Notice of Exempt Solicitation

NAME OF REGISTRANT: Meta Platforms Inc.

NAME OF PERSONS RELYING ON EXEMPTION: Arjuna Capital

ADDRESS OF PERSON RELYING ON EXEMPTION: 13 Elm St. Manchester, MA 01944

WRITTEN MATERIALS: The attached written materials are submitted pursuant to Rule 14a-6(g)(1) (the "Rule") promulgated under the Securities Exchange Act of 1934, in connection with a proxy proposal to be voted on at the Registrant's 2023 Annual Meeting. Submission is not required of this filer under the terms of the Rule but is made voluntarily by the proponent in the interest of public disclosure and consideration of these important issues .

April 27, 2023

Dear Meta Platforms Inc. Shareholders,

We are writing to urge you to **VOTE "FOR" PROPOSAL 9** on the proxy card, which asks the Company to minimize risks associated with abortion-related law enforcement requests. The Proposal makes the following request:

> **Resolved**: Shareholders request our Board issue a public report assessing the feasibility of diminishing the extent that the Company will be a target of abortion-related law enforcement requests by expanding consumer privacy protections and controls over sensitive personal Meta user data. The report should be produced at reasonable expense, exclude proprietary or legally privileged information, and be published within one year of the annual meeting.

We believe shareholders should vote "FOR" the Proposal for the following reasons:

1. The company collects sensitive user data that may be vulnerable to abortion-related prosecutions.

Reproductive rights are under siege in the United States. Following the unprecedented revocation of the constitutional right to abortion in June 2022, 24 states have banned abortion or are likely to do so.[1] Law enforcement in these abortion-restrictive states are expected to rely on consumer data to investigate and prosecute individuals who provide, aid, or receive an abortion, even if the procedure was conducted in a state where abortion remains legal.

Meta amasses large troves of consumer data from 3.74 billion monthly active users.[2] Across its platforms, Meta collects data via users' chat messaging, search queries, and geolocation. Given the current environment the company is operating in following the Supreme Court's decision in *Dobbs v. the Jackson Women's Health Organization*, users' digital reproductive health footprint is at risk of being obtained through law enforcement data requests with the intent to prosecute those who have received an abortion. It is crucial that Meta does what it can to protect users from these risks.

---

[1] https://www.guttmacher.org/2023/01/six-months-post-roe-24-us-states-have-banned-abortion-or-are-likely-do-so-roundup.

[2] https://investor.fb.com/investor-news/press-release-details/2023/Meta-Reports-Fourth-Quarter-and-Full-Year-2022-Results/default.aspx

2. Meta has shown vulnerabilities in protecting users' sensitive, personal data.

Meta's data has already been accessed by law enforcement to prosecute a user for allegedly obtaining an illegal abortion. Last year, our company fulfilled a data request from a Nebraska police department for private Facebook messages between a mother and daughter, who were both subsequently charged with felony crimes related to the alleged illegal termination of the daughter's pregnancy (for additional examples, see Addendum A). Following significant negative press, Meta responded by stating that: (1) the warrants in that case "did not mention abortion at all," but rather "[c]ourt documents indicate[d] that police were at that time investigating the alleged illegal burning and burial of a stillborn infant," and (2) "the warrants were accompanied by non-disclosure orders, which prevented [Meta] from sharing information about them."[3] This example could not illustrate better why it is essential that Meta considers additional data security and data request fulfillment practices that would safeguard users from these risks—risks that are likely unknown to the average Meta user.

It is evident that Meta is vulnerable to additional law enforcement data requests related to abortion, particularly with respect to interstate conflicts regarding exercise of reproductive rights in states where abortion remains legal. Shareholders have reason to be concerned about whether the enforcement of criminal abortion laws will betray the trust of users, resulting in reputation loss, user migration to other platforms, and consequent harm to financial wellbeing of the Company. The Proposal therefore calls upon management to examine the risks associated with the Company's current data handling practices, including its response to government information requests, in the face of new restrictive abortion laws.

Board Opposition Statement

1. Meta states its commitment to addressing issues of safety, security, and privacy, yet the company has a terrible track record on data protection and privacy.

Meta objects to the need of the report by outlining its commitment to addressing issues of safety, security, and privacy. Yet, the company's failures to privacy protections in recent years leads one to be skeptical of their current commitments. Recent failures of privacy protection include:

- In 2018, Facebook admitted to mishandling data from about 87 million Facebook users which had been improperly obtained by political data-analytics firm Cambridge Analytica.[4] As a result of that data breach, in 2019 the Federal Trade Commission imposed a record-breaking $5 billion penalty on Facebook and forced the Company to submit to a modified corporate structure to settle charges that the company violated a 2012 FTC order by deceiving users about their ability to control the privacy of their personal information.[5]
- In April 2021, it was reported that personal information of over 500 million Facebook users was shared online in a massive data leak.[6]
- In April 2022, Meta engineers admitted that they do not have control and understanding of how their systems use all the data they collect on users.[7]

---

[3] https://about.fb.com/news/2022/08/meta-response-nebraska-abortion-case/

[4] https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3

[5] https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook

[6] https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+typepad%2Falleyinsider%2Fsilicon_alley_insider+%28Silicon+Alley+Insider%29

[7] https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes

- In October 2022, Meta warned users that as many as one million Facebook users' login info may have been compromised due to malicious apps stealing data through the Facebook third-party login.[8]

It is essential that Meta does more to rebuild users' and investors' trust in the company's privacy practices. The report requested by the Proposal would provide Meta an opportunity to fully assess its current data handling practices as it relates to reproductive health information, while providing greater transparency to investors. This transparency is essential to restore trust in the company's protection of user data.

2. While Meta has built tools to help users secure their information and give them more control, the Company has left the onus on the user to protect their data.

In its opposition statement to this proposal, Meta describes options for users to secure their information by opting into encrypted messaging on Messenger and Instagram, using the Off-Facebook Activity tool, and disabling location services. Currently, these are all steps that users themselves must know about and opt into to be able to protect their data. Unfortunately, the average user may not know of these possibilities and/or understand the steps to better secure their information. Indeed, a 2022 Ipsos poll found that most (70%) Americans agree that controlling who can access their online personal information has become increasingly difficult.[9]

Instead of placing the onus on the users to protect their data, Meta must consider ways that it can protect all its users from their data being inappropriately accessed. Default end-to-end encryption on Messenger and Instagram is one of the ways that Meta could better protect its users. Our company has promised default encryption on these platforms for quite some time, but still has not rolled out this function which would take the onus away from the users themselves protecting their data.

Meta should also strengthen its process for handling law enforcement data requests. The Company could require law enforcement to report on the "records request" form whether the request concerns reproductive health information or is related to the enforcement of abortion restrictive laws. Emergency data requests, which do not require submission of a subpoena or warrant mandating disclosure, should receive extra scrutiny from the Company in order to avoid providing sensitive data to malicious actors. Indeed, in 2021, Meta provided data to the cybercriminals who forged emergency legal requests.[10] The Company could integrate clear guidelines for processing such emergency requests, including contacting the law enforcement agency to confirm the validity of the request, as is the case with Apple.[11]

3. It is evident that Meta must consider additional law enforcement data request practices to better protect users from abortion-related requests.

The opposition statement discusses how the company's transparency reporting addresses government requests for information. Yet transparency in and of itself did not prevent Meta from complying with the Nebraska police warrant.

---

[8] https://www.cbsnews.com/pittsburgh/news/meta-warns-as-many-as-one-million-facebook-users-that-their-logins-may-have-been-compromised/

[9] https://www.ipsos.com/en-us/news-polls/data-privacy-2022

[10] https://www.bloomberg.com/news/articles/2022-03-30/apple-meta-gave-user-data-to-hackers-who-forged-legal-requests?leadSource=uverify%20wall

[11] https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf

The report requested in this Proposal would allow Meta to better protect its users from these types of requests by considering, after consultation with reproductive rights and civil liberties organizations, questions such as:

- Many privacy experts have concluded that gag orders are overused in courts and are inapplicable in many legal matters. [12] Could Meta commit to challenging gag orders in law enforcement data requests whenever they are overly vague or infringe upon constitutionally protected liberties ?
- Could Meta commit to notifying all subjects of inquiries once the gag order on a warrant has expired? This would provide affected consumers the opportunity to seek advance legal counsel or challenge an ongoing investigation.
- Reporting indicates that law enforcement must complete a form developed by the Company in order to submit a request for Facebook user data.[13] The form includes a field in which law enforcement must select from a dropdown menu the "nature of the case" related to the data request (e.g., credit card fraud, homicide, gang activity). Could Meta consider adding a "reproductive health-related" category under the "nature of case" dropdown ? This could add an additional step to help mitigate instances like the Nebraska case.
- During the reporting period, what lessons were learned by the legal team responding to law enforcement requests, and has this changed Meta's thinking about scrutinizing future requests?

4. Production of the requested report would be cost-effective and a good use of resources.

Meta states in its opposition statement that due to its current efforts in user privacy and ongoing transparency on the topic, the report is unnecessary and would not be a good use of resources. We disagree with this statement as Meta has unfortunately shown over the years that it operates reactively instead of proactively to user safety and privacy issues. Given the unprecedented threat to women's reproductive health in a post-*Dobbs* era amidst a technological world, there are new vulnerabilities that technology companies like Meta must consider. This report would provide an opportunity for Meta to fully consider the risks of becoming a target of abortion-related law enforcement requests so that it may mitigate future controversies and rebuild investors' trust in the company.

Conclusion

For all the reasons provided above, we strongly urge you to support Proposal 9. We believe that implementing the requested report will help ensure that Meta does more to monitor its data handling practices so that they do not expose consumers to serious risks stemming from abortion-related criminal prosecutions, thereby eroding shareholder value by diminishing the Company's reputation, consumer loyalty, brand, and values.

Please contact Julia Cedarholm at juliac@arjuna-capital.com for additional information.

Sincerely,

Natasha Lamb

Arjuna Capital

---

[12] https://apnews.com/article/how-big-tech-created-data-treasure-trove-for-police-e8a664c7814cc6dd560ba0e0c435bf90; https://www.newsweek.com/big-tech-complied-85-government-requests-handed-over-data-first-half-2020-1603070

[13] https://netzpolitik.org/wp-upload/2016/08/facebook-law-enforcement-portal-inofficial-manual.pdf

ADDENDUM A:

Examples of harms from companies' sharing of reproductive health-related data with third parties without consumer consent

https://nebraskaexaminer.com/2022/08/10/facebook-data-used-to-prosecute-nebraska-mother-daughter-after-alleged-abortion/
In 2022, Meta complied with a data request from a local Nebraska police department for private Facebook messages between a mother and daughter, who were both subsequently charged with felony crimes related to the alleged illegal termination of the daughter's pregnancy.

https://scholarworks.law.ubalt.edu/cgi/viewcontent.cgi?article=2078&context=ublr
In 2017, a woman in Mississippi experienced an at-home pregnancy loss. A grand jury later indicted her for second-degree murder, based in part on her online search history, which recorded that she had looked up how to induce a miscarriage.

https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/
A 2019 report in *The Washington Post* revealed that pregnancy app Ovia Health sold user health data to their employers, without user consent.

https://www.leagle.com/decision/ininco20160722184

In 2013, a woman was sentenced to twenty years in prison for "neglect of a dependent and feticide" after taking abortion pills she purchased online. Evidence presented against her at trial included online research she conducted, the email confirmation she received from internationaldrugmart.com, and unencrypted text messages to a friend about her relationship, becoming pregnant, and the pills she purchased.

https://gizmodo.com/data-brokers-selling-pregnancy-roe-v-wade-abortion-1849148426
In 2022, *Gizmodo* identified 32 brokers selling data on 2.9 billion profiles of U.S. residents pegged as "actively pregnant" or "shopping for maternity products."

https://www.propublica.org/article/websites-selling-abortion-pills-share-sensitive-data-with-google
A 2023 investigation by *ProPublica* found online pharmacies that sell abortion medication such as mifepristone and misoprostol are sharing sensitive data (including users' web addresses, relative location, and search data) with Google and other third-party sites — which allows the data to be recoverable through law-enforcement requests.

https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other In 2022, the Federal Trade Commission sued Kochava – a data analysis platform primarily used by companies for marketing purposes – for selling data that tracks people at reproductive health clinics, places of worship, and other sensitive locations.

This is not a solicitation of authority to vote your proxy. Please DO NOT send us your proxy card. Arjuna Capital is not able to vote your proxies, nor does this communication contemplate such an event. The proponent urges shareholders to vote for Proxy Item 9 following the instruction provided on the management's proxy mailing.

The views expressed are those of the authors and Arjuna Capital as of the date referenced and are subject to change at any time based on market or other conditions. These views are not intended to be a forecast of future events or a guarantee of future results. These views may not be relied upon as investment advice. The information provided in this material should not be considered a recommendation to buy or sell any of the securities mentioned. It should not be assumed that investments in such securities have been or will be profitable. This piece is for informational purposes and should not be construed as a research report.