil society organisations, it is very important that the researchers provided access to company data be broadly defined.

The provisions in the Data (Use and Access) Bill are drawn widely, and could allow for a variety of groups with interests in online safety – e.g. academics and civil society organisations – to obtain data that is impactful to their work. We would recommend that any accreditation process speaks to this spirit, whilst also having safeguards protecting those with commercial interests from obtaining vast quantities of data.

[25] Internal documents revealed that TikTok's time limit tool aimed at 'improving public trust' rather than limiting app usage. See: *TikTok executives know about app's effect on teens, lawsuit documents allege*

[26] Varney, M. (2022) *A family's battle against the tech giants – Molly Russell's inquest*, Leigh Day

To minimise such risks and ensure researchers are independent from commercial interests, publicly accessible transparency requirements in terms of funding, declared purposes and financial and non-financial links to companies may be appropriate.

Importantly, the accreditation of researchers must offer a degree of flexibility, as the ways in which academia and civil society organisations will wish to use and analyse data will inevitably vary. Considerations therefore should not only focus on the academic and/or technical credentials of the applicant, but also consider the specific risk that the research is seeking to analyse and its potential – to allow consideration, participation and contributions of vulnerable groups, such as children.

Additionally, researchers outside of the UK should have the ability to request UK data. This is a possibility under the current drafting of the EU's Delegated Act on data access[27] and would allow for proper analysis of systemic risks by comparing and contrasting trends in other regions.

a. What models, arrangements or frameworks exist allowing researchers access to sensitive information beyond the online services industry?

We acknowledge some of the research methods already used by researchers in the first part of our response.

Trusted data institutions

There are a number of trusted data institutions whose role is to steward data on behalf of others, often towards public, educational or charitable purposes.[28] Supporting these organisations can help bolster the use of data for public good by protecting sensitive data and creating open datasets and standards.[29]

Trusted data institutions already operate in a number of different sectors, including education (Higher Education Statistics Agency (HESA)),[30] health (UK Biobank),[31] as well as across sectors, such as Smart Data Research UK.[32]

b. Are there any models or arrangements in the online services industry already that might provide increased access to information for research purposes if applied more generally across the industry?

We acknowledge some of the research methods already used within the industry the first part of our response.

APIs

[27] See: 5Rights Foundation (2024) *Access to data under the DSA: Response to the European Commission consultation on the proposed Delegated Regulation*

[28] Open Data Institute (2020) *Designing trustworthy data institutions*

[29] Open Data Institute (2021) *What are data institutions and why are they important?*

[30] Higher Education Statistics Agency

[31] UK Biobank

[32] Smart Data Research UK

Many social media services do offer API support, but increasingly this is only at a significantly high bar of entry for researchers.[33]

The value of API systems in being able to programmatically access specific datasets has the ability to produce impactful research. APIs generally also require less time and effort to use (as compared to scraping methods), and are generally accompanied by documentation making the initial knowledge barrier for researchers lower.

However, APIs can sometimes be challenging or lacking for online repositories – the EU's DSA Transparency Database[34] is one such case as, up until recently, access was limited to services themselves.

Sandboxed environments

Sandboxed environments allow researchers to test and analyse design features and functionalities in a controlled environment.

For researchers, the ability to use features and functionalities in sandboxed environments allows for A/B testing in a secured space with minimal risks of adverse impacts from research on users.

Examples of sandboxed environments already in use include:

- The Information Commissioner's Office's (ICO) Regulatory Sandbox,[35] which is free to organisations creating products and services that use personal data.
- Meta operates its AI Sandbox[36] for a subset of public content posted in groups/pages based in the EU and other select countries.

c. What are some possible models for providing researchers with access to relevant information that may not exist or be widely used yet, but which might be implemented by industry?

The EU's provisions on data access for researchers under Article 40 of the Digital Services Act are set to be adopted in the next few months.[37] The provisions mean Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) are required to provide access to data.

For more information, please refer to 5Rights consultation on the final version of the draft Delegated Regulation, published in December.[38]

---

[33] See: Section 2

[34] European Commission, DSA Transparency Database

[35] Information Commissioner's Office, Regulatory Sandbox

[36] Meta, *Introducing the AI Sandbox for advertisers and expanding our Meta Advantage suite*

[37] See: European Commission, Delegated Regulation on data access provided for in the Digital Services Act

[38] *Access to data under the DSA: Response to the European Commission consultation on the proposed Delegated Regulation*

About 5Rights Foundation

5Rights develops new policy, creates innovative frameworks, develops technical standards, publishes research, challenges received narratives and ensures that children's rights and needs are recognised and prioritised in the digital world. While 5Rights works exclusively on behalf of and with children and young people under 18, our solutions and strategies are relevant to many other communities.

Our focus is on implementable change and our work is cited and used widely around the world. We work with governments, inter-governmental institutions, professional associations, academics, businesses, and children, so that digital products and services can impact positively on the lived experiences of young people.

5Rights is a registered charity. Charity number: 1178581.

Annex 1 – Examples of data that could be requested relating to service design

1. Details on all algorithms used, together with:
2. List of all algorithms used in the provision of the service/feature;
3. Detailed explanations of;
    i. The intentions, including the issue(s)/challenge(s) that those implementing the algorithm sought to address;
    ii. The model;
    iii. The specified design and success criteria; and
    iv. Any assumptions used in building the algorithm.
4. Product development information, documents and internal communications such as emails and meeting notes in which the service or product was discussed;
5. Sample input/output data demonstrating the functioning of the algorithm;
6. Data sets used to train algorithms;
7. Data sets used in testing or sandboxing; and
8. Outcome data sets from testing or sandboxing.
9. Information on data processing and specific data sets, including:
    a. User data sets, outcomes recorded;
    b. Distribution within the dataset (e.g. is there a group that is clearly under sampled or not represented?);
    c. Data journeys;
    d. Combined data sets (e.g. of behavioural data together with data on push or pull factors used);
    e. The categories (and sub-categories) of data processed by any service or feature thereof, the purposes therefor and any limitations posed on the use or sharing of certain categories of data (including inferred personal data);
    f. Access to real-time data further to perform on-platform independent testing.
10. Documentation (including internal documents and communications) providing detailed information regarding:
    a. Internal structures and roles, competencies relations between, allocated budgets and evolution over time;
    b. Internal processes for product design and operation, decision-making, oversight and accountability;

c. The categorisation of risks, harms and positive impacts on the enjoyment of rights, as well as the measurement metrics and mechanisms used to track risks and outcomes over time and inform decisions;

d. The categorisation of rights and interests, the criteria and decision-making process used to balance any differing rights or interests, the records of these decisions, and the mechanisms used to identify and flag for resolution any potential conflicts between rights and interests;

e. Child rights impact assessments (CRIAs);

f. Data Protection Impact Assessments (DPIAs);

g. The functioning as well as the design of features, notably purposes and intended outcomes underpinning design decisions, including but not limited to:

    i. Data related to the issue(s)/challenge(s) that those designing the given system sought to address and how and why these elements changed over time;

    ii. Product development information, documents and internal communications such as emails and meeting notes in which the service or product was discussed;

    iii. Data regarding types of, formats and timing of notifications, pop-ups, nudges, information delivery and consent/choice requests (together with data regarding any push/pull factors); and

    iv. Data regarding design of reporting, complaint and support systems.

h. Why a certain feature, process or system was considered necessary, and who was involved and their role in defining its issue(s) and desired outcome(s), including but not limited to:

    i. Data on the role of those involved in defining the problem(s) and outcome(s), including internal and external stakeholders; and

    ii. Data on if, how and why these elements changed over time.

i. The inputs or elements considered when designing and/or operating a certain feature or system, possible alternatives explored and the rationale for their consideration and evaluation, as well as the datasets used to inform such consideration and testing of the feature or system, including but not limited to:

    i. Data on the variables/features that the system's designers want to include as inputs and the rationale for their inclusion;

    ii. Data on whether and why those variables/features were included, substituted for others and/or excluded;

11. Information on dataset(s) used for building, training, and testing the systems, and whether and why other datasets were (not) considered for any of those phases; and

12. Information on how and by whom these datasets were evaluated and selected, and against which criteria.
    a. How the provider company (re)uses the feature or system's outputs/outcomes and data generated, as well as internal process, roles and benchmarks for evaluating performance of such feature or system, their impact on users and/or wider communities, and decisions related to their possible update or change;
    b. Product records:
        i. Product design records: detailed documentation of aims, intended outcomes, process, inputs, options, technical assumptions, models, and records of instructions and decisions, with criteria and justifications, pertaining to the design of any given service or features thereof; and
        ii. Product review and optimisation records: detailed documentation of process, inputs, options, technical assumptions, models, and records of instructions and decisions, with criteria and justifications, pertaining to the review, optimisation, upgrade or decommissioning of any given service or features thereof.
13. Access to company personnel, including at the working level (e.g. designers) in order to verify the above and have qualitative insights into company culture and processes; and
14. Access to internal communications (e.g. emails), meeting agendas, meeting minutes, action plans, communication materials, surveys, consultation documents, codes, etc.