noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna
AUSTRIA

Overview of Meta's falsehoods and "spin"

We are used to Meta sharing false narratives, information or claims with decision makers, journalists and the general public. Much of this information is given in semi-confidential or confidential background communications that are not available to the general public. We are often confronted with questions based on such claims by Meta. Given that our complaints regarding "Meta AI" are lengthy and that AI is still a novel technology, we have decided to summarise the main arguments put forward by Meta in response to the outcry about Meta AI, and why they are inaccurate.

We would like to point out that some Meta employees may be acting in good faith, and are often neither technology or legal experts themselves, and may not be aware that the claims they are making in their role in the media or public policy teams are inaccurate.

1) Meta only uses public information

Meta now refers to a [PR blog post](#) to claim that it only uses information that users have shared publicly. This is false and irrelevant:

- The blog post is inconsistent with the [official information that has been shared with users](#) over the past week(s), which explicitly states:

  "We also use information shared on Meta's Products and services. This information could be things like posts or photos and their captions. We do not use the content of your private messages with friends and family to train our AIs."[1]

- Furthermore, the legally relevant document is the new [Meta privacy policy](#) (not a blog post). The privacy policy explicitly allows the use of <u>any personal data</u> (public, private, "on" Meta systems or "off" Meta systems, as well as any third party data) for any purpose that uses "AI technology" with anyone (any "third party") as the recipient of information.

- The relevant table is not linkable or easy to find (see screenshot on the next page) but clearly states the following:

  - Under the column "*Why and how we process your information?*" (commonly known as the "purpose" in the GDPR), they say the (almost unlimited) purpose is:

  "To develop and improve artificial intelligence technology (also called AI at Meta) we provide, on our Products and to Third Parties."

---

[1] See https://www.facebook.com/privacy/genai, under "*Where does Meta get training information?*"

noyb – European Center for Digital Rights | Goldschlagstr. 172/4/3/2, 1140 Vienna, AUSTRIA | ZVR N°: 1354838270
www.noyb.eu | General email: info@noyb.eu | IBAN: AT21 2011 1837 8146 6600

Page 1 of 3

- Under the column "*Legitimate interests relied on*" Meta lists:

    "*To create, provide, support and maintain artificial intelligence technology that enables people, businesses, and others to express themselves, communicate, and discover and engage with information relevant to their interests.*"
    "*To offer artificial intelligence technology to Third Parties, including developers and researchers.*"
    "*To develop and improve artificial intelligence technology in a consistent manner while ensuring appropriate safeguards, such as improving model responses for safety and accuracy.*"
    "*To get feedback on how our users engage with artificial intelligence technology and to improve its performance.*"

- Under the column "*Information categories we use?*" for this Meta lists:

    "*Your <u>activity and information that you provide</u>. <u>Content that you create</u>, like <u>posts, comments or audio. Messages you send or receive</u> from businesses, professional accounts, or Meta (such as to Meta's artificial intelligence technology), and messages in features designed to be public, including message content and metadata, subject to applicable law. <u>Apps and features you use, and what actions you take in them.</u>*"

    as well as

    "*<u>Information from partners, vendors and third parties</u>.*"

Screenshot from the privacy policy

Last but not least: Even such <u>public</u> social media data is protected under the GDPR and an overriding "legitimate interest" is unlikely (see below EDPB on OpenAI, scraping such public social media data).

Overall, the claim that Meta only uses "public" information is not reflected in the privacy policy or the information sent to users – it is only claimed in a PR blog post. The claim is (in relation to all relevant legal documents) <u>false</u>.

2) The EDPB allowed "legitimate interest" in a case on Open AI

In initial statements, Meta also seems to claim that the EDPB has approved the use of "legitimate interests" to train Large Language Models ("LLMs") in a decision on OpenAI. This is incorrect:

- The EDPB had a <u>report from an (informal) "task force"</u>, which has no legal status under the GDPR.
- The EDPB task force merely <u>described</u> OpenAI's approach of scraping <u>public</u> information that also <u>contained some personal data</u>.
- The EDPB task force mentions that OpenAI currently relies on "legitimate interests" but does <u>not take a position whether this is legal</u>:

    "While <u>the assessment of the lawfulness is still subject to pending investigations…"</u>[2]

- However, the EDPB task force itself mentions that even public social media data could be excluded from the training data, as a measure to potentially strike a balance that would allow OpenAI to claim a legitimate interest:

    "… safeguards could inter alia be technical measures, defining precise collection criteria and ensuring that certain data categories are <u>not collected or that certain sources (such as public social media profiles)</u> are excluded from data collection." [3]

Overall, the EDPB task force did not say that OpenAI was lawfully relying on a "legitimate interest" – and has even mentioned "public social media data" as a situation where such a legitimate interest is unlikely to prevail.

This claim by Meta is <u>absolutely false</u>.

3) The new privacy policy is broad, but Meta does (currently) not use data in this way

We also notice a very (old) pattern in Meta's arguments. The "two step" implementation:

- **Step 1:** Change the policy and all legally relevant documents, but claim you're not actually doing it (yet). This is technically correct, as you need to inform users first, so naturally you don't engage in the processing (yet).
- **Step 2:** Turn on the systems a couple of months later If there is any public knowledge about it (usually people can't find such changes on a server), then just refer to the privacy policy update in step 1 and say 'this isn't new' because it came with the last update of the privacy policy.

The arguments at both points in time are (technically) correct, but overall they are just used to make sure that the general public does not get too angry about the changes because they are "not yet" active and later "not new". It is a simple, but rather effective playbook.

This claim is therefore technically correct (at best)

---

[2] https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf § 17.
[3] https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf § 17.