

## NOTICE OF EXEMPT SOLICITATION

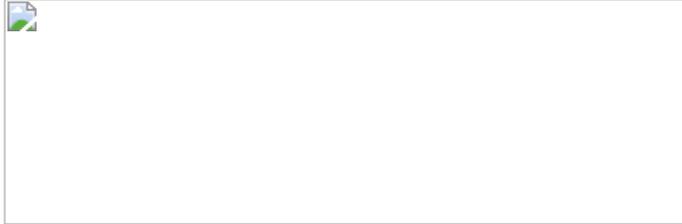
Pursuant to Rule 14a-103

Name of the Registrant: Microsoft Corporation

Name of persons relying on exemption: National Center for Public Policy Research

Address of persons relying on exemption: 2005 Massachusetts Avenue NW, Washington, DC 20036

*Written materials are submitted pursuant to Rule 14a-6(g) (1) promulgated under the Securities Exchange Act of 1934. Filer of this notice does not beneficially own more than \$5 million of securities in the Registrant company. Submission is not required of this filer under the terms of the Rule but is made **voluntarily** in the interest of public disclosure and consideration of these important issues.*



### **PROXY MEMORANDUM**

**TO:** Shareholders of Microsoft Corporation (“Microsoft” or the “Company”)

**RE:** The case to vote **FOR** Proposal 5: (“European Security Program Censorship Risk Audit”). European Security Program Censorship Risk Audit submitted by NCPPR.

*This is not a solicitation of authority to vote your proxy. Please DO NOT send us your proxy card; National Center for Public Policy Research (“NCPPR”) is not able to vote your proxies, nor does this communication contemplate such an event. NCPPR urges shareholders to vote **for Proposal 5**, following the instructions provided on management’s proxy mailing.*

*The following information should not be construed as investment advice.*

#### **In Support of Proposal 5**

We write to encourage you to vote in favor of our proposal.

In order to allow you to make a more informed decision when deciding how to vote for this proposal, we include two relevant publications below (1) “Shareholders Are Right To Ask Microsoft Questions,” and (2) “The Global Network Initiative: A Quiet Risk for Free Expression?”

---

## I. Shareholders Are Right To Ask Microsoft Questions

(Internal links available at [https://www.realclearmarkets.com/articles/2025/10/06/shareholders\\_are\\_right\\_to\\_ask\\_microsoft\\_questions\\_1138983.html](https://www.realclearmarkets.com/articles/2025/10/06/shareholders_are_right_to_ask_microsoft_questions_1138983.html).)

When investors ask serious questions about corporate practices, they deserve more than a brusque dismissal. Yet that appears to be how Microsoft responded to a shareholder proposal filed by the National Center for Public Policy Research (NCPFR). (Microsoft's answer came in the form of an opposition statement to the proposal, which is on file with the author of this op ed.)

The proposal sought basic transparency about the company's European Security Program and its potential implications for political expression. Instead of engaging, Microsoft waved away the concerns, insisting that it "fail[s] to see" how its activities could chill free speech. That answer is not good enough.

The shareholder proposal at issue was straightforward. It asked Microsoft to clarify whether its work in Europe—particularly in partnership with governments and nongovernmental organizations—could expose the company to pressures that would compromise viewpoint neutrality. Shareholders should be told what safeguards exist to prevent European-style speech restrictions from influencing how Microsoft's technology is employed. The proposal did not ask the company to change its business model or stop protecting customers from cyberattacks. It asked for transparency.

Microsoft's opposition statement seemed designed to shut down the conversation rather than open it. The company appeared to assert that defending against cyberattacks is unrelated to free expression, as though the two issues exist in isolation. But investors know that the line between cybersecurity and speech regulation is not always so neat. Authoritarian regimes, and even democratic governments, sometimes justify censorship under the banner of "safety" or "security." That is why shareholders are right to ask how Microsoft ensures that its partnerships in Europe do not bleed into viewpoint discrimination.

There are reasons for concern. Independent watchdogs have flagged Microsoft for ideological bias in how it evaluates and manages content. Reports from the 1792 Exchange (here and here) and Alliance Defending Freedom's Viewpoint Diversity Score project (here) point to a pattern of one-sided decision-making that tends to disfavor conservative or dissenting perspectives. Then there are the House Judiciary Committee subpoenas from earlier this year related to apparent corporate involvement, including Microsoft, in censorship of U.S. citizens at the behest of foreign governments. None of this proves that

---

the company's European programs are censorious. But it does demonstrate a track record that justifies scrutiny.

Equally troubling is Microsoft's lack of engagement with NCPPR, the shareholder proponent of the proposal. While SEC rules contemplate corporate engagement with proposal proponents, and Microsoft's own public disclosures tout its commitment to engaging with shareholders, Microsoft never engaged NCPPR on this matter beyond sending its opposition statement. (Elsewhere, Microsoft states: "Effective corporate governance includes regular, constructive conversations with our shareholders to proactively seek shareholder insights and to answer shareholder inquiries.") If Microsoft is confident its programs pose no risk to free expression, why not walk NCPPR through its reasoning? Why not demonstrate safeguards? Silence only invites suspicion.

Then there is Microsoft's reliance on the Global Network Initiative (GNI) as a proxy for accountability. In its opposition statement, the company pointed to its founding membership in GNI as evidence that it takes free expression seriously. Yet shareholders are entitled to ask whether GNI oversight is sufficient. Where are the conservative voices in that process? Does the initiative provide real ideological diversity, or does it reinforce the same perspectives shareholders are already concerned about? All these concerns could ultimately be unfounded, but by not engaging NCPPR directly Microsoft just fosters suspicion.

To be clear, no one is disputing the importance of cybersecurity. Protecting citizens and institutions from digital threats is a vital service. Nor is anyone claiming to have definitive proof that Microsoft's European Security Program will inevitably be repurposed to include censorship. NCPPR would welcome evidence that these fears are unfounded. But the absence of such evidence—combined with the company's seemingly dismissive response only underscores the need for greater transparency. For example, the proposal specifically references two concerning organizations that tout their commitment to combatting "online hate speech" and "harmful content" directly identified by Microsoft as participating in the program, but Microsoft either ignores the substance of those concerns or ignores the named entity entirely.

Shareholders are not asking for micromanagement of Microsoft's operations. They are asking for accountability on a matter that goes directly to reputational and financial risk. If Microsoft were found to be complicit in ideologically driven censorship abroad, the fallout could significantly damage shareholder value. As NCPPR notes in its proposal, Facebook lost roughly \$134 billion in market value in connection with the Cambridge Analytica scandal. Transparency is the best protection against that outcome.

Microsoft's leadership had an opportunity to reassure investors by addressing the proposal seriously. Instead, it chose to minimize the issue and rely on vague appeals to trust. That

---

may be expedient in the short term, but it is shortsighted in the long run. A company of Microsoft's size and influence cannot afford to appear indifferent to legitimate shareholder concerns about free expression.

The path forward is simple: engage with critics, demonstrate safeguards, and commit to viewpoint neutrality in all partnerships. If Microsoft is as confident as it claims, it should have nothing to hide. Until it does so, shareholders are right to keep asking hard questions.

## II. **The Global Network Initiative: A Quiet Risk for Free Expression?**

How companies may be complicit in censoring legitimate speech through their GNI Membership

(Internal links available at <https://dustindevito.substack.com/p/the-global-network-initiative-a-quiet> .)

Many companies have leaned on their association with the Global Network Initiative (GNI) to reassure stakeholders that their products aren't being used to censor legitimate speech. On its face, that sounds comforting. After all, who could object to an organization that claims to be a "multistakeholder collaboration to protect freedom of expression and privacy in tech"?

But scratch beneath the surface, and a more complicated picture emerges.

### **The Precedent: GARM**

This isn't the first time major corporations have used industry groups as cover. Many companies that claim to champion free speech were previously members of the Global Alliance for Responsible Media (GARM). This "responsible media" group which was publicly aiming to counteract "harmful content" was privately working to censoring mainstream perspectives online.

GARM's brand safety framework demonetized or suppressed content it deemed to:

- Spread "hate speech" or "misinformation"
- Discuss "debated social issues in a negative or partisan context"
- "Vilif[y]" individuals based on sexual orientation or gender identity

In practice, that meant legitimate speech from mainstream voices, including The Federalist, The Daily Wire, and The New York Post, was flagged and suppressed. GARM members were, at minimum, complicit in this censorship.

### **Enter: The Global Network Initiative (GNI)**

Although the GNI's framework differs from GARM's, the outcome is not necessarily distinct. The GNI is governed by its Principles on Freedom of Expression and Privacy, which,

---

according to its website, “provide high-level guidance to the tech industry on how to respect, protect, and advance users’ rights” when governments impose demands or restrictions.

These principles are “based on internationally recognized laws and standards for human rights”, including:

- The Universal Declaration of Human Rights (UDHR)
- The International Covenant on Civil and Political Rights (ICCPR)
- The International Covenant on Economic, Social and Cultural Rights (ICESCR)

The application of GNI’s principles is further informed by:

- The UN Guiding Principles on Business and Human Rights (UN Guiding Principles)
- The Protect, Respect, and Remedy Framework
- OECD Guidelines for Multinational Enterprises

On the surface, these documents contain boilerplate human-rights language no one opposes. However, hidden in some of these documents is a catch.

### **The “Other Status” Clause**

Documents like the ICCPR and ICESCR prohibit discrimination on grounds such as race, sex, religion, but also “other status.” This vague phrase has, in recent years, been interpreted to include gender identity.

In practice, this means speech challenging gender ideology could be construed as discriminatory under GNI’s guiding framework. And if GNI members, like Google or Microsoft, are bound to these interpretations, they may end up censoring lawful, legitimate viewpoints simply because they cut against prevailing progressive norms.

It is also worth noting that GNI’s internal Code of Conduct explicitly recognizes gender identity as a protected category.

### **Case Study 19: LGBT Apps in Asia**

In case anyone thinks this is hyperbolic, GNI’s own materials illustrate this risk. In its 2018/2019 report, *The GNI Principles at Work*, GNI highlighted real-world case studies on freedom of expression and privacy challenges in the Information and Communication Technology (ICT) sector, showing how governments and companies interact in ways that affect human rights online. This report uses real-world examples, including censorship requests, surveillance demands, and content removals, to illustrate the application of the Global Network Initiative Principles.

---

Case Study 19 provides a great example of how GNI Principles could influence the decisions of major tech companies. This case involves governments in Asia requesting the removal of 65 LGBT-related applications, including dating services and community platforms, from app stores. According to the company that received the government request for takedown, it came with a threat of police action and blocking the company from operating in the country.

To avoid this scenario, the company applied a step-by-step review for each app:

1. Has this app violated any developer content policies or terms of use?
2. Has the content from this app directly violated any local laws, including obscenity laws?
3. If there are any identified issues, can they be corrected by the app developer?
4. What impact would the removal of the app have on human rights?

In short, some apps were removed for violating company policies or obscenity laws, but many remained since the company “identified freedom of expression and association as key issues at stake”.

GNI frames this case study as a vindication of its Principles and a victory for the LGBT community. While the case study does not explicitly state it, the takedown request contravened international law and the GNI Principles by discriminating against individuals based on their “gender identity” - an area safeguarded under the ICCPR’s and the ICESCR’s “other status” provision.

This framing is revealing: GNI recognizes “gender identity” as a real ontological category, the acknowledgement and protection of which is essential to the advancement of human rights. Therefore, when a government restricts transgender content, according to the GNI Principles, this would be discriminatory. Pre-emptively labeling content that challenges the concept of gender identity as discriminatory and in violation of international law contributes to a climate where those who do not believe in modern gender ideology are unable or unwilling to respectfully voice dissent for fear of online, legal, or physical consequences.

### **Following the Money**

Finally, it’s worth noting that the GNI has received funding from George Soros’ Open Society Foundation and is currently supported by the Ford Foundation, two organizations well known for advancing progressive political causes.

This doesn’t automatically discredit the GNI. But it does raise questions about ideological leanings and whether its guidance to members reflects a genuinely neutral defense of expression or the advancement of a particular worldview.

---

## **A Solid Yellow Flag**

Here's the concern: as long as the GNI's framework is grounded in human rights treaties that include the elastic phrase "other status," there is no guarantee that its members won't use or be complicit in their services censoring legitimate speech.

The risks of using GNI's framework are not as obvious as the risks of using GARM's were (for those who read its Brand Safety Framework anyway). But risks are there all the same. So when companies raise their GNI membership as a defense from concerns over censorship, stakeholders should not back off from pressing for clarity.

Membership in the Global Network Initiative should not reassure us that companies are not censoring speech, but it also should not make us panic. For now, it should raise a solid yellow flag.

THE FOREGOING INFORMATION MAY BE DISSEMINATED TO SHAREHOLDERS VIA TELEPHONE, U.S. MAIL, E-MAIL, CERTAIN WEBSITES AND CERTAIN SOCIAL MEDIA VENUES, AND SHOULD NOT BE CONSTRUED AS INVESTMENT ADVICE OR AS A SOLICITATION OF AUTHORITY TO VOTE YOUR PROXY.

THE COST OF DISSEMINATING THE FOREGOING INFORMATION TO SHAREHOLDERS IS BEING BORNE ENTIRELY BY THE FILERS.

THE INFORMATION CONTAINED HEREIN HAS BEEN PREPARED FROM SOURCES BELIEVED RELIABLE BUT IS NOT GUARANTEED BY US AS TO ITS TIMELINESS OR ACCURACY, AND IS NOT A COMPLETE SUMMARY OR STATEMENT OF ALL AVAILABLE DATA. THIS PIECE IS FOR INFORMATIONAL PURPOSES AND SHOULD NOT BE CONSTRUED AS A RESEARCH REPORT.

**PROXY CARDS WILL NOT BE ACCEPTED BY US. PLEASE DO NOT SEND YOUR PROXY TO US. TO VOTE YOUR PROXY, PLEASE FOLLOW THE INSTRUCTIONS ON YOUR PROXY CARD.**

For questions regarding Microsoft Corporation – Proposal 5 – “European Security Program Censorship Risk Audit,” sponsored by National Center for Public Policy Research, please contact Stefan Padfield, Executive Director, Free Enterprise Project, NCPPR, via email at [spadfield@nationalcenter.org](mailto:spadfield@nationalcenter.org).