

Navigating Data Access for Social Media Monitoring: A Practical Guide



EU SEE

SUPPORTING
AN ENABLING ENVIRONMENT
FOR CIVIL SOCIETY

Hivos
people unlimited



DEMOCRACY
REPORTING
INTERNATIONAL

Index

- 3 Introduction**
- 5 Glossary**
- 8 Access to platform data as an essential tool for researchers: Where do we stand?**
- 10 Main methods for accessing social media data**
 - 10 Platforms' protocols
 - 13 Social Media Listening Tools
 - 15 Manual data collection
 - 15 Other alternative ways to circumvent data access restrictions
 - 15 Web scraping
 - 16 Data Donation
- 17 Types of accessible data**
- 19 Key limitations**
- 20 Ethical considerations in accessing and analysing social media data**
- 23 Further Guidance to Access Platform Protocols**
 - 23 Access to platforms protocols with project-based applications requirements
 - 23 Access to Meta Content Library
 - 24 Access to TikTok Platform Protocols
 - 25 Access to Reddit API
 - 26 Access to platform protocols requiring only account creation
 - 26 Access to platform protocols that require a paid subscription

Introduction

The data access resource offers a practical guide to navigating the complex ecosystem of data access on digital platforms, with a focus on social media monitoring. It is designed to help researchers and civil society organisations understand why access to social media data is essential when monitoring social media, explore the main methods for collecting it, learn about the types of data that can be accessed, and reflect on key limitations and ethical considerations. Since there will always be limits to data access, this guidebook presents the full landscape to help researchers understand what is possible, recognise the constraints, and select the most suitable approach for their research needs. Ultimately, understanding social media data access is not only a technical matter but a democratic imperative: one that enables transparency, platform accountability, and the protection of democratic values.

With access to social media data, monitoring can generate concrete insights. The following examples show how data access has enabled the detection of harmful content, such as disinformation, hate speech and online gender-based violence.

Table 1: From Data Access to Insights: Examples of Social Media Monitoring

Case	Focus	Data accessed	Insights
<u>Sri Lanka: Election Monitoring (2019-2020)</u>	Monitored Facebook during parliamentary elections, capturing the amplification of both hate and positive narratives post-2019 Easter attacks.	Facebook page and group posts	Showed negative and positive messaging in Facebook posts, including efforts to counter false information and hate speech.
<u>Tunisia, Jordan, and Lebanon: Democratic processes monitoring (2021-2023)</u>	Monitored online discourse on Facebook and X during 2022 democratic processes in Tunisia, Jordan, and Lebanon, documenting gendered attacks against women candidates, religious hate campaigns in Lebanon, and coordinated disinformation in Tunisia.	Facebook page and group posts, as well as X posts (tweets)	Uncovered regional trends and tactics used by different actors to spread hate speech and disinformation.
<u>Brazil: Election Monitoring (2023-2024)</u>	Tracked online narratives on X, YouTube, and Instagram during Brazil's 2024 elections, revealing gendered attacks and institutional disinformation threats.	X posts (tweets), YouTube videos, and Instagram posts	Identified online violence targeting women, aimed at delegitimising female political participation, as well as disinformation narratives that eroded trust in institutions.

An important first step in addressing the overall data access landscape is to distinguish between public and non-public data. While there is no consensus on the definition, publicly available data typically refers to content that is visible to any user with an account on the platform, such as posts, comments, reactions, views, and some types of metadata, including timestamps indicating when posts were created. In contrast, non-public data is not visible through the platform interface for regular users and, in most cases, is not accessible at all. If accessible, such data can only be obtained under specific legal, technical, and ethical conditions. Examples include content recommendation data (such as information used to personalise social media feeds), content protected by privacy settings (e.g., private messages, private profiles), and internal engagement metrics (e.g., time spent viewing a post).

In this resource, we focus on publicly available data because it is more easily accessible, supports transparent and reproducible methodologies, and aligns with ethical research standards without requiring privileged access.

Glossary

Boolean search rules

Logical operators (such as AND, OR, NOT, and quotation marks) used in social media monitoring to search for specific content. They help filter and refine results to find posts related to certain topics, events, or names. For example, a search request like “elections AND climate change” will retrieve posts that mention both terms.

CSV (Comma-Separated Values)

A simple file format that stores information in a table, similar to a spreadsheet. Each row is a line of data, and the values are separated by commas. In social media monitoring, CSV files are often used to download or share lists of posts, comments, or accounts, which can then be opened in Excel, Python or R.

Data access

The ability to obtain information from a source, such as a social media platform like Facebook. In social media monitoring, data access means being able to collect posts, comments, or account information using different tools.

Digital Platforms

Online social media services where people interact, share, and access information. Examples include Facebook, Instagram, or TikTok. In social media monitoring, digital platforms are the main sources of data, since they host the posts, comments, and accounts being analysed.

Digital Services Act (DSA)

A European Union law that sets rules for digital platforms, especially large social media platforms, to make the digital space safer and more transparent. It introduces obligations on how platforms handle illegal content, protect users' rights, and provide researchers with access to data for accountability.

Digital threats

Risks and harmful activities that occur online, such as disinformation, hate speech, harassment, or cyberattacks. In social media monitoring, digital threats refer to content or behaviours on platforms that can harm individuals, groups, or democratic processes.

JSON (JavaScript Object Notation)

A file format used to store and share data in a structured way. Unlike CSV, which organises information in a simple table (rows and columns), JSON organises data with labels (keys) and values, making it better for complex information. For example, a JSON file can include details of a social media post such as the author, date, text, likes, and comments, all grouped together.

Online Safety Act (OSA)

A law in the United Kingdom that sets rules for how online platforms, including social media, must protect users from harmful content. It requires platforms to take steps against risks such as disinformation, hate speech, and online abuse, while also ensuring transparency and accountability.

Platform Data

Information generated and stored by social media platforms, such as posts, comments, likes, shares, or user profiles. In social media monitoring, platform data is the main source of evidence, since it shows what content is being published, shared, and interacted with on platforms like Facebook, Instagram, or TikTok.

Platform documentation

Official guides and reference materials provided by social media platforms to explain how their tools and systems work. This includes instructions on using APIs, data access rules, or safety policies. In social media monitoring, platform documentation is key to understanding what data can be accessed, under which conditions, and how to use it correctly.

Platform interfaces

The different ways in which users and tools can interact with a social media platform. This includes the regular user interface (what people see when they log into Facebook, Instagram, or TikTok) and technical interfaces like APIs that allow researchers to access data. In social media monitoring, platform interfaces determine how information can be collected and analysed.

Sentiment analysis

A method used to identify whether the tone of a text is positive, negative, or neutral. In social media monitoring, sentiment analysis helps to understand how people feel about a specific topic, event, or public figure by analysing large numbers of posts or comments.

Social media monitoring

The process of systematically collecting and analysing content from social media platforms, such as posts, comments, hashtags, or accounts, to track conversations, identify trends, and detect risks or opportunities. It is widely used by researchers and civil society organisations to study issues like disinformation, hate speech, or public debate dynamics.

VLOPs and VLOSEs (Very Large Online Platforms and Very Large Online Search Engines)

Categories defined in the EU Digital Services Act (DSA) for the biggest platforms (such as Facebook, Instagram, TikTok) and search engines (such as Google). They have more than 45 million users in the EU and therefore carry extra responsibilities, including stronger transparency requirements, stricter risk assessments, and obligations to give researchers access to data.

Access to platform data as an essential tool for researchers: Where do we stand?

Access to social media data is essential to ensure transparency, hold social media platforms accountable and protect democratic values in the digital age. From election monitoring and disinformation analysis to understanding online gender-based violence and hate speech, researchers and civil society actors rely on data to document and respond to emerging digital threats. The Global Digital Compact (GDC), adopted by the United Nations in 2024, underscores this need by explicitly calling on digital platforms to grant data access to researchers, under appropriate safeguards, as part of their broader responsibility to uphold human rights and support public-interest oversight. As stated in the GDC, states and stakeholders should:

“Call on social media platforms to provide researchers access to data, with safeguards for user privacy, to ensure transparency and accountability to build an evidence base on how to address mis - and disinformation and hate speech that can inform government and industry policies, standards and best practices (SDGs 9, 16 & 17)” — [\(GLOBAL DIGITAL COMPACT, REV. 2, JUNE 2024, PARA. 35\(B\)\)](#).

The GDC recognizes that meaningful transparency is not possible without independent access to platform data and that such access is a foundational element of a safe, rights-respecting, and accountable digital environment.

Although these guidelines are non-binding, they reflect a growing consensus on the need for meaningful transparency and public-interest oversight in digital spaces. In some regions, such as the European Union, this principle has already been translated into enforceable obligations. Under [the Digital Services Act \(DSA\)](#), platforms designated as Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), such as Instagram, Facebook, TikTok, X, YouTube, among others, are now legally required to provide researchers with access to publicly available data as well as non-public data. Additionally, the [United Kingdom has adopted the Online Safety Act \(OSA\)](#), which places new duties on tech companies to protect users and includes provisions for data access. While not identical to the DSA or the UK's OSA, several countries such as India, Brazil, and Chile have also developed regulatory frameworks to govern the digital space and establish rules for how digital platforms operate.

These developments signal a normative shift: access to platform data is increasingly seen as a precondition for accountability in digital governance frameworks.

Main methods for accessing social media data

There is no clear, coherent, or unified pathway to access social media data, as each platform sets its own rules and procedures, often without consistency. Instead, those who need this data must rely on a mix of tools, each with its own rules, limitations, and technical barriers. This resource outlines some of the key methods currently available to help navigate this fragmented and inconsistent data landscape.

Platforms' protocols

Platform protocols are technical and procedural rules that define how computer systems, applications or tools interact with social media platforms to securely and efficiently access data. These rules are used by researchers and developers to collect information, usually through services provided by the platform itself, such as application programming interfaces (APIs), platform user interfaces, or secure research environments. Each of these options comes with trade-offs in terms of accessibility, complexity, and depth of access.

The following are among the most common protocols available:

Protocol	Definition	Data accessibility	Need for Technical/Coding Skills
API (Application Programming Interface)	A structured interface that allows automated access to data using code.	Medium: Platforms have full control over what data they share through their APIs, which means only select types of data are accessible, often within strict time and usage limits.	Technical knowledge and coding skills are required for interaction with APIs and interpreting documentation.
Platform User Interfaces	Web-based interfaces provided by platforms that allow users to access and explore data without requiring coding skills (e.g. Ad Libraries, Meta Content Library)	Medium: Researchers often face limitations when downloading large datasets.	No technical knowledge or coding skills are required.
Secure Research Environments	Secure, platform-hosted environments that allow researchers to access and view data under controlled conditions, often with restrictions on downloading, copying, or external sharing (e.g. TikTok's Virtual Computing Environments (VCEs)).	Medium to Low: Access to data is tightly controlled, often requiring prior approval of scripts or datasets. Data cannot be downloaded or exported, and researchers must work within a closed system with limited tools.	As with APIs, technical knowledge and coding skills are required.

We have included below the relevant links to each platform’s documentation covering data accessibility and research procedures, ordered from the least to the most complex application process.

It is important to monitor potential updates to the application process, as requirements may evolve over time.

Platform	Platform protocols	Documentation	Application process
YouTube	▶ YouTube Data API v3	YouTube Data API Google for Developers	▶ A Google account is required
Telegram	▶ Telegram API	Telegram APIs	▶ A Telegram account is required (mainly designed for commercial use)
Bluesky	▶ Bluesky API	Bluesky Documentation Bluesky	▶ A Bluesky account is required
LinkedIn	▶ LinkedIn API	Extracting LinkedIn Search Results via API: Best Practices a	▶ A LinkedIn account is required
Reddit	▶ Reddit Research API	Developer Platform & Accessing Reddit Data - Reddit Help	▶ Project-based application ▶ More on the application process: reddit4researchers
META (Facebook, Instagram & Threads)	▶ Meta Content Library (platform user interface) ▶ Meta Content Library API	Meta Content Library and API Transparency Centre	▶ Project-based application ▶ Authorisation process required
TikTok	▶ TikTok Research API (for academic researchers) ▶ Virtual Computing Environment (for non-profit researchers)	Research API TikTok for Developers	▶ Project-based application ▶ Authorisation process required (currently, TikTok tools are available only to researchers based in the US, EU, UK and Switzerland).
X	▶ X API	Use Cases, Tutorials, & Documentation Twitter Developer Platform	▶ Subscription required (often high costs)

Social Media Listening Tools

As access to platform-provided data protocols is often limited by data volume restrictions, the need for technical expertise or regional availability, researchers may turn to commercial social media listening tools. Social media listening tools are powerful analytical tools that provide historical access to platform data. Research can be conducted by topic (primarily through keyword searches) or by target (by selecting specific accounts or users to monitor).

These services collect publicly available social media data through partnerships, APIs, or web monitoring, and offer dashboards and built-in analytics features. They are generally more user-friendly and accessible for individuals without coding skills.

Among their key advantages are comprehensive data extraction across major platforms, such as Facebook, X, Instagram, YouTube, VKontakte, Reddit, Tumblr, and TikTok, as well as other sources like blogs, podcasts, and email newsletters. These tools often allow data export in structured formats (e.g., JSON and CSV) and support advanced filtering and boolean search rules, a way of combining keywords with operators like AND, OR, and NOT to refine results. However, access typically requires a high-cost subscription and platform coverage can also vary, depending on the tool's partnerships and licensing arrangements. In addition, researchers should vet the tools' built-in analytics features, such as sentiment analysis, as these may not always be accurate.

When using social media listening tools, researchers should be aware of potential privacy and data protection implications. Depending on the country, these tools might conflict with local data protection laws. It's important to review and ensure compliance with relevant regulations before using such services. Below are some of the most widely used:

SMM Listening Tool	Pro	Cons
<u>BrandWatch</u>	<ul style="list-style-type: none"> ▶ Powerful real-time monitoring and customizable dashboards. ▶ Data access to blogs and media outlets is included. ▶ Provides in-depth analytics features (e.g. sentiment analysis, engagement metrics, advanced filtering options, data visualisation). 	<ul style="list-style-type: none"> ▶ No public pricing as plans are customized. Estimated cost between \$800-\$3,000/month
<u>SentiOne</u>	<ul style="list-style-type: none"> ▶ Intuitive and easy to use. ▶ Data access to blogs, media outlets, review sites is included. ▶ Provides in-depth analytics features, such as sentiment analysis and data visualisation. 	<ul style="list-style-type: none"> ▶ Pricing starts at ~ \$350/month (Team plan) ▶ Data visualisation options are limited.
<u>Inoreader</u>	<ul style="list-style-type: none"> ▶ Affordable pricing: Pro plan at less than \$9 per month (billed annually). ▶ Data access to blogs, podcasts, and email newsletters is included. ▶ Enables shared dashboards, folders, and tags. It also integrates with Slack and Microsoft Teams. 	<ul style="list-style-type: none"> ▶ The tool focuses on content aggregation and does not offer in-depth analytics or detailed engagement metrics. ▶ It does not cover all social media networks, potentially missing out on discussions occurring elsewhere.

Manual data collection

If platform protocols or social media listening tools do not align with your research purposes and needs, or if you simply wish to complement them, you always have the option to collect the data yourself. Manual data collection involves systematically navigating the platform to identify and record relevant content by hand, such as posts, comments, or profiles, often using spreadsheets or basic databases. While this method is time-consuming and prone to human error, it may be the only viable solution when data access is restricted or unavailable.

Some examples of DRI's research based on manually collected data:

- ▶ [Scroll, Like, Deceive: Murky Political Accounts on TikTok before the German 2025 Elections | Democracy Reporting International](#)
- ▶ [Filtered for You: Algorithmic Bias on TikTok and Instagram in Germany | Democracy Reporting International](#)

Other alternative ways to circumvent data access restrictions

If platform protocols or social media listening tools do not provide access to the data needed to address your research purposes, or if manual data collection proves insufficient or too costly in terms of time and labour, there are alternative ways to overcome data access restrictions. One such method is web scraping, which involves using automated tools or scripts to collect data that are publicly available on websites or platforms. Another option is data donation, a method of data access and collection in which researchers collaborate with individuals who voluntarily share the digital traces they have left behind for research purposes.

Web scraping

Scraping can be an effective way to extract structured information from social media at scale, enabling the collection of both user and content data, such

as number of followers, followings, likes, comments, and shares. However, it requires a certain level of technical expertise, as automation is primarily implemented through code.

Web scraping must be carefully planned to ensure compliance with legal regulations, platform terms of service, and ethical standards. Researchers should be aware that scraping often violates the terms of service of most major platforms, which can lead to IP blocking, account suspension, or civil legal action. When personal data is involved, it may also trigger substantial legal and financial penalties under data protection regulations, including fines for unlawful processing of personal information. Other risks include copyright infringement if protected content is extracted without permission, as well as prosecution under computer misuse or anti-hacking laws in certain jurisdictions. The legal implications depend on factors such as the nature of the data collected (if public or private), compliance with data protection laws, and whether the site's terms and conditions have been breached. Any scraping activity should therefore be preceded by a thorough legal review and, where possible, the use of officially provided APIs or approved data access channels.

Data Donation

Today, users can often access data that a specific platform has stored about them by filing data access requests based on data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union. This has allowed that researchers invite participants to voluntarily donate their data. Data donations are sensitive and therefore require researchers to be rigorous, transparent, and accountable for how they use the data that they ask users to hand over. Additionally, researchers need to consider the size of the needed data set to address the research purposes.

Types of accessible data

As mentioned before, this guide focuses on publicly available data. This type of data, generally available across all major social media platforms and accessible through the methods outlined here, can be broadly grouped into three main categories:



User data:

This category includes publicly accessible information about public users, such as usernames, display names (if available), bios, aggregated data on number of followers and followings.



Content and engagement data:

This category includes aggregated engagement metrics such as number of likes, comments, shares, and views associated with each piece of content posted by public users.



Metadata:

This category includes contextual information about content, such as post timestamps, geolocation data, and occasionally provenance or authenticity tags, for example, flags identifying AI-generated material.

The table below presents the data points that social media platforms, according to their documentation or codebooks, make available to researchers through platform protocols (APIs, mostly). While most platforms offer a broad range of data points and metadata, LinkedIn stands out as a notable exception, providing significantly less detail in their documentation.

Available Data Points and Metadata by Platform

✓ Yes | ✗ No | N/A : Not applicable

Platforms	Facebook			Instagram	LinkedIn	TikTok	X	YouTube	Bluesky	Reddit	Telegram	Threads		
Spaces	Account	Groups	Pages	Account	Account	Account	Account	Channel	Account	Sub-reddits	Super-groups	Channel	Account	
Name	✓	✓	✓	✓	Data dictionary not available	✓	✓	✓	✓	✓	✓	✓	✓	
Geolocation (user)	✓	✗	✓	✗		✗	✓	✓	✓	✗	✓	✗	✓	✗
Follower Count	✓	N/A	✓	✓		✓	✓	✓	✓	✓	N/A	N/A	✓	✓
Member Count	N/A	✓	N/A	N/A		N/A	N/A	N/A	N/A	✓	✓	N/A	N/A	N/A
Post ^{***}	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Comments	✓*	✓*	✓*	✓*		✓	✓	✓	✓	✓	✓	✓	✓	✓
Timestamp of post	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Views	✓	✓	✓	✓		✓	✓	✓	✓	✗	✗	✓	✓	✓
Original Source	✓	✓	✓	✗		✓	✓	✗	✓	✓	✓	✓	✓	✓
# of Reactions	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Post URL	✗	✗	✗	✗		✓	✓	✓	✓	✓	✓	✓	✓	✗
Media Type	✓	✓	✓	✓		✓	✓	✓	✓	✓	✗	✓	✓	✓
Video	✓	✓	✓	✓		✓	✓	✓	✓	✓	✗	✓	✓	✗
Documents	✓	✓	✓	✓		✓	✓	✓	✓	✗	✗	✓	✓	✗
Image	✓	✓	✓	✓		✓	✓	✓	✓	✓	✗	✓	✓	✗
Audio	✓	✓	✓	✓		✓	✗	✓	✓	✗	✗	✓	✓	✗
Reels/Stories/Shorts	✓	✓	✓	✓		✓	✓	✗	✓	✓	✗	✓	✓	✗
Historical Data	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Real-time Data	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓

* Comments can be only be downloaded in the API, and only from profiles with more than 25K followers.

** Data on Threads its only accessible through the MCL User-Interface.

*** For YouTube and TikTok post equals link to videos and/or description of videos.

Key limitations

Data access is not perfect, and researchers must navigate practical constraints when designing their approach.



There is no one-size-fits-all solution, each approach comes with trade-offs. The best choice depends on your research objectives, context, available resources, and the level of depth or precision your analysis requires.

Ethical considerations in accessing and analysing social media data

When accessing social media data, it is important to consider both ethical and legal implications, including responsibilities and potential risks related to how data is collected and used. The following principles can help guide ethical and responsible access to social media data:

1. Proportionality:

Proportionality is a principle that helps determine the appropriate scope of data access, ensuring that access is limited to what is necessary to achieve a clearly defined purpose. Accessing social media data should always be driven by a legitimate and justifiable research objective and should avoid excessive or intrusive data retrieval.



Key principle:

Access should be limited to the minimum amount of data required for the intended research purpose. Data should not be accessed or reused for unrelated objectives.



Best practice:

When defining the research question, clearly specify what data will be accessed, why it is needed, and how long it will be stored or retained.

2. Privacy:

Even when social media content is publicly available, users may still hold a reasonable expectation of privacy, particularly concerning how their data is accessed, interpreted, used, and stored. Researchers must take this expectation seriously when handling social media data.



Key principle:

The fact that data is publicly available does not automatically grant third-parties unrestricted permission to analyse, repurpose, or publish insights without appropriate safeguards or consent, especially since this data often include sensitive information, such as users' political views.



Best practice:

Apply anonymisation techniques, avoid identifying individuals, and ensure all data access practices comply with applicable privacy laws. Regularly review your data privacy protocols, ideally in consultation with a data protection expert.

3. Data Bias and Representation:

Social media data is not representative of the entire population. Certain groups may be overrepresented or underrepresented due to platform demographics, algorithmic amplification, and even the specific research focus or keywords chosen.



Key principle:

Drawing conclusions from biased data can reinforce stereotypes, produce misleading insights, and contribute to unfair treatment of specific groups.



Best practice:

Acknowledge the limitations of the dataset, incorporate complementary data sources when possible, and critically evaluate how platform algorithms and usage patterns may shape the data being accessed.

4. Transparency:

Transparency relates to how openly researchers communicate about their data access practices. It includes disclosing what types of social media data are being accessed, the methods and tools used, the purpose of access, and who is responsible for managing the data.



Key principle:

A lack of openness about data access can undermine trust, reduce accountability, and make it difficult for others to evaluate or reproduce the research.



Best practice:

Share detailed documentation on how data was accessed, including technical methods (e.g. APIs, platform tools), timelines, and access conditions.

Further Guidance to Access Platform Protocols

This section provides additional information on how to request access to platform protocols that require project-based applications as well as access procedures for platforms with simpler requirements. It is also important to monitor potential updates to data access requirements, as these may evolve over time.

Access to platforms protocols with project-based applications requirements

Access to several major platform protocols, such as the Meta Content Library, TikTok Research API and Virtual Computer Environment (VCE), and Reddit API, require a project-based application. While each platform has its own access pathway and eligibility criteria, applicants are generally expected to demonstrate a clearly defined research project, a verified institutional affiliation, and a commitment to ethical data use.

Access to Meta Content Library

Researchers can apply for access to both, Meta Content Library (User Interface) and API, or choose to request access to only one of them, depending on their needs.

To request access, researchers must submit an application through the Meta Research Tools Manager, Meta's platform for managing research data access requests.

Applicants must meet specific eligibility requirements:



The Secure Data Access Center (CASD), a secure data hosting and access service that manages and controls access to sensitive datasets, will review the application. If approved, Meta will grant access credentials to the platform user interface and/or API. In our review process typically takes around a month.

For detailed instructions and the application process, visit Meta's official documentation:

<https://developers.facebook.com/docs/content-library-and-api/get-access>



Access to TikTok Platform Protocols

Researchers from eligible regions can apply to the TikTok API (if affiliated with an academic institution) or to the TikTok VCE (if affiliated with a non-profit organisation). To request access, researchers must submit a formal application through TikTok's application form, providing details about themselves, their organization, and their research project.

Applicants must meet specific eligibility requirements:

-  **Be in an eligible region** and affiliated with an eligible organization (e.g., academic institutions in the US, EEA, UK, Switzerland; or non-profits in the EU)
-  **Have relevant** research expertise and data analysis experience.
-  **Be independent** from commercial interests and conduct research on a non-profit/public-interest basis.
-  **Disclose** research funding.
-  **Provide a clear research proposal** showing that the requested access is necessary and proportionate.
-  **Commit to data security**, confidentiality, and protection of personal data.
-  **Show evidence** of ethical review.
-  **Agree to the TikTok Research Tools Terms of Service.**

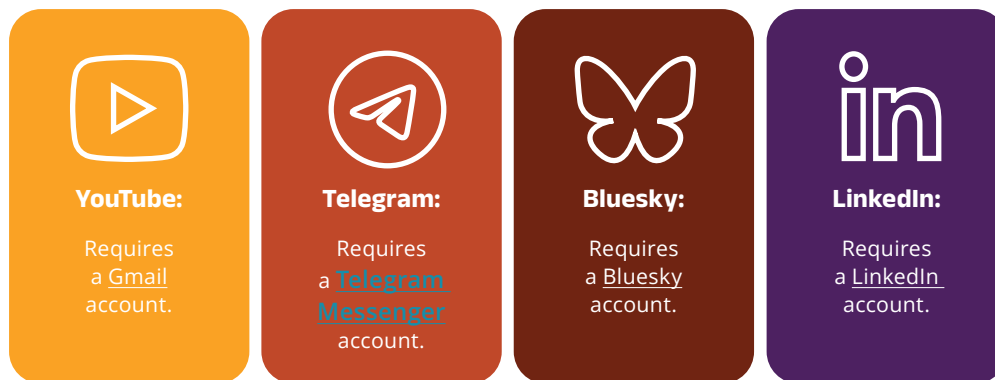
The platform will review the application within a month of submission. According to TikTok, they are working on expanding data access to other regions. For more details on the application process and updates, visit TikTok's official website: [Research API | TikTok for Developers](#)

Access to Reddit API

Reddit also provides researchers with access to its API through an application process. However, as this program is still in development, further details on the application process are not yet available. For updates, visit the Reddit channel dedicated to this purpose: [reddit4researchers](#)

Access to platform protocols requiring only account creation

Researchers can access YouTube, Telegram, Bluesky and LinkedIn platform protocols by only creating an account on the respective platforms, without any additional eligibility criteria.



Access to platform protocols that require a paid subscription

Researchers can access the X API by creating a platform account and selecting a subscription plan. For detailed information, visit X's official website: <https://x.com/>

Navigating Data Access for Social Media Monitoring: A Practical Guide

This publication was funded/co-funded by the European Union. Its contents are the sole responsibility of the author and do not necessarily reflect the views of the European Union.



SUPPORTING
AN ENABLING ENVIRONMENT
FOR CIVIL SOCIETY



Funded by
the European Union



DEMOCRACY
REPORTING
INTERNATIONAL



European
Partnership for
Democracy



forus

CONNECT
SUPPORT
INFLUENCE



TRANSPARENCY
INTERNATIONAL
the global coalition against corruption