December 2025

Fairer Terms for Data Access

Towards Fairer Terms for Data Access under Article 40(12) DSA

Mozilla Foundation

Towards Fairer Terms for Data Access under Article 40(12) DSA

Analysis of contractual terms used by platforms in the context of Article 40(12) data access

Introduction

Article 40(1) of the EU's Digital Services Act ('DSA') introduced obligations on providers of very large online platforms and search engines (hereafter 'platforms') to provide Digital Services Coordinators ('DSCs') and the European Commission ('EC') access to data *'that are necessary to monitor and assess compliance'* with the DSA. To assist in this monitoring and assessment, and empower other actors in scrutinising systemic risks and platforms' practices, Article 40 of the DSA also creates two obligations on platforms to provide access to data to researchers:

i. Article 40(4) requires platforms to provide access to data (including non-public data) to 'vetted researchers' (those who meet the requirements of Article 40(8)) upon a 'reasoned request' from DSCs, for the 'sole purpose of conducting research that contributes to the detection, identification and understanding of systemic risks' pursuant to Article 34(1) and 'to the assessment of the adequacy, efficiency and impacts of the risk mitigation measures' pursuant to Article 35. This only applies to 'research organisations' that meet the criteria in Article 2(1) of Directive (EU) 2019/790 (the Copyright in the Digital Single Market Directive)

ii. Article 40(12) requires platforms to give access to data that is 'publicly accessible in their online interface' to researchers who comply with the conditions set out in Article 40(8)(b)-(e) and who use the data 'solely for performing research that contributes to the detection, identification and understanding of systemic risks' pursuant to Article 34(1)

Since the DSA came into force, platforms have set up processes for researchers to apply to be granted access to data under Article 40(12). Typically, access is only permitted under certain contractual terms and conditions imposed by platforms on researchers. Per our discussions with researchers, platforms in some cases seek to justify these terms as

required by the DSA itself, or by other regulation such as the General Data Protection Regulation ('GDPR').

Researchers consulted shared with us that these terms often impose unreasonable conditions on access that exceed the requirements of Article 40(12) and/or the GDPR, and which can seriously constrain their research.

AWO was asked by Mozilla Foundation to investigate and analyse this issue. We based our analysis on the terms that are either the main terms through which researchers sign up to for access to data (usually specifically named 'research terms'), or terms that are otherwise integrated to these primary research-specific terms and are binding on researchers (usually developer-related terms):

Meta

i. ICPSR Terms of Use: https://www.icpsr.umich.edu/web/ICPSR/studies/42/terms

ii. Restricted Data Use Agreement ('Meta RDUA')[1]: https://myumi.ch/y2x8d

LinkedIn

i. Additional Terms for the LinkedIn Research Tools Program ('LinkedIn Research Terms'): https://www.linkedin.com/legal/l/research-api-terms

TikTok

i. Research Tools Terms of Service ('TikTok Research ToS'): https://www.tiktok.com/legal/page/global/terms-of-service-research-api/en

ii. Global Data Sharing Research Appendix ('TikTok Research DSA'): https://www.tiktok.com/legal/page/global/global-data-sharing-research-appendix/en

iii. TikTok Compliance Certification: https://www.tiktok.com/legal/compliance-certification?lang=en

iv. Developer Terms of Service ('TikTok Developer Tos'): https://www.tiktok.com/legal/page/global/tik-tok-developer-terms-of-service/en

v. Developer Data Sharing Agreement ('TikTok Developer DSA'): https://www.tiktok.com/legal/page/global/tiktok-data-sharing-agreement/en

[1] We understand that in some cases, individual researchers are not required to sign up to the RDUA where their organisation does not permit this. In such cases, the research organisation is instead asked to sign up to an information sharing agreement, so that Meta's terms are instead enforceable against the institution: https://developers.facebook.com/docs/content-library-and-api/get-access

X

i. X Developer Agreement: https://developer.x.com/en/developer-terms/agreement

ii. X Developer Policy: https://developer.x.com/en/developer-terms/policy

iii. X Developer Terms – Commercial and non-commercial use of the X API: https://developer.x.com/en/developer-terms/commercial-terms

YouTube

i. Researcher Program Terms of Service ('YouTube Research ToS'): https://research.youtube/policies/terms/

ii. API Service Terms of Service ('YouTube API ToS'): https://developers.google.com/youtube/terms/api-services-terms-of-service

iii. API Service Developer Policies ('YouTube API Developer Policies'): https://developers.google.com/youtube/terms/developer-policies

To analyse these terms, we:

i. Carried out an analysis of the terms & whether they are justified by the DSA, GDPR or other regulation, and whether they could constrain research (Summer 2025).

ii. Discussed the analysis with a steering group of platform researchers and obtained their feedback on whether these terms were creating problems in practice, and what they considered as priority areas. This took place in three phases between June and October 2025: (a) sharing a detailed table of terms analysed for written comments, (b) discussing issues and priorities with researchers remotely via video call, and finally (c) workshopping the issues raised by Article 40(12) terms during a session at an in-person event focused on researcher access to data. We are unable to share the identities of the specific researchers we consulted, but they come from leading academic and civil society organisations involved in platform research, including those who have been among the very first to begin to make use of the processes mandated by Article 40 DSA.

iii. Have now summarised this combined analysis and feedback below, structured around key thematic issues, with examples of potentially problematic terms and some case studies and anonymous testimonies of how researchers say these terms have delayed or blocked their access to data.

Summary

Our analysis shows that all of the five platforms impose terms that exceed the requirements of DSA Article 40(12) and GDPR. Based on discussions with platform researchers, we understand that these terms can restrict access to data in a range of ways which constrain research. We have categorised the problems that these terms may raise according to the different stages or aspects of the data access relationship between the researchers and the platforms[2]. The table below gives a high-level overview, for each category, of the types of terms analysed.

Issue Category	Terms which may constrain research[3]
Qualification criteria	Requiring evidence of experience and expertise in relevant research area and/or data processing Requiring academic qualification or anything beyond DSA Article 40(8)(b)-(e)
Access method restrictions	Absolute prohibition on downloading or exporting data from the platform's environment Prohibition on processing certain types of data (children's, criminal offence, sensitive…) outside of the platform's environment
Use restrictions	Prohibition on use of research data for anything objectionable to, or critical of, the platform Broad or vague restrictions on use of research data; in some cases as part of application approval Prohibitions on aggregation of data, cross-dataset analysis, and other data

[2] Dashed-line boxes set out reports of the impact in practice of terms which can constrain research. Coloured boxes highlight example term wording.
[3] In some cases, the potential for terms to constrain research depends on how they are (sought to be) enforced by platforms. As discussed in detail below, the potential for arbitrary enforcement of broad and vague restrictions on researchers can itself, however, be a significant constraint on research.

	analysis methods that require exporting the data
Platform rights to monitor and terminate access	Platform's right to terminate or suspend access at any time without notice
Rate/Quota restrictions	Determination, adjustment and suspension of access rates or quotas at platform's sole discretion Prohibition on exceeding 'reasonable request volume'
Scraping restrictions	Absolute prohibition on scraping and other access via automated means, including for verification Restrictions on scraping at the platforms' sole discretion
Onward sharing restrictions	Absolute prohibition on sharing both data and derivatives with any third party Broad or vague restrictions on the release of derived data and statistics
Data management obligations	Strict, unconditional data refresh and deletion requirements Data management plans or impact assessment requirements regardless of risk posed Broad and vague obligations to delete data Imposition of unreasonably onerous data security protocols, disproportionate to the data protection issues raised.
Publication-related obligations and rights	Advance notice requirements with right for platform to revise or edit output Unrestricted right for platform to use and divulge research project and output

	Platform rights to use researchers' work for commercial purposes
Indemnity and liability	Indemnification obligations arising from wide, indirect causes of action Unlimited liability

Detailed analysis: terms not justified by the DSA which may constrain research

Qualification criteria

Article 40(12) of the DSA provides that platforms must provide access to data to:

> *researchers, including those affiliated to not for profit bodies, organisations and associations, who comply with the conditions set out in paragraph 8, points (b), (c), (d) and (e), and who use the data solely for performing research that contributes to the detection, identification and understanding of systemic risks in the Union pursuant to Article 34(1).*

The conditions in Article 40(8) points (b) to (e) are:

> *(b) they are independent from commercial interests;*
>
> *(c) their application discloses the funding of the research;*
>
> *(d) they are capable of fulfilling the specific data security and confidentiality requirements corresponding to each request and to protect personal data, and they describe in their request the appropriate technical and organisational measures that they have put in place to this end;*
>
> *(e) their application demonstrates that their access to the data and the time frames requested are necessary for, and proportionate to, the purposes of their research, and that the expected results of that research will contribute to the purposes laid down in paragraph 4;*

A significant concern with some of the terms we have analysed, based on researchers' feedback, is that platforms impose excessive or vague criteria for researchers' qualification for access, purportedly in relation to the requirements in Article 40(8) points (b) to (e) . When excessive, criteria may prevent researchers who should be entitled to data from

accessing it. When vague, criteria may be applied and interpreted by platforms in an opaque manner that researchers cannot understand nor challenge, effectively leaving researchers reliant on the 'goodwill' of platforms in relation to each data request or research project; this could be seen as undermining the independence of research.

An issue related to excessive or vague qualification criteria is that platforms sometimes seem to use them to delay access to data, which can undermine or even kill a research project. This was the case when Democracy Reporting International (DRI) sought access to publicly available data from X for the 2025 German general election period, to study the influence of platforms on the election. Obtaining data before and during the election was important to the project, as publicly available data can change at any time (e.g. by users deleting their posts or the platform taking them down). DRI's requests were significantly delayed, and ultimately X refused to provide access to the data. [4]

TikTok Research ToS I.3

Access only granted to *"Academic research institutions and other non-academic research bodies, organizations and associations that meet the following criteria: (i) have demonstrable experience and expertise in the relevant research areas and in the processing and analysis of data; and (ii) has as one of its principal aims the conduct of research on a not-for-profit basis pursuant to a public-interest mission;"*

This term raises several issues and uncertainties for researchers. First, *'Not-for-profit […] pursuant to a public interest mission'* is narrower than the DSA Article 40(8)(b) requirement of being *'independent from commercial interests'*. It rather reflects the DSA Article 40(8)(a) requirement of being a 'research organisation' as defined in the Copyright in the Digital Single Market Directive, which is only relevant for Article 40(4) access, not Article 40(12).

Second, having *'demonstrable experience and expertise in the relevant research areas'* is not a DSA requirement, and irrelevant to the necessity and proportionality of researchers' access to data for the purposes of systemic risk research. Finally, having *'demonstrable experience and expertise […] in the processing and analysis of data'* is narrower than the DSA Article 40(8)(d) requirement of being *'capable of fulfilling the specific data security and confidentiality requirements corresponding to each request and to protect personal data'*.

[4] GFF, X Prevents Research on Potential Election Interference https://freiheitsrechte.org/en/themen/digitale-grundrechte/x.

Meta RDUA

I.E. "Restricted Data" are the research dataset(s) provided under this Agreement that include potentially identifiable information in the form of indirect identifiers that if used together within the dataset(s) or linked to other dataset(s) could lead to the re-identification of a specific Private Person, as well as information provided by a Private Person under the expectation that the information would be kept confidential and would not lead to harm to the Private Person. Restricted Data includes any Derivatives.

I.F. "Private Person" means any individual (including an individual acting in an official capacity) and any private (i.e., non-government) partnership, corporation, association, organization, community, tribe, sovereign nation, or entity (or any combination thereof), including family, household, school, neighborhood, health service, or institution from which the Restricted Data arise or were derived, or which are related to a Private Person from which the Restricted Data arise or were derived.

III. C. Investigators must meet each of the following criteria: 1. Have a PhD or other research-appropriate terminal degree; and 2. Hold a faculty appointment or have an appointment that is eligible to be a principal investigator at Institution.

IV. The Institution represents that it is: A. An institution of higher education, a research organization, a research arm of a government agency, or a nongovernmental, not-for-profit, agency. B. Not currently debarred or otherwise restricted in any manner from receiving information of a sensitive, confidential, or private nature under any applicable laws, regulations, or policies. C. Have a demonstrated record of using sensitive data according to commonly accepted standards of research ethics and applicable statutory requirements.

Reading these terms together, Meta's RDUA applies to the access they provide (through their secured 'Virtual Data Enclave') under both Article 40(4) and Article 40(12). The definition of 'Restricted Data' is extremely wide – it depends on the definition of Private Person which is also very wide, going beyond the definition of 'personal data' in the GDPR, as it includes data related to non-individuals (groups, companies…). Hence 'Restricted Data' seemingly extends to all data on the Meta platforms. Meta may provide pseudonymised data to researchers that is not 'Restricted Data', but this would not meet their obligation under Article 40(12), since a lot of publicly available data identifies individuals and groups. If this interpretation is correct and Meta's data is only or mostly Restricted Data, these terms severely restrict researchers' ability to analyse it.

While these terms may be appropriate for Article 40(4) access, they are much more restrictive than what Article 40(12) allows, requiring the lead investigator to 'have a PhD

or other research-appropriate terminal degree' and to be appointed by an institution that meets certain requirements. By contrast, Article 40(12) only requires researchers to be not-for-profit, to be capable of keeping data safe, and to be pursuing research into systemic risks.

Term IV.C. also diverges from the 'capability' language of Article 40(8)(d). According to researchers, Meta's application form even specifically asks for 'Evidence of responsible experience or use of sensitive or restricted data'.

YouTube Research ToS

1.d "Qualified Academic Research Institution(s)" means academic institutions that are: i. dedicated to the pursuit of education and research with the intended outcome being the receipt of academic degrees; ii. accredited as indicated by information provided on the institution's website (e.g. a university) and/or as demonstrated by documentation provided to YouTube; iii. qualified to give out educational degrees (undergraduate, graduate, doctoral, etc.); and iv. a not-for-profit endeavor (i.e. not a business whose sole purpose is to make a profit).

1.e "Qualified Institution(s)" means and includes (a) Qualified Academic Research Institutions and (b) any government or other institution required by law or regulation to have access to Program Data.

4.c In order to be accepted into the Program, you must: be affiliated with a Qualified Institution;

YouTube's qualification terms are more generous than TikTok's or Meta's. The definition in 1.d may unduly restrict the definition of an 'academic institution', but the catch-all term 1.e(b) can effectively be interpreted to cover any researcher that fulfils the DSA Article 40 criteria. Researchers have told us that in practice, YouTube has been more flexible with access than other platforms.

Restrictions on mode of access

Platforms' terms generally involve providing Article 40(12) data access to researchers through a secure virtual environment. Researchers consulted find that the functioning of those environments often imposes restrictions on researchers' ability to export or download data. This can be a significant problem for researchers, both in relation to running

bespoke analyses on raw data (including independent verification, replication, and cross-dataset analysis), and for the data they analyse to be up-to-date and responsive:

> *Whether the goal is to merge platform data with external datasets, conduct cross-platform comparisons, or identify emerging patterns, researchers need direct and granular access to raw data. Research exploration, iteration, and methodological transparency all depend on access to raw data.*[5]

These restrictions also go against the recent approach taken by the European Commission to enforcement of Article 40(12). Following formal proceedings under the DSA, AliExpress made a series of commitments that the Commission has made binding, including on access to public data for researchers.[6] Of relevance here is:

> *A commitment to maintaining a dedicated API, allowing eligible researchers to retrieve and download relevant data.*

According to consulted researchers, platforms use these types of terms to create additional approval steps before providing access to the data that researchers request. For example:

> *TikTok's VCE design envisions researchers submitting queries through a two-stage process within a virtual cleanroom—a secure environment specifically designed for conducting research on sensitive data. In the first stage, known as the testing stage, researchers can explore the VCE by running queries limited to a daily sample of up to 5,000 individual records, drawn only from accounts with at least 25,000 followers. Importantly, this data cannot be downloaded and is accessible solely through the VCE interface. In the second stage, researchers submit scripts to query the full set of publicly available data. However, instead of just receiving raw data, researchers need to include their analyses—such as topic modeling or network analysis—directly within the data request script they upload. TikTok reviews these scripts to ensure that only aggregated results—never individual-level data—are shared. Once approved, researchers receive a link via email to download the aggregated results.*[7]

Researchers from civil society organisations have noted that this two-stage process only applies to them and not to academics, even if the latter's access is also provided under Article 40(12).[8]

These types of restrictions on the nature of access provided are not justified by Article 40(12), which simply requires access to data that is *'publicly accessible in their online*

[5] Alvarado Rincón, Denkovski and Romano, Unpacking TikTok's Data Access Illusion (12 June 2025) Tech Policy Press https://www.techpolicy.press/unpacking-tiktoks-data-access-illusion/.
[6] European Commission, Commission makes AliExpress' commitments under the Digital Services Act binding (18 June 2025) https://digital-strategy.ec.europa.eu/en/news/commission-makes-aliexpress-commitments-under-digital-services-act-binding.
[7] Ibid.
[8] Ibid.

interface', *'including, where technically possible, to real-time data'*. The two-stage process described above may also be a significant obstacle to obtaining real-time data for time-sensitive research. Researchers shared with us that they experienced significant delays on responses to these requests, which can render projects obsolete.

TikTok Research ToS III.1. *You must […] not access any data or TikTok content other than through the TikTok Research Tools (including without limitation, no use of scraping or other technical or manual techniques for extraction of content)*
Meta RDUA I.L. *The "Virtual Data Enclave" permits monitored access to data that are not available to the general public. The virtual machine is isolated from the user's physical desktop computer, restricting the user from downloading files or parts of files to their physical computer. The virtual machine is also restricted in its external access, preventing users from emailing, copying, or otherwise moving files outside of the secure environment, either accidentally or intentionally.*
These terms both prevent access to data outside of platform-provided research environments, and prevent the downloading or copying of data from these environments. As the Meta RDUA applies to access to all Restricted Data (see issues about the breadth of this definition above), researchers are prevented from downloading any data from Meta platforms, including that which is publicly available. Researchers have told us that Meta does allow some downloading of data below certain thresholds, but not to an extent that is useful for most researchers: they can (1) view public profiles with a verified badge or 1,000+ followers; (2) download posts from public profiles with a verified badge or 25,000+ followers or posts from public Pages with 15,000+ followers.[9]

YouTube API Developer Policies III.E.1. *You and your API Clients must not, and must not encourage, enable, or require others to: a. download, import, backup, cache, or store copies of YouTube audiovisual content without YouTube's prior written approval, b. make content available for offline playback*
This term likely stems from YouTube's desire to prevent IP infringement of audiovisual works by copying, but it also prevents offline analysis of all content on their platform.

[9] Meta Transparency Center, Meta Content Library and API (Updated 18 August 2025) https://transparency.meta.com/en-gb/researchtools/meta-content-library/.

TikTok Research ToS III.4.e. *you shall […] not undertake any processing activities (including access) in respect of any Personal Data in the TikTok Research Data which relates to an identified or identifiable individual user under the age of 18 outside of the TikTok dedicated environment*
Researchers have noted that it is unclear how TikTok enforces this term, as they already struggle to identify which of their users are under 18.

A. Use restrictions

Closely related to qualification criteria, platforms' terms often impose restrictions on the use that researchers can make of the data. These types of terms range from preventing uses that have not been previously authorised by the platform (a restriction that may in some cases be legitimate considering that platforms are responsible for granting access for the purposes of Article 40(12)), to uses that are in *any way* detrimental to the platform's reputation (which is not justified by Article 40(12)).

The view among researchers consulted was that these terms create a situation in which access to data relies on the goodwill of platforms, which may be withdrawn. This can be seen as inconsistent with the underlying purpose of Article 40, which is to create *obligations* on platforms to share data.

YouTube Research ToS 7.b. *Use Restrictions. You may only use Program Data for research on topics approved by YouTube as part of your application to and acceptance in the Program or that are reasonably related to an approved research topic. Any other research by you using Program Data will require additional written YouTube approval. You may not use or distribute Program Data in, for, or with any applications (e.g. desktop software applications, mobile apps, etc.) developed by you for any purpose other than your own personal use in performance of research permitted under this Program ToS.*
TikTok Research ToS III.3.b *You may only use TikTok Research Data for Research on the topics approved (by TikTok or otherwise in accordance with TikTok's legal obligations) as part of your Research Application.*
These terms don't impose absolute restrictions on use of data for certain purposes, but

they do restrict researchers to using data for the purposes approved as part of their application. These terms fail to guarantee access for the full scope of Article 40(12), and prevent researchers from exploring emerging risks or tangential research directions that they did not foresee in their application. A term that truly reflects the scope of Article 40(12) DSA would be one that enables use of data for any purpose that complies with it.

TikTok Research ToS III.2.d.

When accessing TikTok Research Tools, you will not (or allow others to): […] use the TikTok Research Tools in connection with or for any illegal, unauthorized or otherwise improper purposes, or in any manner which would violate any right of any person, including intellectual property rights, or breach any laws or regulations, or in any manner that is misleading, defamatory, infringing, libelous, disparaging, obscene or otherwise objectionable

The restrictions in this term are wide, vague and undefined – in particular the terms 'unauthorized', 'improper', 'misleading', 'disparaging', 'obscene' and 'objectionable'. In practice, (short of litigation), TikTok is free to interpret these terms as they wish, leaving researchers exposed to arbitrary decisions to refuse or suspend access.

TikTok Developer ToS III.3.d)

When accessing the TikTok Developer Services, you will not (or allow others to): […] use the TikTok Developer Services or TikTok Services in connection with or for any illegal, unauthorized or otherwise improper purposes, or in any manner which would violate any right of any person, including intellectual property rights, or breach any laws or regulations, or in any manner that is misleading, defamatory, infringing, libelous, disparaging, obscene or otherwise objectionable to TikTok;

This term is almost the same as the one in TikTok's Research ToS except for the addition of 'to TikTok' at the end, which significantly expands its scope. What is 'objectionable' can hereby be determined at TikTok's sole discretion.

TikTok Developer ToS III.3.s)

When accessing the TikTok Developer Services, you will not (or allow others to): […] act in a manner that is likely to weaken, damage, or be detrimental to the reputation or goodwill associated with TikTok, the TikTok Services, or the TikTok Developer Services

This term prevents any research that may be critical of TikTok and its systems. Researchers have told us that in practice, TikTok has been very restrictive on the topics it approves, and that it has been common for researchers to refrain from seeking access to TikTok data as their research may be critical of TikTok.

X Developer Agreement XIV.B.

Unless explicitly approved by X in writing, you shall not use, or knowingly display, distribute, or otherwise make X Content, or information derived from X Content, available for purpose of: […] (c) monitoring sensitive events (including but not limited to protests, rallies, or community organizing meetings); or (d) targeting, segmenting, or profiling individuals based on sensitive personal information, including their health (e.g., pregnancy), negative financial status or condition, political affiliation or beliefs, racial or ethnic origin, religious or philosophical affiliation or beliefs, sex life or sexual orientation, trade union membership, X Content relating to any alleged or actual commission of a crime, or any other sensitive categories of personal information prohibited by law.

This type of term may be a problematic restriction for certain types of research involving sociological or behavioural studies. The terms 'monitoring' and 'sensitive events' are vague, and unclear as to whether they capture research into platforms' responses to such events and other behaviour on platforms, which can be directly relevant to systemic risks under Article 34(1). The term 'segmenting' is also unclear, potentially catching classification-type processing, such as classification of users' political beliefs. Finally, the inclusion of content 'relating to any alleged or actual commission of a crime' may be a challenge for research into illegal content on platforms.

The last sentence's wording is also unclear as to whether it is intended to (1) limit use of sensitive data only as prohibited by law, or (2) prohibit any use of sensitive categories of personal information as defined in law.

X Developer Agreement III.A.(k)

You shall not and you shall not attempt to (or allow others to): […] use the X API or X Content to fine-tune or train a foundation or frontier model

This term may restrict researchers' ability to explore or deploy research methods that use LLMs. The term is not specific about the threshold at which a model is considered a 'foundation or frontier model', nor about which types of models are caught (e.g. transformer models, all deep learning models…).

YouTube API Developer Policies III.E.2. *a. Do not aggregate API Data except that you may only aggregate API Data relating to YouTube channels that are under the same content owner as recognized by YouTube pursuant to content licensing agreement(s) between YouTube and such content owner. Such aggregated API Data must only be viewable by that content owner.* *b. Do not aggregate API Data or otherwise use API Data or YouTube API Services to gain insights into YouTube's usage, revenue, or any other aspects of YouTube's business.*
Term a. prevents any aggregation of data, while term b. makes a significant part of Article 40(4) research impossible, especially the term 'usage'. Indeed, Article 40(4) requires access for research into systemic risks pursuant to Article 34(1), which are defined as *'stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services'* (emphasis added).

B. Platform rights to monitor and terminate access

We observed a number of platform terms that grant platforms absolute or near-absolute discretion to monitor researchers' use of their data, and to terminate access with or without cause. To a certain extent, these terms may be a necessary implication of Article 40(12) DSA putting platforms in charge of vetting access, and restricting it to certain purpose-limited research.

But researchers told us that in practice, these discretionary terms can undermine the independence of research projects if they can be enforced arbitrarily. The sudden termination of access can have significant impacts on researchers' resources, staffing and funding. Researchers are understandably concerned about these types of terms, in the absence of clear criteria for termination. Researchers are less likely to make full use of Article 40.12 – and the investment of time and effort that involves – where they believe that their access to data may be revoked at any time, leaving them with incomplete research and unrecoverable sunk costs.

Some researchers have suggested that there should be independent assessments of platforms' concerns before access is suspended, or shortly after if the platform can justify urgency of suspension.

Terms range from giving absolute termination discretion to platforms, to giving them conditional discretion:

YouTube API ToS 24.2 *YouTube may suspend or terminate your access, your API Client(s), or the Agreement at any time, with or without notice – especially in cases of breach, legal order, or potential liability. Upon termination or suspension, developers must immediately stop using all YouTube API Services and delete all API Data and Confidential Information.*
This is the most extreme form of termination right – it is not conditional on any breach or other justification for termination of access.

TikTok Research ToS III.6. *TikTok may monitor your use of the TikTok Research Tools and the Research at any time and without notice conduct an audit of their activities or ask them to confirm that their use of the TikTok Research Tools is compliant with these Research Terms.* X.2. *Termination. We may modify, suspend or terminate your access to, or discontinue the availability of, any parts of the TikTok Research Tools at any time subject to our legal obligations, including, without limitation, where we determine that you have breached these Research Terms. Upon termination of these Research Terms, you must immediately cease use of any and all the TikTok Research Tools and permanently delete all TikTok Research Data.*
This term provides both monitoring and termination rights to TikTok, but it does make termination rights subject to their legal obligations – which should prevent them from terminating access to researchers who meet all of the DSA Article 40(12) conditions. In practice however, researchers may struggle to challenge arbitrary termination.

C. Rate/quota restrictions

Article 40 of the DSA does not expressly allow platforms to impose quotas on researchers' access to data. In practice, we heard from researchers that the imposition, determination, adjustment and suspension of any quotas at platforms' sole discret nooo ion can constitute significant limitations on research. For example:

> *Some of the APIs had very limited quotas so that a researcher might be limited to returning 500 or 1000 observations of data per API call, and are limited to a small number of API calls per day. When studying relatively rare events (e.g., with prevalence rates < 2%), it is probable that API calls might not return any relevant content, which makes it difficult to study the prevalence of harms. This is important*

to flag, because even though harmful or violating incidents might have low prevalence on VLOPSEs, because VLOPSEs have billions of users globally and tens of hundreds of millions of users in the EU, the total number of occurrences of harms can be significant and have significant impact on people and societies[10]

The TikTok API for querying followers and following has a rate limit of '2M records per day by making up to 20,000 calls per day.' Developers 'get a maximum of 100 records in each call' and '[t]he daily quota gets reset at 12 AM UTC.[11] A researcher explained to us that this means they can extract a maximum of 2 millions of followers per day ('if everything works'), which significantly limits the efficiency of research into follower networks or users with large follower bases – Donald Trump, for example, has 15.5 million followers, such that researchers would need more than a week to access all of his followers through API calls.

Some researchers noted that there may be reasonable technical thresholds that can or should apply, as researchers may otherwise run the risk of unintentionally overburdening API services with requests. Hence the issue here may be the 'sole discretion'. Platforms should be able to set rates or quotas for access, but only in a way that is reasonably necessary for the integrity of the service, and predictable for researchers.

Minimum quota guarantees to support robust systemic risk research could be considered to avoid platforms arbitrarily using their quota discretion to constrain research. Researchers have expressed the need to get platforms to articulate what represents wholesale 40(12) data access and the cost of it to them, in order to set sensible limits in terms of cost or engineering load (instead of invoking vague 'security' justifications for arbitrary limits).

Researchers told us that Google guidance on scraping from the Play Store[12] states that queries in the 100 per second range per IP address are unlikely to damage the service or users. This may be a sensible rate for queries in some contexts, although the rate is likely to differ between services. In contrast, one researcher shared with us their experience with TikTok only allowing for about 130 followers in total to be requested per day, which makes any research on follower networks impossible in practice.

[10] European Digital Media Observatory (EDMO), Platform Datasets - Challenges, Insights, and Examples for Researchers under Article 40 of the Digital Services Act (August 2025) p.22 https://edmo.eu/wp-content/uploads/2025/08/EDMO-Report-Platform-Datasets_.pdf.
[11] TikTok for developers, Research API Usage Frequently Asked Questions https://developers.tiktok.com/doc/research-api-faq?enter_method=left_navigation.
[12] Provided to researchers privately: the guidance itself is not public.

TikTok Research ToS III.2.g. *When accessing TikTok Research Tools, you will not (or allow others to): […] use the TikTok Research Tools in a manner that (as determined by TikTok) exceeds reasonable request volume, constitutes excessive or abusive usage*
The lack of definition or criteria for determining 'reasonable request volume', or 'excessive or abusive usage' leaves researchers in the dark as to when their access may reach those thresholds. They are only told that this will be determined by TikTok.

TikTok Research ToS III.3.a. *As part of your Research, you will receive a certain quota assigned by TikTok for accessing TikTok Research Data during your Research. The quota is determined by TikTok at its sole discretion, and TikTok may adjust your quota, suspend, or revoke your access to the TikTok Research Tools at any time, including in the event that Researcher is in breach of the Research Terms, following the completion of your Research, in accordance with TikTok's legal obligations.*
The imposition of a quota at platforms' sole discretion can be a significant limit for research, and one that exceeds the DSA Article 40(5)'s principle of *'data access under proportionate conditions'.* There are no minimum guarantees to support robust systemic risk research. The adjustment of this quota is also said to be possible at any time, and not only in the case of a breach of terms. The phrase 'following the completion of your Research' is unclear – it may mean either (1) that TikTok reserves the right to suspend access at any time *but only* 'following the completion of your Research', or (2) that TikTok reserves the right to suspend access at any time, including in case of breach *and including* 'following the completion of your Research'.

YouTube Research ToS 5.b. *Quota. On request, and with sufficient justification, you will receive sufficient API quota for use as specified by this Program ToS.*
YouTube API ToS 15 *YouTube may set a quota on usage of any YouTube API Services at any time as applied to any specific YouTube API Services user or API Client, category of users or API Clients, or all users or API Clients.*
The Research ToS term here gives less absolute discretion to YouTube to determine the API quota provided, as it should be based on researchers' request and aims to provide 'sufficient' API quota for the relevant research use. What is considered 'sufficient', however, remains at YouTube's discretion – as is what they consider to be 'sufficient justification'. The API ToS term is more absolute, but we expect that in the relevant context the Research ToS term would prevail.

D. Scraping restrictions

Closely related to access method restrictions, but raising slightly different issues, platforms all impose some form of restrictions on scraping. These restrictions apply either to general scraping of their interfaces for data, or verification/QA (Quality Assurance) scraping. It is notable that these restrictions are imposed through access terms under Article 40(12), as opposed to through user terms and conditions. That is, platforms use the Article 40(12) process to obtain a further opportunity to seek to bind researchers to contractual restrictions on scraping, even if they are scraping without being logged in, and therefore would not typically be bound by restrictions platforms' ordinary user terms.

Researchers note that this is a major issue across all platforms. Some told us that they have not signed up to platforms' research programmes specifically to avoid being bound by their terms prohibiting scraping – in short, it makes researchers pick between applying for access via the platform's API, vs. accessing publicly-available data via independent scraping tools, which may reduce the quality of research and prevent the full protection of the DSA.

These restrictions also go against the recent approach taken by the European Commission regarding AliExpress mentioned above. Among the binding commitments, AliExpress makes specifically:

A commitment to enable researchers who meet the criteria set out in Article 40(12) of the Digital Services Act to independently access and use public data to analyse systemic risks via automated means, such as 'data scraping'.

A researcher also noted that researchers can get some of this data through NewsWhip, Meltwater, Bright Initiative, and other platforms (generally for a cost), which rely on scraping. This may be relevant when designing mutually agreeable terms, since scraping is clearly taking place at scale, and it can be argued that the intention of Article 40(12) was to give researchers access to data at a similar scale, but without having to pay for it. The lawfulness of scraping is contested, and it may not be possible or appropriate to fully resolve the issues in the scope of Article 40(12) terms. But researchers were clear in telling us that Article 40(12) access terms are further complicating the picture in ways they find unhelpful.

TikTok Research ToS III.1.c. *You must [...] not access any data or TikTok content other than through the TikTok Research Tools (including without limitation, no use of scraping or other technical or manual techniques for extraction of content)*
This term is a very wide restriction on access to *all* TikTok data, including through scraping and manual access to publicly available data without using the TikTok Research Tools. It makes verification/QA research impossible. It seems even stricter than the restriction in TikTok's Terms of Service preventing use of their platform to *'extract any data or content from the Platform using any automated system or software that is not provided by TikTok or approved in writing by TikTok'*.[13] One researcher did say however that in practice TikTok does not enforce this restriction, given that many projects have used scraping for verification.[14]

[13] TikTok EEA/UK/CH Terms of Service (Last updated August 2025), Term 4.5, https://www.tiktok.com/legal/page/eea/terms-of-service/en.
[14] E.g. AI Forensics, TikTok's Research API: Problems Without Explanations (12 June 2025) https://aiforensics.org/work/tk-api.

YouTube API Developer Policies III.E.6. *You and your API Clients must not, and must not encourage, enable, or require others to, directly or indirectly, scrape YouTube Applications or Google Applications, or obtain scraped YouTube data or content.*
This term seems to restrict all scraping of YouTube data, and researchers have told us that how this applies to them is a priority area for clarification.

E. Onward sharing restrictions

All the terms we analysed impose restrictions on onward sharing of data with third parties. Researchers note that this is generally an issue for compliance-focused research, if results and underlying data cannot be shared with regulatory authorities (European Commission and DSCs). This also hinders reproduction, replication and verification of research (including when using 'data rehydration' methods). Researchers noted that when alternative methods of sharing social media data are used, the research tends to suffer from substantial data loss, increasing the importance of being able to legitimately share data obtained from platforms through Article 40(12).[15]

Researchers agree that onward sharing should only be for legitimate purposes related to the research they are carrying out. They also agree that *some* types of data may rarely be appropriate to share (e.g. children's data or sensitive data which is not fully public). The real problem therefore is the vagueness of restrictions on sharing and the consequences of their being enforced arbitrarily or indiscriminately. Some researchers felt that platforms may be reticent to permit sharing due to their perception of the research community's data protection standards being weak. They expressed a need for (1) clarification and communication of suitable standards[16] and (2) capacity building among researchers to improve practices, which could alleviate platforms' concerns.

Some sharing restrictions are also arguably unclear or excessively wide, sometimes seeming to extend to any derivative of the original data, i.e. including research outputs. Researchers have told us that in practice, these terms have not prevented researchers from publishing work but have limited cross-researcher collaborations.

[15] Assenmacher and others, The End of the Rehydration Era The Problem of Sharing Harmful Twitter Research Data (2020) Association for the Advancement of Artificial Intelligence https://workshop-proceedings.icwsm.org/pdf/2023_56.pdf.
[16] For example, those developed by The George Washington University Institute for Data, Democracy & Politics, Ethical Use of Pervasive Data for Research: Actions for Academia and Civil Society (July 2025) https://iddp.gwu.edu/sites/g/files/zaxdzs5791/files/2025-07/iddp_next_steps_pervasive_data_ethics_july_2025.pdf.

TikTok Research ToS IV. *you agree not to disclose, copy, reproduce, share, sell, or otherwise transfer to any third party any TikTok Research Data-or any data derived or aggregated from TikTok Research Data*
This term is the most absolute, extending to any analysis or research output derived from TikTok data.

X Developer Agreement III.H. *You may not disclose, reproduce, license, or otherwise distribute the Licensed Material (including any derivatives thereof) that you retrieve through the X API to any person or entity outside the persons specified within your approved application unless (i) the information is disclosed to the Digital Services Coordinator or other party specifically permitted by the DSA pursuant to the "vetted researcher" status and procedures described in Article 40, or (ii) disclosure is required by law.*
While this term makes an exception for disclosure of information to DSCs under Article 40(4), it prevents any sharing, including of derivatives, with any third party outside those specified in approved applications.

YouTube Research ToS 7.a. *You will not disclose, reproduce, sell, license or otherwise transfer to any third party, in part or in whole, any Program Data.*
This term is more sensibly constrained to data obtained through the YouTube API services as part of the research program, but still does not discriminate between sensitive and non-sensitive data.

Meta RDUA VI.F. *Restrictions on release of statistics or other content derived from the Restricted Data*
This term imposes potentially significant restrictions on the release of analyses of data, and on the replication of research.

F. Data management obligations

All the terms we analysed impose obligations on researchers to adopt certain data management practices. Many of these are sensible obligations in line with data protection law, but some appear to be problematic or excessive for many researchers. Article 40(8)(d) only requires researchers to demonstrate that they are *'capable of fulfilling the specific data security and confidentiality requirements corresponding to each request and to protect personal data'*. This is an objective standard for each request, such that 'one-size-fits-all' obligations – especially those which unduly constrain research – are not justified by Article 40(12) or the GDPR.

All the researchers we spoke to share concerns about these obligations, but some have also voiced the other concern that some researchers do indeed lack data management skills and understanding of the importance of (e.g.) data deletion. As mentioned, they note the need to build data protection capacity among platform researchers.

i. Data refresh and deletion

Based on feedback from researchers, the most problematic obligations are data refresh and deletion requirements, which prevent researchers from backing up their findings, from conducting research over a long period of time, and from conducting longitudinal research.

TikTok Research ToS III.3.e.
Where you are able to access or download Personal Data through the TikTok Research Tools, you agree to regularly refresh TikTok Research Data at least every thirty (30) days, and delete data that is not available from the TikTok Research Tools at the time of each refresh. TikTok Research Data shall not be kept by you for longer than is necessary for Research approved as part of your Research Application. You agree to provide TikTok with written certification of data deletion upon TikTok's request.
This seems highly burdensome for research that can be conducted over many months or years. It is also unclear what researchers should do about analysis and results derived from data that is no longer in the TikTok Research Tools at the time of a refresh.

X Developer Agreement IV.
A. Updates. X may update, modify or discontinue any features or function of the Licensed Material, in whole or in part, from time to time (in each instance, an "Update"). You shall implement and use the most current version of the Licensed Material and make any changes to your Services that are required as a result of the Update, at your sole expense.

Updates may adversely affect the way your Services access or communicate with the X API or display X Content. X will not be liable for damages of any sort that result from any Update.

B. Removals. If X Content is deleted, gains protected status, or is otherwise suspended, withheld, modified, or removed from the X Applications (including removal of location information), you will make all reasonable efforts to delete or modify that X Content (as applicable) as soon as possible, and in any case within twenty four (24) hours after a written request to do so by X or by an X user with regard to its X Content unless prohibited by law or regulation and with the express written permission of X.

This term implies an ability of researchers to constantly monitor the status of the data they have accessed, collected and analysed. This is highly burdensome, and if enforced may entirely disrupt a research project.

YouTube Research ToS 7.c

You agree to regularly refresh Program Data as specified by the Developer API ToS (i.e. every 30 days) until such time as you need the Program Data to be fixed as to a point in time for the purposes of finalizing your analysis and drawing of conclusions with respect to your Researcher Publications.

This term caveats the refresh obligation for analysis and publication purposes. It is unclear how it applies, however, to research carried out over months or years to identify trends or evolutions.

LinkedIn Research Terms 4.2

you will permanently delete (in ten (10) days or less): (a) all Stored Research Data upon LinkedIn's reasonable written request (email acceptable) […] (d) all Stored Research Data upon termination of these LRT Terms or the relevant Research Project (except Stored Research Data incorporated in Research Work Product that is still available to Research End Users).

It is unclear what a 'reasonable written request' would be in this context – in any case, a researcher would likely struggle to challenge a request from LinkedIn without their access being simply suspended.

ii. Data management plans or impact assessments

Some platforms require researchers to put in place onerous data management plans or to carry out data protection impact assessments in circumstances where data protection law would not require them, creating additional disproportionate costs for research projects.

TikTok Research ToS I.4. & Sch C *Minimum Security Measures: means the technical and organizational security measures with which you as the Eligible Researcher must comply, as set out in Schedule C.*
The measures in Schedule C are likely to be overly burdensome for independent researchers or NGOs (and some academic researchers) – they include *'Appliances for the monitoring of temperature and humidity in data centers'*, using *'a combination of full, differential, and cumulative backups to ensure data integrity and timely restoration for core data', or 'redundant power supply units'*.

TikTok Compliance Certification[17] *We have conducted a data protection or privacy impact assessment (which our organisation's DPO, person responsible for data protection compliance or equivalent has advised on) for our proposed data usage and management plan (e.g. the Consortium of European Social Science Data Archives offers a Data Management Expert Guide) submitted together with the research proposal.*
This is a statement that we understand researchers must make before receiving access to TikTok data. It may be overly onerous for researchers to be required to conduct a data protection or privacy impact assessment before receiving access to publicly accessible data, notably because their processing may not pose a high risk to data subjects and therefore would not be required under GDPR Article 35. In practice however, researchers have told us that they aren't aware of any applications that did submit any assessment or data management plan, and yet all received access.

iii. Adherence to data security policies and guidelines

Some platforms require researchers to adhere to certain external policies or guidelines that may be unsuitable for the type of research they are undertaking, or that they do not have the resources or capacity to comply with.

[17] https://www.tiktok.com/legal/page/global/compliance-certification/en.

Meta RDUA VI.F. *the Institution agrees […] To avoid inadvertent disclosure of Private Persons by being knowledgeable about what factors constitute disclosure risk and by using disclosure risk guidelines, such as but not limited to, the following guidelines [footnote to the National Center for Health Statistics checklist, NCHS Disclosure Potential Checklist at http:// http://www.cdc.gov/nchs/data/nchs_microdata_release_policy_4-02A.pdf; and FCSM Statistical Policy Working Paper 22 (Second Version, 2005) at http://www.hhs.gov/sites/default/files/spwp22.pdf] in the release of statistics or other content derived from the Restricted Data.*
The guidelines cited were developed for the protection of health statistics, which are particularly sensitive, and may therefore be excessive for social science research using public data.
Meta RDUA VI.F. *the Institution agrees […] That use of the Restricted Data will be consistent with the Institution's policies regarding scientific integrity and human subjects research.*
Policies on 'human subjects research' may be too onerous for social science researchers using public data, as these types of policies are usually intended to protect individuals in the context of 'live studies' directly on human subjects, rather than retrospective research that uses personal data.

G. Procedural obligations

A number of platforms' terms impose procedural obligations on researchers once they are granted access to data, usually for purposes of monitoring their compliance with the terms of access, or in case the conditions of access need to change to align with changes in researchers' circumstances. Some of these may be legitimate and proportionate obligations for ensuring that the researchers' access continues to comply with the requirements of Article 40(12). Others appear to be excessive and are not justified by Article 40(12) purposes, for example requiring researchers to implement resource-intensive monitoring and reporting systems.

Meta RDUA VI.J. & K. *the Institution agrees:* *J. To provide annual reports to ICPSR […] which include:* *1. A copy of the annual IRB [Institutional Review Board] approval for the project described in the Research Description; 2. A listing of public presentations at professional meetings using results based on the Restricted Data or Derivatives or analyses thereof; 3. A listing of papers accepted for publication using the Restricted Data, or Derivatives or analyses thereof, with complete citations; 4. A listing of Research Staff using the Restricted Data, or Derivatives or analyses thereof, for dissertations or theses, the titles of these papers, and the date of completion; and 5. Update on any change in scope of the project as described in the Research Description.* *K. To notify ICPSR of a change in institutional affiliation of the Investigator, a change in institutional affiliation of any Research Staff, or the addition or removal of Research Staff on the research project. Notification must be in writing and must be received by ICPSR at least six (6) weeks prior to the last day of employment with Institution. Notification of the addition or removal of Research Staff on the research project shall be provided to ICPSR as soon as reasonably possible. Investigator's separation from Institution terminates this Agreement.*
These terms impose potentially onerous procedural obligations for which researchers may have to put a monitoring and reporting system in place. These requirements do not follow from Article 40(12). While they may be suitable to academic researchers, civil society researchers are unlikely to be able to comply with them.

H. Publication-related obligations and rights

All platforms impose certain terms related to the publication of research outputs. While none are required under Article 40(12), researchers have noted that some terms of this nature may be legitimate:

i. Use of brand names

Some platforms reserve the right to refuse permission for researchers to mention their brand name as the source of data. This could be seen as creating a 'chilling effect' on researchers criticising a platform's practices, and may affect the credibility of their research as it prevents transparency and replicability.

LinkedIn Research Terms 7.3 *Any marketing, advertising, or promotional announcement, material, press release, blog, or any other communication to third parties relating to the Research Tools, Research Data, or your Research Project that includes any of the other party's Brand Features is subject to that party's prior written approval (email acceptable).*
TikTok Research ToS III.3.g. *You may not use the TikTok name, logo, trademarks, service marks, domain names, or other distinctive brand features of TikTok without TikTok's prior written approval.*

ii. Advance notice requirements

Many platforms require researchers to submit any outputs from their research for review before publication. Researchers consider this an obstacle to independence, as it may be used by platforms to stop publication of research that is critical of them. This could be achieved by the removal of data access or by platforms threatening other action (e.g. actions in defamation) which would put researchers in the difficult position of quantifying and managing legal risks prior to publication.

Advance notice and pre-publication review are not obligations provided by Article 40(12), and cannot be justified by platforms' data protection obligations. Some platforms caveat these advance notice requirements by stating that their sole purpose is to verify that they do not pose a risk of identifying individuals, but the procedure itself can become an obstacle to timely publication. Researchers note, however, that it may be legitimate in some circumstances for platforms to be given a right to review planned disclosures, for example in case of research into foreign interference, which may raise national security concerns which require prospective management.

Ultimately, whilst researchers may wish to notify platforms of publication in advance – and it may even be in their interests to do so – it is not justified by the DSA or GDPR for this to be a requirement imposed on researchers in all cases.

Meta RDUA I.e. & Attachment A (Data Security Plan) *You must submit all statistical outputs/results from the VDE to ICPSR for a disclosure review prior to sharing or giving such outputs to unauthorized persons. You also agree to revise or alter such outputs as required by ICPSR in order to minimize disclosure risk prior to ICPSR approving these outputs for dissemination to unauthorized persons. [Note: we assume that 'Confidential Data' in Attachment A is the same defined term as 'Restricted Data' in the Agreement, as it is not defined elsewhere.]*
These advance notice requirements can be a significant burden for researchers, both substantively (they give the platform rights to object to disclosures) and procedurally (they constitute an additional administrative step before publication).

TikTok Research ToS III.3.f. *You agree to provide TikTok with a copy of any publications pertaining to or containing the results and findings of the Research outputs, and any supporting information, at least seven (7) days before publication primarily to identify any user private Personal Data that may need to be removed prior to publication or disclosure.*
This term gives TikTok a pre-publication right of scrutiny that is not limited to identifying personal data that needs redaction (through the use of the word 'primarily').

YouTube Research ToS 6.d *You agree to use reasonable efforts to provide YouTube with a copy of each Researcher Publication at least seven (7) days before its publication. This is meant solely as a courtesy notice to YouTube. YouTube will not have editorial discretion or input in any Researcher Publication.*
This is a lighter version of an advance notice requirement, preventing any editorial discretion or input.

iii. Platforms' rights to use research

Some of the terms we analysed involve the reservation of rights to use the researchers' research projects and outputs for internal or external purposes. While these types of terms are not necessarily obstacles to research, they could cause confidentiality problems for researchers who carry out sensitive research, or ethical problems for researchers who carry out their research in the public interest and consider that their research should not be a source of profit for platforms they seek to hold to account.

LinkedIn Research Terms 7.4 *You acknowledge that LinkedIn may support other researchers with research projects that may be similar to or competitive with your Research Project and LinkedIn is not, in any way, restricted from: (a) granting such researchers access to any Research Tool or Research Data; or (b) disclosing information relating to your Research Project to any third party. You further acknowledge that LinkedIn is not obligated (under these Terms or any applicable law) to treat any information regarding your Research Project (including your Research Work Product) as confidential.*
This term raises a risk of research ideas and projects being divulged, copied or spoiled, and researchers have told us that it may also pose a security risk. In a complex social and political climate, there may be risks of researchers being threatened or their research tampered with if their research is considered to follow a particular political line.

YouTube Research ToS 6.c *After you publish a Researcher Publication, you agree YouTube, its parent company, and its affiliates will have free and unlimited access to and use of the Researcher Publication and all related Program Derived Research. This use includes, without limitation, the right to: i. for internal review, presentation, and training purposes, make, distribute, and use copies of the Researcher Publication and all Program Derived Research; and ii. for marketing, training, and presentation purposes, use and distribute reasonable excerpts from the Researcher Publication and all Program Derived Research.*
This term grants YouTube sweeping, royalty-free rights to use researcher outputs for internal purposes, and 'reasonable excerpts' for marketing purposes. This may contradict certain academic publication terms, and some researchers have noted that companies should not be allowed to use researchers' work without proper remuneration.

I. Indemnity and Liability

All platforms, except for LinkedIn, include an indemnity clause in their terms. Some are all-encompassing, while others only arise from breaches of the applicable terms. Researchers' liability is not limited in any of these cases. The risk of these terms being enforced could be significant, especially for researchers with more limited resources or thinner institutional protections. That is especially the case when indemnification obligations arise from a wide range of indirect causes of action, providing extensive scope for - potentially arbitrary – enforcement by platforms. They may also contradict certain insurance requirements.

Researchers have told us that platforms have previously sued or attempted to sue researchers under these types of terms. Some consider that because the research is required to be non-commercial, and access is required by law, they should not have any liability towards platforms, regardless of the impact of their research.

Even where the effect or enforceability of these indemnity and liability terms may be questionable, their inclusion in Article 40(12) terms presents a problem for researchers, who have to undertake legal analysis or obtain advice in each case in order to assess and manage the risk of their being (sought to be) enforced.

Meta RDUA VII.C. *Institution agrees, to the extent not prohibited under applicable law, to indemnify the Regents of the University of Michigan from any or all claims, losses, causes of action, judgments, damages, and expenses arising from Investigator's, Research Staff's, and/or Institution's use of the Restricted Data, except to the extent and in proportion such liability or damages arose from the negligence of the Regents of the University of Michigan. Nothing herein shall be construed as a waiver of any immunities and protections available to Institution under applicable law.*
The indemnity here arises from any cause of action related to the researchers' use of the data, which can be interpreted extremely broadly and extend in time beyond the conclusion of the research. Researchers' liability is unlimited.

TikTok Research DSA 6 *6.1 Researcher shall indemnify and keep indemnified TikTok Group and its affiliates in respect of all costs (including legal costs), claims, demands, actions, settlements, ex-gratia payments, compensation, fines, charges, procedures, expenses, losses and*

damages suffered or incurred by, awarded against or agreed to be paid by, TikTok Group and its affiliates arising from or in connection with any actual or alleged breach by Researcher of its obligations under this DSA or Applicable Data Protection Law. *6.2 Researcher's liability for the indemnity provided in this Clause 6, shall not be limited or excluded (including by any provision in the Agreement).*
<u>TikTok Developer ToS VIII.</u> *To the maximum extent permitted by applicable law, you agree to hold harmless and indemnify TikTok, its subsidiaries, affiliates, licensors, licensees, assigns and successors, and each of their officers, directors, employee, agents, advisors and shareholders from and against any third-party claim, suit or action including any liability, losses, damages (actual and/or consequential), expenses, litigation costs and reasonable attorney fees, of every kind and nature arising from or in any way related to (a) actual or alleged breach of your obligations under these Developer Terms; (b) your use of TikTok Developer Services; (c) any Developer Content or data derived therefrom; or (d) the performance, promotion, sale or distribution of the Application. TikTok shall use reasonable endeavours to provide you with written notice of any such claim, suit, or action.*
While the Research DSA indemnity only arises from a breach of this DSA or applicable data protection law, the indemnity in the Developer ToS arises from any cause of action related to researchers' use of the TikTok Developer Services, or any content or data derived therefrom. This can similarly be interpreted extremely broadly and extend in time beyond the conclusion of the research.

Conclusion

Our work has shown that these platforms are imposing terms on researchers when they seek access to data under Article 40(12) DSA which:

> (i) constrain research, whether by preventing it entirely, delaying it, or making it more expensive and difficult that it need be; and
>
> (ii) are **not** justified by the terms of the DSA, GDPR or any other legislation.

This is confirmed by our analysis of those terms, in-depth engagement with researchers, and case studies which show the impact of these terms on research in practice. Our analysis and consultation shows a broad range of ways in which platforms' terms can constrain research. In some cases the impact can be very severe, for example preventing researchers from replicating their findings.

Not all platforms' terms are the same. This variance itself may impose further costs on researchers, who could find themselves having to analyse Article 40(12) terms on a platform-by-platform basis, and take case-by-case decisions on their risk appetite for engaging.

It is for researchers and platforms to pursue a way forward on this issue. However we have also been asked to draft a 'model' data sharing agreement, which may be useful in guiding parties on what terms are genuinely required by the DSA and GDPR, and how agreements may be drafted in ways less likely to constrain research. This model data sharing agreement is being published by Mozilla Foundation alongside this report.

Questions about the report?

Contact: press@mozillafoundation.org

Mozilla Foundation