HANGING BY META’S THREADS

[*NB: check the byline, thanks. /~Rayne*]

If you are very much online in social media, you’ve likely heard the buzz about Threads — the new microblogging platform owned and operated by Facebook’s parent, Meta.

I’m not going to get into a detailed discussion of Threads versus its problematic competitor Twitter or ex-Twitter CEO Jack Dorsey’s problematic alternative, Bluesky Social. You’re perfectly capable of doing the homework on them and other competing microblogging platforms.

Of concern to me: how will Threads eventually interact with the open source federated universe (fediverse) of platforms including Mastodon. Threads is expected to federate eventually and allow easy sharing of communications and content between member platforms in the fediverse.

There has been so much conversation about this topic in Mastodon that I’ve had to filter it out. The discussion has been warranted, but the subject has been polarizing and frankly exhausting.

Some Mastodon users — mostly those who left Twitter and miss it badly — want this new Meta project to integrate seamlessly with Mastodon so that they can encourage former Facebook folks to come over to Mastodon. They’re missing much busier levels of activity in their timelines which was driven by algorithms at Twitter and as well at Facebook. And some simply can’t handle the increased complexity Mastodon poses, from choosing an instance to finding friends old and new, or building a feed.

Some Mastodon users — like me — don’t really care to federate with Meta’s users whether from Facebook or Instagram. In my case my primary concerns are data privacy and remaining ad free. While I feel fairly confident my experience

within Mastodon won't ever involve ads, I can't say that will be the case once I make contact with someone in Threads just as looking at a tweet on Twitter will likely expose me to advertising. I simply do not want to give my attention without my *advance* consent to any business advertising in social media.

(Side note: look around here in emptywheel — see any ads? How's that shape your experience here?)

Because of these concerns I've been looking for ways to limit exposure of personal data now that Meta has begun a soft launch of Threads over the last 24 hours.

~ ~ ~

Ahead of a formal launch, Eugen Rochko, Mastodon's creator, published a statement about the way Threads and Mastodon are supposed to work. This statement was the result of meetings he had with Meta about the way Threads was expected to work once it joined the fediverse.

See https://blog.joinmastodon.org/2023/07/what-to-know-about-threads/

Note this paragraph in particular:

> **Will Meta get my data or be able to track me?**
>
> Mastodon does not broadcast private data like e-mail or IP address outside of the server your account is hosted on. Our software is built on the reasonable assumption that third party servers cannot be trusted. For example, we cache and reprocess images and videos for you to view, so that the originating server cannot get your IP address, browser name, or time of access. A server you are not signed up with and logged into cannot get your private data or track you across the web. What it can get are your public profile and public posts, which are publicly accessible.

There’s still a problem here, if you think back to what researcher Aleksandr Kogan could do with Facebook’s data harvested ~2014. The network of people around those whose data had been obtained could still be deduced.

If some users outside Meta have past usernames in Facebook/Instagram/WhatsApp which match; and/or if users have had previous long-term contacts with Meta users, and/or if data from Twitter or other social media platforms can also be acquired and correlated, it wouldn’t be difficult to build out the social network of Threads users who interface with Mastodon or other fediverse platform users.

This gets around the reason why Mastodon in particular has been resistant to integrating search across the fediverse. Search was intentionally limited during Mastodon’s development to prevent swarming and brigading attacks and other forms of harassment targeting individuals, particularly those identified in minority and/or protected classes.

Consider for example the case of a gay person who associates with other gay people who know each other locally but communicate using these tools. It won’t take that much effort especially with the aid of GPT AI to to create the means to identify entire networks of gay persons related one to several degrees apart. Once identified, it wouldn’t take much to begin brigading them if enough other hostile accounts have been established. One could even imagine the reverse identification process applied in order find persons who are violently anti-gay and likely to welcome opportunities to harass gays.

Imagine, too, how this could affect young women contacting others looking for reproductive health care information.

~ ~ ~

There is a temporary saving grace: Threads is not approved in the EU. Not yet.

The server which hosts my Mastodon account is

located in the EU and therefore will not yet allow Threads users access through federation.

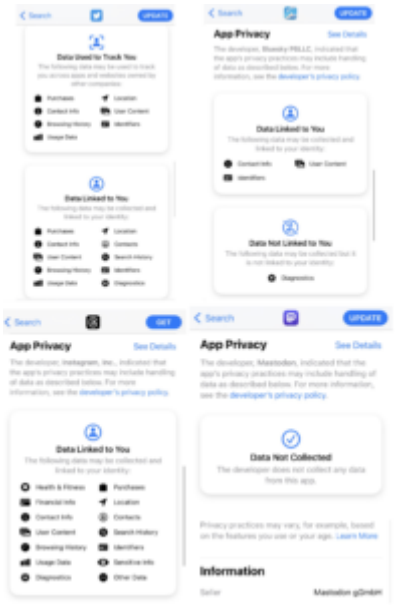
The same server's administrator also polled users and asked if they wanted to allow Threads to federate with this server — they voted it down.

So I guess I'm okay where I'm at for the moment.

There are fediverse servers out there which will never allow Threads to federate with them. I've seen a Mastodon server which has said it will never allow Meta applications to federate because it's against their server's terms of use to allow entities which enable genocide and crimes against humanity to do so.

Good for them.

And good for us: PressProgress editor Luke LeBrun collected the app privacy policies for Threads, Bluesky, Twitter and Mastodon for contrast and comparison:



Can't imagine why I would have any concerns about Threads…ahem.

~ ~ ~

This is all fairly new and unfolding even as I write this. What the fediverse will look like once Threads makes full contact is anybody's guess.

But there are several things we do know right now, with certainty:

> — Meta has been and remains a publicly-held holding company for a collection of for-profit social media businesses. Its business model relies on selling ad space based on targeted markets, and selling data. This will not change short of a natural disaster like a meteor strike taking out all of Silicon Valley and the greater San Francisco area, and that may still not be enough to change the inevitable monetization of Threads and all the platform touches.
>
> — Meta has been operating under a consent decree issued by the Federal Trade Commission since 2011 after violating users' privacy; it violated that agreement resulting in a $5 billion fine which it has fought against paying. Meta's track record on privacy is not good and includes the non-consensual collection of personal data by academic Aleksandr Kogan. The data was later used by Cambridge Analytica/SCL and may have been involved in influence operations during the 2016 election.
>
> — The EU is light years ahead of the US when it comes to privacy regulations. California as a state comes closest to the EU in its privacy regulations but it shouldn't matter which state we are in — our privacy concerns are the same across the country, and opt-in should be the standard, period. US state and federal lawmakers have been and will likely continue to be slow to take any effective action unless there is considerable pressure by the public to meet the EU's efforts.
>
> — Law enforcement in the US have purchased and used without a warrant personal data collected through users' use of social media. There has been inadequate pressure by the public to make this stop and will

> put the health and safety of women and minority groups at risk.

Changing the direction in which this is headed requires engagement and action. By now you know the drill: contact your representatives in Congress and demand legislation to protect media users' privacy. (Congressional switchboard: (202) 224-3121 or Resist.bot)

That's no slip: no form of media on the internet should be immune from protecting its users' privacy.

You should also contact your state's attorney general and as well as your legislators and demand your state matches California's Consumer Privacy Act (CCPA) when it comes to privacy protections – at a minimum. Meeting the EU's General Data Protection Regulation (GDPR) would be better yet.