PLATFORM RISK & COMPLIANCE

Platform risk and compliance: is Oriane allowed to use data from Instagram and TikTok?

Yes, within a clear scope. Oriane only indexes public videos posted by public accounts. We never access anything behind a login, a privacy setting or a follow approval. We work like a search engine over content that creators and brands chose to make public.

The short version

- We index public videos from public accounts only.
- We do not index private accounts, private videos or stories.
- We never log in. We read public pages as a visitor.
- We do not use any platform API.
- We do not create accounts, comment or interact on platforms.
- Any account can opt out of Oriane at any time.
- Our method has been reviewed by the legal, security and data protection teams of large enterprise customers.
- US courts have ruled for logged-off collection of public data in cases brought by Meta and X.

What does Oriane index, and what does it not index?

Oriane indexes public videos posted by public accounts. Our index is built on the content and the metadata of publicly available videos.

We do not index:

- private accounts
- private videos
- ephemeral formats such as stories

We do not access anything behind a login, a privacy setting or a follow approval. This is the same operation a classic search engine performs on a public web page.

What do Instagram and TikTok say about indexing public content?

Both platforms state in their own help centers that public content can be indexed by search engines and surfaced outside their apps.

Instagram

Instagram's Help Center says search engines can index photos and videos from public reels and posts, for accounts that are public, professional (Business or Creator) and held by someone over 18. Meta widened this rollout in July 2025. Source: Instagram Help Center.

TikTok

TikTok states that public accounts and videos may be indexed by search engines and surfaced outside the app. Source: TikTok Help Center.

TikTok's own robots.txt does not block general crawlers from public profile and video pages. It restricts app, login and utility paths, and lists some AI training crawlers by name. Source: TikTok robots.txt.

Oriane is a search layer over public video. Videos cannot be watched on Oriane, so every result sends attention back to the creator and to the original post.

How does Oriane collect videos?

Oriane does not use the platforms' APIs. APIs can change without notice, so we do not build on them. We visit public pages and index what is publicly displayed.

1. We build a list of public accounts to follow. New accounts are discovered from public mentions in captions, co-authors and bios.
2. We check whether these accounts have posted new public videos since the last check.
3. AI analyzes each new video: what is visible, what is said and what text appears on screen.
4. The results are stored in our search index.

By design, Oriane does not:

- log in to any platform
- create fake accounts or operate multiple accounts
- comment, message or interact on the platforms

The product has no such capability.

What does Oriane store?

Oriane stores the data that powers search: extracted frames, their embeddings, thumbnails, transcripts and public metadata. Source video files are not kept as part of the index.

What can customers do with the data, and who owns the content?

Customers receive public metadata and AI-extracted data through the Oriane app, API and MCP. This lets them find and analyze videos by what is in them, not only by captions and tags.

The content belongs to the creators who posted it. Customers do not receive any rights over the underlying videos. As with any search tool, customers are responsible for using the data lawfully, including respecting copyright.

Because Oriane finds video by its content, it can also help rights holders see where their content travels once it is clipped, remixed and reposted.

What does the law say about collecting public data?

Platform terms of service are contracts. They are not the same as law. Recent US court decisions have gone against platforms that tried to use their terms to control access to public data.

- **Meta v. Bright Data** (N.D. Cal., January 2024). The court held that Facebook and Instagram terms do not prohibit logged-off collection of publicly available data. Meta later dropped its remaining claim. Read the client alert.
- **X Corp v. Bright Data** (N.D. Cal., May 2024). The court dismissed X's claims. It held that using scraping tools is not inherently unlawful and that the Copyright Act preempted X's contract claims. X later refiled narrower claims about server load. Read the analysis.

Terms of service and robots.txt are not the law

A platform can write anything in its terms of service or its robots.txt file. Neither is a statute. Courts treat terms of service as a contract and robots.txt as a convention.

- **hiQ Labs v. LinkedIn** (9th Cir.). The court held that the Computer Fraud and Abuse Act's "without authorization" rule does not apply to public websites. The case later settled. Read the analysis.
- **robots.txt** is a file where sites tell crawlers which pages they would like them to visit. It creates no legal duty for a visitor reading public pages.
- **Instagram** lists Bright Data's crawler by name in its robots.txt and disallows it. Meta still lost its contract claim against Bright Data over public, logged-off data.

These are US court decisions. They do not settle every question in every country. This page describes our position and is not legal advice.

GDPR

For personal data under GDPR, we rely on legitimate interest. We documented this in a Legitimate Interest Assessment that has been reviewed by the data protection teams of enterprise customers. See our Privacy and Cookies policy and our DPA.

Have enterprise customers reviewed Oriane's approach?

Yes. Large luxury and consumer groups have put Oriane through long, formal reviews covering IT security, AI governance and data protection. We have passed every review completed so far, and others are in progress. Each team reviewed our specific method.

For these reviews we have produced:

- a GDPR Legitimate Interest Assessment
- full security and privacy questionnaires
- a SOC 2 Type 2 report and ISO 27001 certification

Every new enterprise customer triggers a fresh review, so we keep this documentation current.

Is Oriane the first company to collect public social data?

No. Public web data is an established industry. Bright Data and Oxylabs, its two largest providers, collect public data from the same platforms at scale. They report more than $300M and $350M in annual recurring revenue. Meta and X both sued Bright Data over public data, and the courts ruled for Bright Data on the key claims.

Platforms take part in this market too. Meta was itself a Bright Data customer before it sued over its own platform, and ByteDance runs its own web crawler, Bytespider. In July 2025, Instagram opened public posts and reels from eligible professional accounts to Google and Bing.

Could a platform restrict Oriane's access?

Oriane uses no platform API, so there is no access agreement a platform could withdraw. We read public pages the same way search engines and public data providers such as Bright Data do. To block Oriane alone, a platform would have to restrict logged-off access for every visitor and every search engine, or stop the whole public data industry, which Meta tried against Bright Data and lost in court. We track changes to platform terms and help center policies, and we are ready to adjust our scope if they change.

We are also not tied to any single source. We index Instagram, TikTok and now YouTube, and we keep adding public video sources so that no single platform controls the index.

Does Oriane work with the platforms?

We are not an adversary to the platforms. We make public content discoverable and send traffic back to creators and brands. We engage with platform teams openly and aim for official partnerships over time, as social listening tools such as Brandwatch, Talkwalker and Meltwater did. A partnership would be an upside for us, not a technical requirement.

How can an account opt out of Oriane?

Any creator or brand can opt out of being indexed at any time. Use the opt-out page.

Frequently asked questions

Does Oriane access private accounts or content behind a login?

No. Oriane only indexes public videos from public accounts. It never logs in, and it never accesses anything behind a login, a privacy setting or a follow approval.

Does Oriane use the Instagram or TikTok API?

No. Oriane does not use any platform API. It reads public pages as a visitor, the way a search engine does.

Does Oriane create accounts, comment or interact on social platforms?

No. Oriane does not create fake accounts, operate multiple accounts, comment, message or interact on platforms. The product has no such capability by design.

Does Oriane store the original videos?

No. Oriane stores extracted frames, embeddings, thumbnails, transcripts and public metadata. Source videos are not kept as part of the index.

Can creators or brands remove their content from Oriane?

Yes. Any account can opt out of being indexed at any time on the opt-out page.

Who owns the videos in Oriane?

The creators who posted them. Oriane gives customers metadata and AI-extracted data to find and analyze videos. Customers do not receive rights over the underlying content and must respect copyright in their use.

Is Oriane the first company to collect public social media data?

No. Bright Data and Oxylabs have collected public web data from the same platforms for years. Meta and X sued Bright Data over public data, and the courts ruled for Bright Data on the key claims. Oriane works on the same public, logged-off basis.

Sources

Platform pages and court decisions behind the statements above. Law firm and news summaries are linked for convenience. Read the platform pages and the court orders for the full text.

Platform rules

- Instagram Help Center: search engine indexing of public content. Sets the criteria for indexing: public, professional and over 18.
- afaqs: Search engines can now index public content from Instagram. News coverage of the July 2025 change and its eligibility criteria.
- TikTok Help Center: public content and search engines.
- tiktok.com/robots.txt and instagram.com/robots.txt. Retrieved November 25, 2026.

Court decisions

- **Meta Platforms, Inc. v. Bright Data Ltd.**, No. 3:23-cv-00077-EMC (N.D. Cal. January 23, 2024), summary judgment for Bright Data on Meta's breach of contract claim. Quinn Emanuel client alert and Farella Braun + Martel analysis.
- **X Corp. v. Bright Data Ltd.**, No. C 23-03698 WHA (N.D. Cal. May 9, 2024), complaint dismissed with leave to amend. Courthouse News report and Frankfurt Kurnit Klein + Selz analysis.
- **hiQ Labs, Inc. v. LinkedIn Corp.** (9th Cir. 2022), on the Computer Fraud and Abuse Act and public websites. Morgan Lewis analysis.

Industry

- Bright Data: data for AI is fueling growth. Company-reported ARR.
- Entrepreneur: Oxylabs takes $130M. Company-reported ARR.
- Courthouse News: Meta v. Bright Data. Meta's past use of Bright Data.
- Fortune: ByteDance's Bytespider crawler.

Last updated: November 26, 2026. Questions about compliance, or a security or legal review to run? Contact us.