# Open Measurement Gatherings (OMG)

Convening 4
Public Report

Photo Credit: Melissa Newcomb (M-Lab)

M-Lab · IODA · OONI · CS&S Code for Science & Society · Censored Planet · Open Technology Fund

# Introduction

From 2024 to 2025, Measurement Lab organized four convenings called **Open Measurement Gatherings (OMG)** with Censored Planet, IODA, and OONI. The intention of these convenings was to build understanding, trust, and collaboration across open Internet measurement groups and this initiative was made possible with the support of the Open Technology Fund (OTF).

## Review of OMGs 1-3

The first two convenings in 2024 took place in Atlanta, Georgia at Georgia Tech where the IODA team generously hosted the OMG groups (OMG 1 June 11-13; OMG 2 December 10-12, 2024). The intention was to have the subsequent two convenings in Ann Arbor, Michigan hosted by the Censored Planet team. However, several factors in 2025 compelled the OMG groups to switch formats for the following convenings. The third convening (June 25, 2025) was held virtually and featured public presentations from each OMG group. The fourth convening was held in Estoril, Portugal following joint programs run by the OMG groups at the Global Gathering conference.

## OMG 4

From September 8-12, 2025, the OMG groups gathered in Estoril, Portugal. From Sept 8-10 they hosted an Open Measurement Village at the Global Gathering (GG). At the Village, OMG groups took turns hosting a booth, circle discussions, and a game called "Are You My Measurement Tool?" to help compare the use cases and data of each OMG group's measurement tool. Based on the feedback from the GG community, the OMG groups created the OMG User Guide (Appendix C) as a public resource to help users determine which measurement tool they should use or how to compare data from OMG groups.

Balancing innovation in Internet measurement with accessibility is a key challenge that came up throughout the Global Gathering. Open measurement groups must keep up with increasingly sophisticated Internet interference while educating the non-technical community. Another takeaway the OMG groups had was that smaller sessions would be more beneficial if tailored to the interests or technical level of user groups. While it is important that these user communities interact, when soliciting feedback or generating collaborative ideas it seemed that distinct sessions for technical level would have been more beneficial and effective. Overall, the OMG groups learned that to get the most out of hosting programs at future global conferences is to focus on holding joint booths and one or two "main event" sessions advertised to all participants. For more details from sessions at the Open Measurement Village refer to section, The OMG Groups Host The Open Measurement Village at Global Gathering. For the Open Measurement Village program, refer to Appendix A.

> *Balancing innovation in Internet measurement with accessibility is a key challenge that came up throughout the Global Gathering.*

Following the Global Gathering, the OMG groups remained in Estoril from September 11-12 to reflect on community feedback, the previous OMG convenings, share updates, and strategize on how to continue the momentum to deepen collaboration following the completion of the OTF-funded program.

Throughout the fourth convening three themes emerged: that OMG groups face shared challenges, to counter those challenges we need to increase coordination, and to continue the work the open measurement groups must become sustainable. The section OMG 4 Key Takeaways goes into more details about the three themes. For a comprehensive summary of all the OMG internal sessions, refer to section Open Measurement Gathering 4. For the full agenda, refer to Appendix B.

## Impact of the OMG Program

The OMG convenings deepened mutual understanding among the groups about each platform, tools, data pipelines, and user groups. Most importantly though, these convenings deepened the interpersonal relationships across OMG groups and built trust so that OMG groups can hold joint public events, preview upcoming changes, problem solve together, and strategize for the future of open measurement to meet a moment of unprecedented challenges. These convenings developed a default habit to collaborate, incorporate data across groups, and build collective awareness of each group with our users. Going forward, the OMG groups have several actionable, short and long term plans to continue collaboration. Despite reduced resources, open measurement matters now more than ever given current global trends in policy and technology.

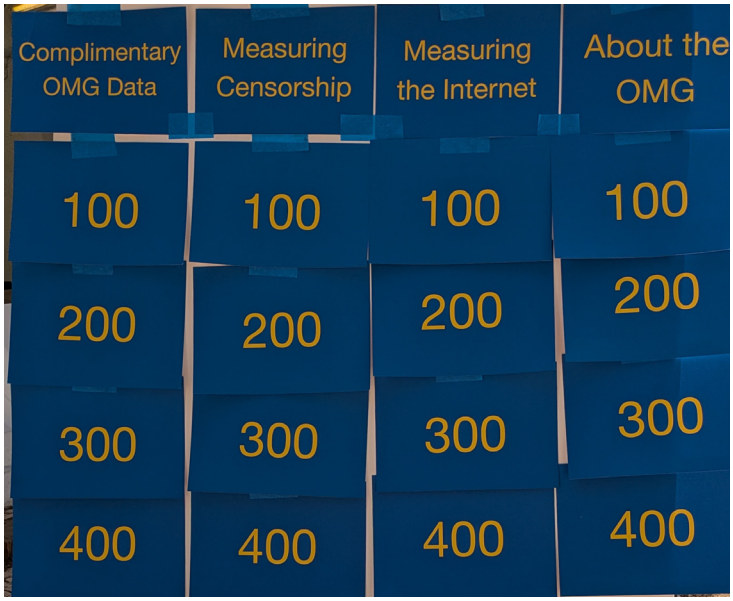
> *Despite reduced resources, open measurement matters now more than ever given current global trends in policy and technology.*

# The OMG Groups Host The Open Measurement Village at Global Gathering

## Global Gathering Sessions

**Are you my measurement tool? (Days 1 and 2)**

In preparation of the Open Measurement Village, the OMG groups created a user guide in the form of a table to help the community better compare open Internet measurement tools and datasets by use-case. To refine the user guide at the Global Gathering, the OMG groups designed a Jeopardy! inspired game, Are You My Measurement Tool? Amanda Meng from IODA facilitated two sessions of the game with support from other OMG group members.




Overall, participants found the user guide table very helpful and enjoyed playing the game. Some participants found the use cases too generic and wanted more in-depth scenarios. Some users were experts in open Internet measurement, while others had more policy or advocacy background. Some participants wanted to know more about why certain tools or

datasets were applicable in each use case.

To address the feedback from the community, the OMG groups added context to the user guide. In the future, depending on resources, OMG groups have ideas to create more interactive and detailed user guides tailored to the technical level of the user community. The OMG User Guide is in Appendix C. The OMG groups intend to iterate on the Are You My Measurement Tool? for future events.

**Fighting Internet Censorship: Challenges and Needs (Day 1)**

The second circle of day one at Global Gathering focused on what the community needs to counter online censorship and was facilitated by Maria Xynou and Elizaveta Yachmeneva from OONI. The most cited challenge was the difficulty for the user community to find relevant data and interpret it. The question of making data accessible relates to the user experience and communications challenge in countering censorship. News articles about censorship or Internet outages often misinterpret data and/or lack nuance. Most news communications are designed for people to read the first paragraph and nothing else.

Lastly, a shared challenge is the funding landscape. Funders often want to see "new" tools, features, or methodologies. Few funders are interested in sustaining projects or funding maintenance. It requires the open Internet measurement community to constantly innovate to maintain the interest of donors, which puts pressure on the day-to-day maintenance of platforms.

**Internet Measurement Wish List (Day 1)**

This session was also facilitated by Elizaveta Yachmeneva from OONI. Only a few participants joined this circle, allowing for an in-depth discussion with long-term OONI users on recent updates.

**Emerging trends and threats in Internet measurement (Day 2)**

On the second day of the Global Gathering, Melissa Newcomb (Measurement Lab) facilitated a session to discuss longer term trends and threats in Internet measurement. The participants also discussed emerging threats to digital rights in general.

**Critical emerging threats to digital rights:**

- The funding landscape has changed dramatically in the last year. The loss of key public-sector funders in the United States will weaken civil society networks and overall negatively impact the Internet freedom movement. At the same time, private-sector funding is becoming increasingly militarized with a heavy focus on Artificial Intelligence.
- Surveillance is increasingly being justified through claims to protect children but has far reaching implications for other populations.
- Commercial VPNs are not necessarily trust-worthy. Auditing requires collaboration, and the industry is reluctant to provide the transparency necessary. However, OONI Probe can measure VPN blocking.

**Key trends in Internet measurement:**

- Actors causing shutdowns are denying them, conducting "micro" shutdowns and communications blackouts which make it difficult to hold them accountable.
- The need to translate sophisticated technical shutdowns so that they are easily understood by the public.
- Potential solutions include looking into

DNS data and collaborating with VPNs, especially open source projects.

**Options to resist threats to digital rights and Internet freedom:**

- Supporting community driven Internet infrastructure.
- Advocating to businesses the economic losses caused by Internet shutdowns.
- Open source projects that can facilitate communication even during a censorship or shutdown, such as Project Ainita.
- Recognition that funders may not be aligned with the mission of Internet freedom and how to protect digital rights during collaboration.

**Internet Censorship Research Questions and Ideas (Day 2)**

During this session facilitated by Maria Xynou and Elizaveta Yachmeneva from OONI, participants shared their areas of interest for research and collaboration. Major themes included:

- How to track the downgrading of networks (e.g from 4G to 2G) rather than shutdowns and network level throttling.
- Transnational censorship and how information controls transfer across countries.
- The collateral damage of censorship and how it impacts cloud providers.
- Projects to conduct open source mapping of cell towers across countries.
- Blocklists and whitelists: who forms them, how they're shared, etc.
- Algorithmic censorship, AI-formed blocklists, and the challenges to research.

As part of this session, participants discussed the above themes, brought examples of how these specific issues are relevant to their countries/regions, and discussed the challenges and need for related research.

# Open Measurement Village Key Takeaways

In different sessions, a key challenge that came up several times was the **need to balance innovating Internet measurement techniques with accessibility for public use**. As Internet censorship becomes increasingly sophisticated, so too are the detection methodologies. However, as the open Internet measurement tools innovate to keep up with censorship techniques, how do we educate the community or make the data accessible to less technical audiences? OMG groups do not yet have an answer for this question, but it is an issue each group is facing.

Another takeaway the OMG groups had was that smaller sessions were more beneficial if tailored to user groups. For example, the **needs of expert users of open measurement tools are very different from the needs of advocacy and policy groups**. Similarly, users with technical backgrounds found the scenarios of the Are You My Measurement Tool? not detailed enough to meet their questions. While it is important that these user communities interact, when soliciting feedback or generating collaborative ideas it seemed that distinct sessions based on technical level would have been more beneficial and effective.

Overall, the OMG groups learned that to get the most out of the Global Gathering or future conferences is to focus on holding joint booths and one or two "main event" workshops or sessions advertised to all participants

that would attract larger numbers. In larger workshops, OMG groups can more effectively scope activities for varied levels of expertise of participants. By having one or two larger joint events, rather than several smaller sessions, it would allow the OMG groups more time network and connect with fellow attendees. Going forward, the OMG groups will coordinate to co-host events at future regional and international events in addition to hosting public events online.

# Open Measurement Gathering 4

## OMG 4 Key Takeaways

Following the Global Gathering, members of the OMG group remained in Estoril to hold internal meetings over two days. Throughout the convening three themes emerged: OMG groups face shared challenges, to counter those challenges OMG groups need to increase coordination, and to continue the work the open measurement groups must become sustainable.

### Shared Challenges

From the tactical day-to-day to the broader trends in politics and industry– the OMG groups noted they face similar challenges. The biggest shared challenge among the OMG groups was that each one is **trying to achieve a lot with limited resources**. The OMG groups determined that they should narrow their scope to focus on what is most important and include maintenance and operational costs in their budgets. OMG groups also discussed how to better share resources, especially with research institutions.

### Increase Coordination

Following the discussion on challenges, the OMG groups outlined action plans for increased coordination. In the short term, OMG groups will create cross-org communication channels, thematic working groups, regular virtual engagements (external and internal), as well as establish a centralized hub for sharing knowledge resources with the open measurement community.

In the long term, OMG groups are interested in hosting OMG events on the sidelines of major conferences, conducting joint research studies, creating complementary data sets, pooling resources, building the capacity of global digital rights researchers, and creating a more detailed OMG tool to help people navigate the various Internet measurements. Overall, OMG groups will leverage existing partnerships to support open measurement.

### Open Measurement Sustainability

Despite the much lower available resources, open measurement matters now more than ever given current global trends in policy and technology. OMG groups determined that strategies for overall sustainability should focus on impact rather than discreet activities. To achieve impact as well as gain interest, OMG groups determined that they should combine trends in the field with open Internet measurement initiatives to continue the work. Refer to Strategies for Sustainability for more details.

Data is both a strength and vulnerability for OMG groups. The data presents opportunities for analysis, insights, and storytelling. Each group has large amounts of data, each representing different aspects of the Internet. If combined, the OMG groups could have a compelling and valuable open data resource that holistically represents the Internet. However, the cost to host data and make it publicly available will only increase, an issue

each OMG group will have to face. In addition, shrinking civic space and strained OMG teams threaten the ability to report on Internet censorship events. The OMG groups agreed on the following priorities for sustainability:

**Strategic**

- Combine AI trends with open measurement work
- Align priorities and focus scope of work to be proactive
- Raise visibility of impact

**Data**

- Increase compatibility of data across OMG groups
- Determine long term data storage and security
- Increase efficiencies for data pipelines and resources
- Generate insights from the data
- Increase capacity of global data researchers

**Resources**

- Focus on team building and cohesion
- Pool resources and diversify funding streams
- Maintain current measurement clients
- Activate and build community to bolster capacity
- Create joint partnership models

# OMG 4 - Day 1

For the first session of day one, the OMG groups shared out from the Global Gathering sessions each hosted and reflected on the process of jointly hosting the Open Measurement Village. The reflections and takeaways shared are described in the previous section of this report, Open Measurement Village Key Takeaways.

## Coordination on censorship monitoring, reporting and rapid response

The second session of day one focused on how the OMG groups could scale-up coordination in censorship monitoring, reporting, and rapid response. First, OMG groups reviewed the context they are operating in and the types of censorship events to focus on: targeted blocking and shutdowns. Major events that are known in advance, such as elections or exams, allow for preparation in advance and there are resources such as election watch lists[1]. However, there are many triggers for Internet shutdown events that are unpredictable such as coups, natural disasters, protests, wars, etc. One potential way to prepare for unexpected events is to train communities to be ready to mobilize during Internet disruptions, especially in communities with low Internet measurements. Each OMG group then shared their challenges

[1] https://www.accessnow.org/campaign/2025-elections-and-internet-shutdowns-watch/

to responding to Internet censorship events. Common issues for each group included:

- Capacity - most OMG groups have small teams and can't be available at all times to respond to questions or have the time to analyze data to confirm censorship events.
- Reliance on local partners - most Internet disruption or censorship events require local partners on the ground to verify and report. If there are no known partners in a given location, then there may be no way to verify an event has occurred.
- Unequal measurement coverage - not all locations have as much Internet measurement data to establish a baseline "normal." Without enough data, it is much harder to confidently verify a disruption occurred.
- Prioritizing impact - with so many Internet disruptions every day, OMG groups must determine which Internet censorship events should be reported on. OMG groups would benefit from agreed-upon thresholds to ensure impact in reporting.

Following the discussion on challenges, the OMG groups brainstormed potential solutions for increased coordination and accessibility to users.

- Leverage existing working groups and community spaces, such as #KeepItOn to communicate.
- Share internal data dashboards that are easier to share among trusted experts as public dashboards are being developed or improved.
- Collaborate with other existing digital helplines for rapid response support.
- Recognize how OMG groups can support or enable one another rather than duplicating effort.
- Update and add features to current open measurement tools. Each OMG group also shared options to improve usability of their tools.
- Decentralize and build the rapid-response capacity of communities to report on Internet censorship and shutdowns. This would require creating materials and conducting training.

## Demos of IODA, OONI and Censored Planet updated tools

The next session of day one included demos of new tools from IODA, OONI and Censored Planet.

## Coordinated Collaborative Censorship tracking with Aggie:

The IODA team shared a pilot project for more coordinated and collaborative censorship tracking. The pilot focuses on one specific country with a closed information environment and current and historic network interference, but the IODA team imagines expanding to include more. Aggie is short for aggregator and is an open source tool built at Georgia Tech that aggregates content from the Internet through API, RSS, etc, and enables incident tracking. Aggie users document censorship incidents and attach various data sources that support verification and confirmation of the censorship incident. Trained and trusted users search incoming data, create incidents, and track incidents through the verification, confirmation, and publication process.

Currently the project incorporates Cloudflare anomalies on 10 networks in country, IODA alerts, and selected social media accounts on

the platform X. As the project continues, it may incorporate other datasets like OONI. The long term plan is that Aggie can become a platform for coordinated censorship tracking and response. The platform relies on the community of trained and trusted users to track and identify events.

## OONI Probe Dashboard Revamp

The OONI team presented designs to update the OONI Probe dashboard to highlight auto-run, one of the most important features of OONI Probe that enables automated testing and continuous measurement coverage. Despite being a key feature, it is currently hidden in the settings. The OONI team presented proposals to emphasize auto-run on the OONI Probe dashboard, highlight how the user contributes, and make it easier to find censorship-related news or research. After the presentation, the OONI team asked other OMG groups to provide feedback about the proposed new design. OMG groups discussed how to encourage users to use auto-run while respecting user consent.

## Censored Planet Dashboard

Censored Planet shared their updated website, general dashboard and CenAlert project.
As seen in the screenshot below, the new dashboard offers the following options and visualizations:

1. **Filter section:** Allows the user to choose the country, data source (DNS, HTTPS, HTTP, ECHO, or Discard), and a date range (up to 6 months at once).
2. **Domain selection:** Enables the user to choose up to 10 domains at once. The dropdown organizes domains based on their website categories from the Citizen Lab test lists.
3. **Probe count column:** Displays the number of measurement probes in the database for the given domain and subnetwork targeted in the measurements.
4. **Unexpected rate column:** Displays the proportion of measurement probes that detected any kind of interference for the given domain and subnetwork.
5. **Outcome Timeline plot:** Provides an aggregated visualization of measurement results grouped by date and classified outcome.
6. **Outcome per Network plot:** Provides an aggregated visualization of measurement results grouped by network, subnetwork, and classified outcome.

Censored Planet also previewed CenAlert, which is still in development. CenAlert uses Google trends data to detect censorship searches using keywords. The CP team went through previously reported censorship events over the past 10 years to create the anomaly tags. Future reporting of events not detected by CenAlert would require manual input.

Each measurement gets a T/F for if it's expected and there is a control measurement and 5 trials. If all or majority match the expected response, then there is a flag if the measurement is unexpected or not. If not expected, the result is divided by how many measurements. In the future, CenAlt will run every day and analyze the data the next day. The CP team plans to fill in more information and improve the UI throughout 2025.

## Day to Day Challenges

For the fourth session of the day, participants broke out into small groups with members of other OMG groups to share the day-to-day

# Censored Planet

Country 1 Colombia | Source HTTPS | Start Date 22.10.2025 | End Date 12.11.2025

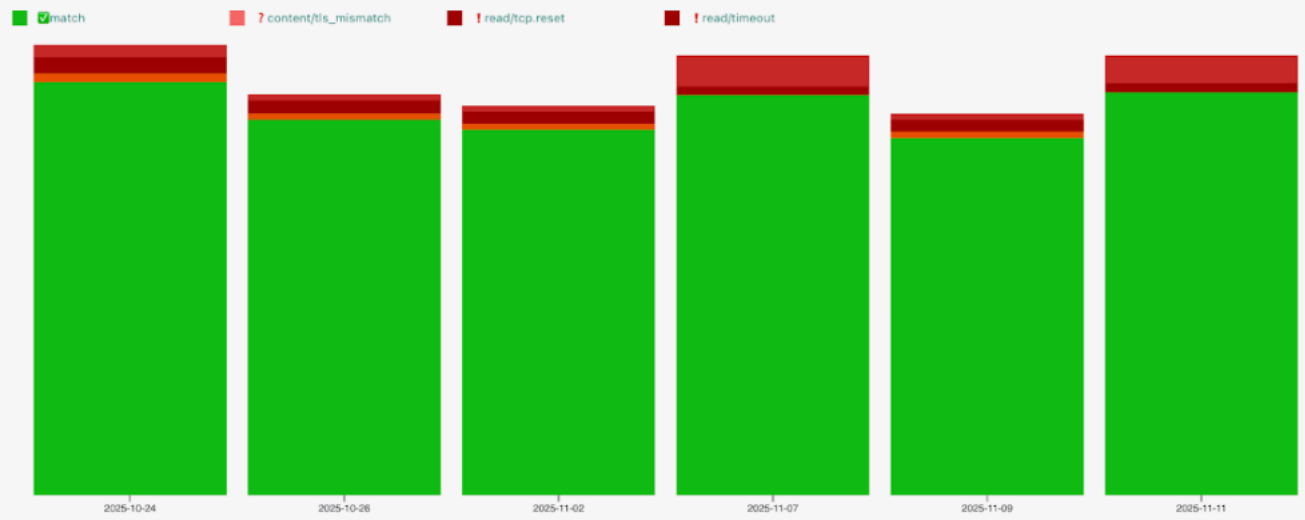
2 Domains: psiphon.ca | www.torproject.org | www.wikipedia.org | www.hrc.org | www.youtube.com | bbc.com | www.occrp.org | www.pornhub.com | facebook.com | www.instagram.com

Search

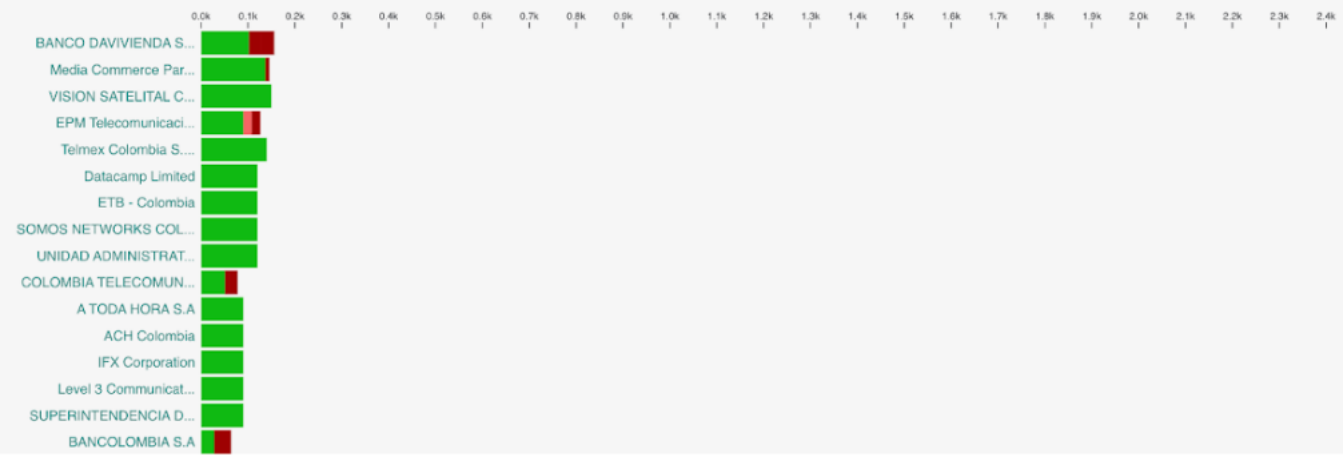
Search 470 results

| domain | category | network | subnetwork | 3 probe_count | 4 unexpected_rate |
|---|---|---|---|---|---|
| www.youtube.com | Media sharing | BANCOLOMBIA S.A | AS27989 - Bancolombia S.A | 12 | 100% |
| www.instagram.com | Social Networking | BANCOLOMBIA S.A | AS27989 - Bancolombia S.A | 12 | 100% |
| www.torproject.org | Anonymization and circumventio... | BANCOLOMBIA S.A | AS27989 - Bancolombia S.A | 12 | 100% |
| www.youtube.com | Media sharing | BANCO DAVIVIENDA S.A | AS263199 - Telmex Colombia S.A. | 27 | 100% |
| facebook.com | Social Networking | COLOMBIA TELECOMUNICACIO... | AS3816 - Itau Corpbanca Colom... | 9 | 100% |
| www.instagram.com | Social Networking | COLOMBIA TELECOMUNICACIO... | AS3816 - Itau Corpbanca Colom... | 9 | 100% |
| www.pornhub.com | Pornography | Media Commerce Partners S.A | AS27951 - Media Commerce Par... | 9 | 100% |
| www.youtube.com | Media sharing | COLOMBIA TELECOMUNICACIO... | AS3816 - Itau Corpbanca Colom... | 9 | 100% |
| www.instagram.com | Social Networking | BANCO DAVIVIENDA S.A | AS263199 - Telmex Colombia S.A. | 27 | 100% |
| psiphon.ca | Anonymization and circumventio... | EPM Telecomunicaciones S.A. E.... | AS13489 - EPM Telecomunicaci... | 10 | 90% |
| www.pornhub.com | Pornography | EPM Telecomunicaciones S.A. E.... | AS13489 - EPM Telecomunicaci... | 10 | 90% |
| www.torproject.org | Anonymization and circumventio... | EPM Telecomunicaciones S.A. E.... | AS13489 - EPM Telecomunicaci... | 10 | 90% |
| facebook.com | Social Networking | EPM Telecomunicaciones S.A. E.... | AS13489 - EPM Telecomunicaci... | 11 | 81.82% |
| www.torproject.org | Anonymization and circumventio... | MERCANET LTDA | AS27810 - Mercanet Ltda | 4 | 75% |
| psiphon.ca | Anonymization and circumventio... | MERCANET LTDA | AS27810 - Mercanet Ltda | 5 | 60% |
| www.instagram.com | Social Networking | MERCANET LTDA | AS27810 - Mercanet Ltda | 5 | 60% |
| facebook.com | Social Networking | MERCANET LTDA | AS27810 - Mercanet Ltda | 5 | 60% |
| www.pornhub.com | Pornography | MERCANET LTDA | AS27810 - Mercanet Ltda | 5 | 60% |
| www.occrp.org | News Media | PIT COLOMBIA SAS | AS272806 - M&B Soluciones Per... | 5 | 60% |

## Outcome Timeline 5




## Outcome per Network 6



challenges each organization faces. While each person had a unique perspective, some general themes emerged for the OMG groups.

- Remote and globally distributed teams
  - Different time zones, isolated work time, and many demands can make it hard for teams to feel connected or work together effectively.
- Resource Sustainability
  - All OMG groups agreed they have too much work and not enough people, with most team members multi-tasking and taking on responsibilities outside their area of expertise.
  - Fundraising and donor management requires time and capacity, sometimes from team members who are not specialists in that field.
  - To keep operational costs down, many OMG group staff are contractors who have less stability and most OMG groups do not have operational teams to support finance, human resources, or other aspects of organizational and staff well-being.

- Balancing productivity, priorities, and well-being
  - Workflows can be unstable and unpredictable, leading to burn out. OMG groups have high impact goals and missions, but limited resources to achieve them.
  - Most teams have single points of failure, which means that if one person is out for an extended period of time then projects cannot move forward.
  - Keeping up with the maintenance and troubleshooting often means sacrificing innovating new features.

- Managing user communities
  - In order for contributors to meaningfully support OMG groups they have to have high levels of expertise or take time to develop the technical skills. This makes it difficult for users to contribute easily.
  - OMG groups sometimes must support and navigate communities that may have conflicts, different needs or threat models, and various levels of risks. Balancing the needs and context of each user community can be difficult.

**Main Takeaways**

The biggest shared challenge among the OMG groups was that each one is trying to achieve a lot with limited resources. The OMG groups determined that they should narrow their scope to focus on what is most important and include maintenance and operational costs into their budgets. OMG groups also discussed how to better share resources, especially with research institutions.

# OMG 4 - Day 2

On day two of the Open Measurement Gathering, the participants focused on assessing the current operational landscape and creating action plans to collaborate and meet shared challenges.

**Strategies for Sustainability**

OMG groups reviewed the current funding landscape, most notably the shift in U.S. foreign policy priorities and loss of funding for Internet freedom initiatives. At present, there is no single equivalent to replace U.S. government funding. Despite much lower available resources, open measurement matters now more than ever given current global trends in policy and technology. OMG groups determined that strategies for overall sustainability should focus on impact

rather than discreet activities.

To achieve impact as well as gain interest, OMG groups determined that they should combine trends in the field with open Internet measurement initiatives to continue the work. OMG groups mapped out thematic and technical areas of focus to include:

**Thematic**

- Democracy
- Cybersecurity
- Measurement
- Networking
- AI

**Technical**

- Data Resiliency
- Data Volume
- Data Science
- Information Products
- Technical Support

This is a working list of ideas that the OMG groups will continue to refine to develop and connect to create comprehensive programs that meet the interests of the public and support open measurement initiatives.

### Strengths, Weaknesses, Opportunities, and Threats (SWOT) Analysis

Building on the previous day's exercise sharing challenges and the Theory of Change exercise from OMG 2, the participants of OMG 4 conducted an interactive SWOT analysis in small groups. Each group moved through stations to discuss and write down the Strengths, Weaknesses, Opportunities and Threats to open measurement and what priorities should be. A summary table of the analysis is below.

### SWOT Analysis Themes and Future Priorities

When the breakout groups reconvened, some key themes emerged. The lack of stable funding came up in several of the discussions. It is critical that all OMG groups become more

**Strengths**

- Passion for the mission
- Abundance of open access data
- Expertise and technical breadth
- A diverse global community including research students
- Trust across OMG groups

**Weaknesses**

- Small overstretched teams
- External communications
- Stuck in reactive rather than proactive mode
- Data is hosted differently by each OMG group and with different taxonomy
- Lack of stable funding
- Asymmetric capacity and power compared to industry and governments
- High turnover among research students

### Opportunities

- Pursue projects that combine open measurement and AI
- Focus on outreach and communications
- Pursue funding jointly
- Leverage one another's partnerships
- Increase collaboration among OMG groups for storytelling and media
- Create complementary datasets
- Monetize aspects of projects to generate revenue

### Threats

- A sudden shift and reduction in the funding landscape
- Rise of authoritarianism globally
- Dominance of AI for attention and funds
- Shrinking civic space for digital rights
- Complexity of Internet censorship and blocks increasing
- Apps becoming entry point of Internet, with embedded censorship and lack of transparency

proactive and that organizations are more resilient so that the collapse of one institution or donor does not bring down the entire open measurement group or broader ecosystem. OMG groups characterized AI and its impact as both a threat and an opportunity. Unlocking partnerships and increasing the capacity of the open measurement community could solve the lack of human resources.

Lastly, data is both a strength and vulnerability for OMG groups. The data presents opportunities for analysis, insights, and storytelling. Each group has large amounts of data, each representing different aspects of the Internet. If combined, the OMG groups could have a compelling and valuable open data resource that holistically represents the Internet. However, the cost to host data and make it publicly available will only increase, an issue each OMG group will have to face. In addition, shrinking civic space and strained OMG teams threaten the ability to report on Internet censorship events.

Based on the SWOT analysis, the OMG groups came up with the following priorities:

**Strategic**

- Combine AI trends with open measurement work
- Align priorities and focus scope of work to be proactive
- Raise visibility of impact

**Data**

- Increase compatibility of data across OMG groups
- Determine long term data storage and security
- Increase efficiencies for data pipelines and resources
- Generate insights from the data
- Increase capacity of global data researchers

**Resources**

- Focus on team building and cohesion
- Pool resources and diversify funding streams
- Maintain current measurement clients
- Activate and build community to bolster capacity
- Create joint partnership models

**Hands On Data Sessions**

Following the SWOT analysis, the OMG groups held a hands-on data session. OONI and IODA shared the status of their methodologies for identifying throttling events. OONI's methodology for measuring targeted cases of throttling (such as the throttling of YouTube) involves the analysis of timing information during HTTPS requests in Web Connectivity data. IODA's methodology develops a measure for latency and probe response/loss based on IODA's Active Probing signal. For both OMG groups, the biggest challenge is distinguishing between intentional throttling and congestion.

In addition M-Lab shared recent internal analysis to better understand how M-Lab data can identify interference events. The M-Lab team focused on three events in the last two years and potential signals in the data include user behavior (increase or decrease in number of tests per region) or measurement indicators such as changes in throughput or discrepancies between networks within the same area. A major challenge for using M-Lab data to detect Internet censorship or shutdowns is that the platform does not have servers placed in every country and there is a 24 hour delay in processing the data.

**Reflections on the Open Measurement Gatherings and Action Items for Next Phase of OMG**

For the final session of OMG 4, participants reflected on the OMG program and discussed action plans for continuing collaboration. The program increased trust and solidarity between OMG groups. Participants noted that hosting a joint booth at RightsCon 2025 and an open measurement program at the Global Gathering were major milestones in collaboration made possible by the teambuilding facilitated during the OMG convenings. In addition, the OMG convenings helped the groups realize they could preview platform changes and share challenges with one another which led to joint problem solving.

Going forward, OMG groups identified short and long term action plans to continue collaboration. Short term plans that groups can execute include:

- Online engagement and connection, such as an annual external event, more frequent internal OMG meetings on a regular basis, and creating a "help desk" for the open measurement community (which has aready been created on the public OONI Slack).
- Knowledge resources, creating a website to host resources, reports, and future materials.
- Establish working groups, featuring members of each OMG group based on themes such as research or operations.

In the longer term, OMG groups are interested to pursue:

- OMG events and meetings on the sidelines of other major conferences.
- Joint research and case studies.
- Complementary and more efficient datasets.
- Capacity building of global digital rights researchers.
- Sharing partnerships and networks.
- An OMG toolkit or chat bot to help people navigate the various Internet measurements. datasets and more easily figure out which one to use for which scenario.

# Conclusion

Over the last two years, the OMG groups deepened their interpersonal relationships, operational familiarity, and developed a sense of solidarity that is difficult to cultivate among globally distributed organizations. OMG groups better understand how each of their open measurement tools are complementary, demonstrated by the OMG User Guide (Appendix C).

OMG groups will continue collaborating and supporting one another through a challenging time in Internet freedom. We will continue hosting joint public events, internal meetings, and strategize for the future of open measurement. We recognize that the only way through is together and with community. The OMG groups are grateful for the support of the Open Tech Fund which made these convenings possible.

# Appendix - A

## Open Measurement Gathering (OMG) Village Program at Global Gathering (Sept 8-10, 2025)

| Global Gathering Day - Day One | |
|---|---|
| **Booth 1: OONI** | Since 2012, the Open Observatory of Network Interference (OONI) has built free software tools that empower the public to measure and collect evidence of Internet censorship. Today, thanks to the global OONI community, OONI hosts the largest open dataset on Internet censorship of its kind. Join this booth to learn all about OONI, ask questions, share feedback, and learn how you can get involved in the global fight against Internet censorship!<br><br>Website: https://ooni.org/ |
| **Booth 2: IODA** | In this booth we will showcase both the IODA interface for live demos on how to use the IODA dashboard as well as share new guides developed for less technical users on how and when to use IODA, the IODA signals, and the IODA rapid response shutdown protocol.<br><br>Website: https://ioda.inetintel.cc.gatech.edu/<br><br>IODA's booth is part of the Open Measurement Gathering (OMG) Village, which consists of the following projects/organizations: OONI, M-Lab, IODA, Censored Planet, Netalitica, and Project Ainita. Each of these organizations will have a booth slot throughout the 3-day Global Gathering event. |
| **Circle 1: Jeopardy! Are You My Measurement Tool?** | Have you ever experienced an Internet shutdown or censorship event, but then didn't know which open Internet measurement tool to turn to? Join the Open Measurement Gathering groups (Censored Planet, IODA, M-Lab and OONI) in a game of jeopardy designed to help guide you through which Internet measurement tool you need.<br>This circle aims to build the capacity of the Internet Freedom |

| Global Gathering Day - Day One | |
|---|---|
| | community to understand when to use what measurement tool to monitor and report on Internet shutdowns and censorship events. We will start with a review of when to use which tool followed by a live game show that tests and further builds knowledge, culminating and sweet rewards! Following Global Gathering, the OMG groups will release a public guide on which Internet measurement datasets to refer to depending on the type of Internet shutdown or censorship event you're investigating. |
| **Circle 2: Fighting Internet Censorship: Challenges and Needs** | What challenges have you encountered in monitoring, reporting, or advocating against Internet censorship? How can the Internet measurement community better support your efforts? Join this session to share your experiences, explore common obstacles, and discuss practical needs to strengthen global monitoring and response to Internet censorship. |
| **Circle 3: Internet Measurement Wish List** | If Internet measurement projects like OONI, IODA, M-Lab, or Censored Planet could offer you anything — what would be on your wish list? What features, data, or tools do you wish you had to better monitor Internet censorship? Join this interactive brainstorming session to share your ideas, needs, and feedback. |

| Global Gathering Day - Day Two | |
|---|---|
| **Booth 1: Censored Planet** | Censored Planet is a research lab that investigates how Internet access is being shaped and restricted around the world. As censorship tactics become more complex and harder to detect, we develop new ways to study these systems and understand who they affect. We focus on Internet measurement, network security, and privacy to produce research and tools that support journalists, civil society, and the broader Internet freedom community.<br><br>Website: https://censoredplanet.org<br><br>Censored Planet's booth is part of the Open Measurement Gathering (OMG) Village, which consists of the following projects/ organizations: OONI, M-Lab, IODA, Censored Planet, Netalitica, and Project Ainita. Each of these organizations will have a booth slot throughout the 3-day Global Gathering event. |
| **Booth 2: M-Lab** | Founded in 2009, Measurement Lab (M-Lab) is an open platform for studying Internet performance and neutrality over time. M-Lab recently completed the first phase of the Internet Quality Barometer project, and published the IQB Framework in June 2025. The IQB project seeks to redefine Internet quality beyond the single metric of speed by using available data. As M-Lab continues the IQB project to build a tool to score Internet quality, we are also interested in exploring ways to score Internet freedom with existing data. Come by our booth and share your thoughts! |
| **Circle 1: Mapping Emerging Digital Rights Threats** | What should we be measuring to prepare for the future of digital rights?<br>Based on your work and experience, what major digital rights threats do you foresee emerging globally in the next decade? And as a community, how can we prepare? Join this interactive brainstorming session to share your insights, identify measurement priorities, and help shape a collective response to the evolving digital landscape. |
| **Internet Censorship Research Questions and Ideas** | Internet measurement data is only as valuable as the questions it helps us answer. What research questions should we be asking? What insights do you hope to uncover through Internet censorship data? Join this interactive brainstorming session to share your ideas, highlight pressing research needs, and help shape the future direction of censorship measurement and analysis. |

| Global Gathering Day - Day Two | |
|---|---|
| **Jeopardy! Are You My Measurement Tool?** | Have you ever experienced an Internet shutdown or censorship event, but didn't know which open Internet measurement tool to turn to? Join the OMG groups (Censored Planet, IODA, M-Lab and OONI) in a game of jeopardy designed to help guide you through which Internet measurement tool you need. This circle aims to build the capacity of the Internet Freedom community to understand when to use what measurement tool to monitor and report on Internet shutdowns and censorship events. We will start with a review of when to use which tool followed by a live game show that tests and further builds knowledge, culminating and sweet rewards! Following Global Gathering, the OMG groups will release a public guide on which Internet measurement datasets to refer to depending on the type of Internet shutdown or censorship event you're investigating. |

| Global Gathering Day - Day Three | |
|---|---|
| *On the third day of the Global Gathering, the Open Measurement Village was open for the community to use.* | |
| **Booth 1: Netalitica** | Netalitica Booth will introduce you to the ""Test Lists Project"". We hire local researchers to update the URL test lists (aka Citizen Lab lists) of multiple countries, which are then used by network probes (e.g. OONI Probe) to uncover Internet censorship. Come to our booth to learn how to update the test list of your country, see the results of our project and check-out the vacant research positions! https://netalitica.com/updating-citizen-lab-test-lists/ |
| **Project Ainita** | Project Ainita CTI Platform - Demo: Project Ainita's Cyber Threat Intelligence (CTI) portal aims to be a one stop shop for latest intel, live Internet measurements and contextual analysis for circumvention tool makers, researchers, journalists, funders, decision makers and stakeholders needing current and deep understanding of a country's Internet status. We will be providing a live demo of the CTI portal as well as Internet maps of a few countries. We intend on being fully available for Q&A and hope to foster rich brainstorming discussions of scaling CTI in other needed contexts. |

# Appendix - B

## OMG 4 Internal Sessions (Sept 11-12, 2025)

| OMG 4 - Day 1 | | |
|---|---|---|
| **Time** | **Duration** | **Session/ Description** |
| 9:30 - 10:00 AM | 45 mins | Welcome - Intros, Review Agenda and Goals |
| 10:00 AM - 11:15 AM | 75 mins | Reflection on GG Sessions and Feedback on Are You My Measurement Tool? |
| 11:15 - 11:30 AM | 15 min | Break |
| 11:30 AM -12:30 PM | 60 mins | Discussion: Coordination on censorship monitoring, reporting and rapid response |
| 12:30 PM - 1:30 PM | 60 mins | Lunch |
| 1:30 PM - 2:30 PM | 60 mins | Demos, 15 min each<br>• IODA - AGGIE<br>• OONI Probe dashboard revamp<br>• CP - Dashboard and CenAlert |
| 2:30 PM - 3:00 PM | 30 mins | Break |
| 3:00 PM - 4:30 PM | 60 mins | Discussion: Tactical Challenges in Daily Operations and How to Face Them |
| 4:30 PM - 4:45 PM | 60 mins | Day 1 closing reflections, discuss goals or edits to agenda for Day 2 |

| OMG 4 - Day 2 | | |
|---|---|---|
| **Time** | **Duration** | **Session/ Description** |
| 9:30 - 10:00 AM | 45 mins | Intro to Session for the Day |
| 10:00 AM - 11:15 AM | 75 mins | Discussion: Strategic sustainability in new funding landscape. |
| 11:15 - 11:30 AM | 15 min | Break |
| 11:30 AM -12:30 PM | 60 mins | Discussion: Theory of Change and SWOT analysis |

| OMG 4 - Day 2 | | |
|---|---|---|
| 12:30 PM - 1:30 PM | 60 mins | Lunch |
| 1:30 PM - 2:30 PM | 60 mins | Hands on Data Sessions, 30 mins each:<br>• OONI methodology for identifying throttling<br>• M-Lab: A collab to use data related to Internet shutdown<br>• IODA: AP loss/delay, Mozilla Telemetry, penultimate AS (and traceroute data for manual investigations) |
| 2:30 PM - 3:00 PM | 30 mins | Break |
| 3:00 PM - 4:30 PM | 60 mins | Reflection: What did we accomplish with the OMGs, and what do we want to accomplish going forward? + Planning: **Action Items** for Next Phase of OMG |

# Appendix C - OMG User Guide

## Introduction

From 2024-2025 four open measurement groups (Censored Planet, IODA, M-Lab, and OONI) convened at four Open Measurement Gatherings to build relationships and increase collaboration. One outcome of the OMGs is a user guide to compare each of the datasets to verify or analyze a network interference or censorship event. The following table outlines which use cases are served by the OMG groups' datasets. In addition, OMG groups have provided brief context for each use case as relevant. If you have questions, feel free to find the OMG groups on the OMG Help Slack channel hosted by OONI.

# OMG User Guide

| Types of interference | M-Lab | Censored Planet | OONI | IODA |
|---|---|---|---|---|
| Blocking of a specific website (e.g. facebook.com) | No | Yes | Yes | No |
| Blocking of an instant messaging app (e.g. WhatsApp) | No | No | Yes | No |
| Blocking of a VPN | No | No (unless do targeted research) | Yes | No |
| Generalized network throttling | Yes | No (unless do targeted research) | No | Yes |
| Throttling targeting a specific service (e.g. YouTube) | No | No (unless do targeted research) | Yes | No |
| Internet connectivity shutdown: National level | Yes | Maybe (in progress) | No (maybe visible from lack of measurement coverage, when there is stable coverage over a long period of time) | Yes |
| Internet connectivity shutdown: Subnational/ Regional level | Yes | Maybe (in progress) | No | Yes |
| Internet connectivity shutdown: Network level | Not reported, but could be done in principle | Maybe (in progress) | No (maybe visible from lack of measurement coverage, when there is stable coverage over a long period of time) | Yes |

## Blocking of a specific website (e.g. facebook.com)

Both OONI and Censored Planet provide open data on the censorship testing of websites. Such data can be useful if, for example, you would like to check the blocking of facebook.com in a specific country.

The main difference between OONI and Censored Planet data is that OONI data is collected by volunteers who run experiments (using the OONI Probe app) on local networks around the world, whereas Censored Planet data is collected through remote measurement performed centrally by researchers at the University of Michigan.

Both OONI and Censored Planet measure websites included in the public, community-curated test lists hosted on GitHub by the Citizen Lab. There are two types of test lists:

- Global test list: Includes internationally relevant websites (such as facebook.com), most of which are in English;
- Country-specific test list: Includes websites that are only relevant to a specific country, many of which are in local languages.

To encourage community to the test lists, OONI built a Test List Editor: a web interface through which you can review and contribute to the lists of websites that are tested for censorship.

Both OONI and Censored Planet measure the same lists of websites for censorship, but they measure websites using different methods. The two datasets are therefore complementary.

OONI's Web Connectivity experiment (available through the OONI Probe app) is designed to measure the accessibility of URLs by performing the following steps:

- Resolver identification
- DNS lookup
- TCP connect to the resolved IP addresses
- TLS handshake to the resolved IP addresses
- HTTP(s) GET request following redirects

The above steps are automatically performed from both the local network of the user, and from a control vantage point. If the results from both networks are the same, the tested URL is annotated as accessible. If the results differ, the tested URL is annotated as anomalous, and the type of anomaly is further characterized depending on the reason that caused the failure. Based on their heuristics, OONI is able to automatically confirm the blocking of websites based on fingerprints if a block page is served, or if DNS resolution returns an IP known to be associated with censorship.

Beyond the Citizen Lab test lists (which are tested by default), OONI also enables users to (a) test the websites of their choice through the OONI Probe app and
(b) to generate mobile deep links for the testing of a custom list of websites through the OONI Run tool.

All OONI measurements from the testing of websites globally are published as open data in real-time. To enable the public to explore the data, OONI built OONI Explorer: a web platform that includes a Search Tool for searching through the measurements, as well as a Measurement Aggregation Toolkit (MAT) for generating charts based on aggregate views of OONI data. You can use these tools to explore the blocking of websites, and to easily learn which websites are automatically confirmed blocked based on fingerprints. Learn how to use OONI Explorer through their user guide and documentation on interpreting OONI measurements.

Censored Planet conducts continuous, global measurements of internet censorship through two key tools: Hyperquack and Satellite. Hyperquack tests censorship on multiple protocols (HTTPS, HTTP, ECHO, and Discard), while Satellite focuses specifically on DNS-based interference. Unlike user-driven measurements, Censored Planet's approach relies on remote, side-channel techniques that do not require volunteers to run tests. Hyperquack leverages publicly accessible web servers around the world. typically hosted by ISPs and outside the researchers' control, to detect network interference.

To establish a baseline, Hyperquack first queries each server with a request for a nonexistent benign domain (e.g., control-1000008c8a986f3b.com) and records the server's normal error response. It then requests approximately 2,000 test domains from the same server. If the responses match the baseline, the connection is considered interference-free. However, deviations, such as injected TCP RST packets, modified content, or dropped connections, indicate the possible presence of censorship mechanisms like deep packet inspection middleboxes. During post-processing, these deviations are analyzed and classified to distinguish strong indicators of censorship from ordinary network failures.

Satellite complements Hyperquack by measuring DNS-based interference at a global scale. It discovers and monitors thousands of open DNS resolvers across the internet and uses the same test domain list as Hyperquack. For each test domain, Satellite first queries a set of five trusted control resolvers, which are expected to return correct, uncensored answers, to establish a reference for comparison. It then performs the same DNS lookups using the open resolvers distributed worldwide. For every response, Satellite fetches the corresponding web page and TLS certificate, comparing them against the results obtained from the control resolvers. By examining the validity of certificates, similarity of returned content, and consistency of IP addresses, Satellite can detect DNS manipulation while accounting for legitimate differences caused by CDNs or geographically distributed hosting. This ensures that detected anomalies reflect censorship rather than ordinary network variation.

All Censored Planet data is publicly available and updated daily. The results can be explored through the Censored Planet Dashboard, which provides visualizations of aggregated measurements. Researchers and developers can also access raw and aggregated data programmatically via the GraphQL API, which includes an interactive user interface, query endpoint (/query), and auto-generated documentation for each available data schema.

## Blocking of an instant messaging app (e.g. WhatsApp)

Beyond testing website accessibility, OONI also examines the blocking of several instant messaging apps, including:

- WhatsApp
- Facebook Messenger
- Telegram
- Signal

For each of these apps, OONI has developed dedicated experiments to assess their reachability on local networks. These specific apps were prioritized because they were requested by the internet freedom community and are often blocked during political events around the world. The experiments are available through the OONI Probe app and are conducted by hundreds of thousands of users each month across more than 3,000 networks in approximately 180 countries.

All OONI measurements from the testing of instant messaging apps globally are published as open data in real-time. To enable the public to explore the data, OONI built OONI Explorer: a web platform that includes a Search Tool for searching through the measurements, as well as a Measurement Aggregation Toolkit (MAT) for generating charts based on aggregate views of OONI data. Learn how to use OONI Explorer through their user guide.

To enable the internet freedom community to more easily discover and respond to censorship events, OONI created a new "Blocking of Social Media and Instant Messaging Apps" page which includes:

- Short reports documenting relevant blocks based on OONI data
- Longer research reports documenting relevant blocks based on OONI data
- Charts with the latest OONI data pertaining to the testing of instant messaging apps

## Blocking of a VPN

OONI measures the reachability of several circumvention tools:

- Tor
- Tor Snowflake
- Vanilla Tor
- Psiphon VPN
- OpenVPN

For each of these tools, OONI has developed dedicated experiments to assess their reachability on local networks. These tools were prioritized based on requests from the internet freedom community, their widespread use in highly censored environments, and opportunities for collaboration with their developers. The experiments are available through the OONI Probe app and are conducted by hundreds of thousands of users each month across more than 3,000 networks in roughly 180 countries. Beyond these experiments, OONI Probe users also measure the blocking of circumvention tool websites included in the Citizen Lab test lists.

All OONI measurements from the testing of circumvention tools globally are published as open data in real-time. To enable the public to explore the data, OONI built OONI Explorer: a web platform that includes a Search Tool for searching through the measurements, as well as a Measurement Aggregation Toolkit (MAT) for generating charts based on aggregate views of OONI data. Learn how to use OONI Explorer through their user guide.

To enable the internet freedom community to more easily discover and respond to censorship events, OONI created a new "Reachability of Circumvention Tools" page which includes:

- Short reports documenting relevant blocks based on OONI data
- Longer research reports documenting relevant blocks based on OONI data
- Charts with the latest OONI data pertaining to the testing of instant messaging apps

Unlike OONI, Censored Planet does not directly measure the reachability of circumvention tools such as Tor or VPNs. Instead, its research focuses on the broader security, privacy, and detectability aspects of the VPN ecosystem, providing insights into how VPNs can themselves become vulnerable to censorship, surveillance, or misconfiguration. Through a series of studies, Censored Planet has analyzed both commercial and mobile VPN applications, revealing systemic weaknesses and industry-wide risks:

- **MVPNalyzer: An Investigative Framework for the Security & Privacy Audit of Mobile VPNs** Introduces a large-scale framework for auditing Android VPN apps. By analyzing 281 popular apps, the study found that 61 transmit unencrypted data, 29 leak user traffic outside the VPN tunnel, 169 fail to obfuscate traffic, and 76 exfiltrate device identifiers such as the Advertising ID, exposing hundreds of millions of users to privacy risks.
- **VPNalyzer: Systematic Investigation of the VPN Ecosystem** Presents a cross-platform auditing tool used to test 80 commercial VPN providers. The study uncovered IPv6 and DNS leaks, improper "kill switch" implementations, insecure cryptographic configurations, and extensive infrastructure sharing between nominally independent VPN brands.
- **"All of them claim to be the best": Multi-perspective Study of VPN Users and VPN Providers** Combines a survey of over

1,200 VPN users with interviews of VPN operators, revealing deep misalignments between user expectations and provider practices, particularly regarding data collection, jurisdiction, and transparency.

- **OpenVPN is Open to VPN Fingerprinting** Demonstrates that over 85% of OpenVPN traffic (including many obfuscated configurations) can be reliably fingerprinted by ISPs using packet-level features, highlighting the detectability of VPN traffic even when encryption is correctly implemented.
- **Attacking Connection Tracking Frameworks as Used by Virtual Private Networks** Shows that stateful firewalls and NAT implementations in VPNs can be exploited to inject or drop packets across tunnels, enabling new classes of denial-of-service and traffic-disruption attacks.

## Generalized network throttling

The IODA platform now provides data aimed to capture events of throttling. To create this measurement we use one of the three principal data sources used by IODA is Active Probing. The Active Probing signal is generated by sending ping packets to elicit responses from a large fraction of the routable IPv4 address space. Although throttling can significantly degrade the performance of networked applications by increasing latency and packet loss, it will not block all responses to IODA's active probes. A throttled network might therefore still appear to be available in the IODA connectivity signals graph, e.g., as long as at least one probed IP in a /24 subnet responds successfully to a ping probe. For this reason, the Active Probing Details graph has been added to the country, region, and ASN/ISP views. Use the data in this graph to identify abnormal spikes in RTT latency and abnormal drops in Probe/Response Loss.

M-Lab can detect widespread throttling by comparing current throughput statistics (median, percentiles) to historical baselines within a country and/or ISP using BigQuery. This approach is effective for dramatic performance degradations, as demonstrated in research like "Dimming the Internet" analyzing Iran's network restrictions.

## Throttling targeting a specific service (e.g. YouTube)

OONI has created a methodology for measuring targeted cases of throttling. As part of this methodology, they analyze OONI Web Connectivity data (which is collected through the OONI Probe testing of URLs) to detect targeted cases of extreme throttling that impact specific online services (such as the throttling of YouTube). The OONI Web Connectivity measurements include network_events, which are processed by the OONI Pipeline v5 to extract precise timing information, including the duration of TLS handshakes.

OONI's methodology for detecting targeted throttling involves **analyzing timing information from HTTPS requests** in Web Connectivity data to identify deliberate slowdowns of specific services. Because throttling often appears as normal network congestion, OONI compares the performance of potentially throttled services against a baseline — a similar service hosted on a comparable network path — to rule out natural congestion. By comparing traffic patterns — for instance, examining specific fingerprints such as the TLS Server Name Indication (SNI) field — OONI can distinguish between general network issues and intentional, targeted interference.

OONI's methodology has been applied successfully in measuring various cases of throttling, such as those documented as part of their research reports on throttling cases in Kazakhstan, Russia, and Turkey.

## Internet connectivity shutdown: National level

IODA measures connectivity of Internet infrastructure through various signals including: Active Probing, BGP, and Telescope. Additionally, we integrate signals from Google Transparency Report at the country-level. These signals can all be used to identify abnormal drops in Internet connectivity. Simultaneous drops in two or more signals are a good indicator of an Internet disruption. If a drop in only one IODA signal is identified, we encourage users to cross reference other data sources in the OMG or Cloudflare Radar.

While OONI does not directly measure internet shutdowns, the availability of OONI data itself depends on internet connectivity, since OONI Probe users must be online to submit their measurements for publication. Therefore, a **sudden absence of OONI data** can serve as an *indirect indicator of a potential internet shutdown* – particularly when a country has a consistent volume of measurements before and after the reported event, and the observation is corroborated by external sources such as IODA and Cloudflare Radar. For example, the nationwide internet connectivity shutdown in Tanzania in late October 2025 – which is visible in both IODA and Cloudflare Radar data – can also be inferred from the absence of OONI data during that period.

M-Lab can help identify national shutdowns through dramatic drops in test volume from a country with previously stable testing patterns. In practice, this involves writing a BigQuery query to count tests per time period in a country and visualize trends over time.

At this stage, Censored Planet is developing and finalizing an approach to monitor Google Trends data for VPN-related topics. This method explores whether search data can serve as a complementary signal for detecting connectivity disruptions. In particular, a sudden absence of Google search activity during a period may indicate a widespread loss of connectivity, while a spike in searches for VPNs or circumvention tools shortly after connectivity returns could suggest that users are seeking ways to bypass or respond to a recent shutdown.

## Internet connectivity shutdown: Regional level

IODA measures connectivity of Internet infrastructure through various signals including: Active Probing, BGP, and Telescope. These signals can all be used to identify abnormal drops in Internet connectivity. Simultaneous drops in two or more signals are a good indicator of an Internet disruption. If a drop in only one IODA signal is identified, we encourage users to cross reference other data sources in the OMG or Cloudflare Radar.

M-Lab data includes latitude/longitude annotations derived from client IP addresses using publicly available GeoIP datasets. These geographic coordinates enable investigation of regional shutdowns by allowing analysts to filter measurements near a specific geographic center using BigQuery. While the data is annotated with lat/lon coordinates, keep in mind that GeoIP accuracy varies by region and ISP.

At this stage, Censored Planet is developing and finalizing an approach to monitor Google Trends data for VPN-related topics. This method explores whether search data can serve as a complementary signal for detecting connectivity disruptions. In particular, a sudden absence of Google search activity during a period may indicate a widespread loss of connectivity, while a spike in searches for VPNs or circumvention tools shortly after connectivity returns could suggest that users are seeking ways to bypass or respond to a recent shutdown.

## Internet connectivity shutdown: Network level

IODA measures connectivity of Internet infrastructure through various signals including: Active Probing, BGP, and Telescope. These signals can all be used to identify abnormal drops in Internet connectivity. Simultaneous drops in two or more signals are a good indicator of an Internet disruption. If a drop in only one IODA signal is identified, we encourage users to cross reference other data sources in the OMG or Cloudflare Radar.

While OONI does not directly measure internet shutdowns, the availability of OONI data itself depends on internet connectivity, since OONI Probe users must be online to submit their measurements for publication. Therefore, a **sudden absence of OONI data** can serve as an *indirect indicator of a potential internet shutdown* – particularly when a network has a consistent volume of measurements before and after the reported event, and the observation is corroborated by external sources such as IODA and Cloudflare Radar.

M-Lab data includes ASN (Autonomous System Number) annotations for each test, enabling detection of network-level shutdowns by analyzing test volume from specific ISPs or networks. In practice, this involves writing a BigQuery query to count tests per time period for a specific ASN and visualize trends over time.

At this stage, Censored Planet is developing and finalizing an approach to monitor Google Trends data for VPN-related topics. This method explores whether search data can serve as a complementary signal for detecting connectivity disruptions. In particular, a sudden absence of Google search activity during a period may indicate a widespread loss of connectivity, while a spike in searches for VPNs or circumvention tools shortly after connectivity returns could suggest that users are seeking ways to bypass or respond to a recent shutdown.

## Limitations

Each of the above datasets (M-Lab, Censored Planet, OONI, IODA) have strengths and limitations, as they each measure different things and collect data in different ways. For example, because OONI data is crowdsourced by OONI Probe users around the world, the availability of data varies from country to country (and network to network within a country) over time.

One limitation that they all have in common is the presence of false positives. A false positive is a test result that wrongly indicates that a particular condition or attribute is present.

Within the OONI context, false positives are OONI Probe test results which incorrectly indicate the presence of network interference (such as the blocking of a website or app). Below are some reasons which may trigger false positives in website testing:

- **Transient network failures.** If OONI Probe tests are performed on an unstable network, the test results may show signs of potential interference.
- **Unreliable servers.** If a website is hosted on an unreliable server or otherwise encounters server issues, the tested website may return failures (even though it's not interfered with) and the OONI Probe test may fail.
- **DNS resolution.** If the DNS resolver of an OONI Probe user (such as Google or their local ISP) provides an IP addresses that is closest to the user geographically, that IP address may differ from the IP address resolved from a control vantage point, potentially incorrectly indicating the presence of DNS tampering (though some precautions are taken to minimize this).
- **Geographical distribution of content.** Many websites serve different content depending on the country that the user is connecting from. In these cases, the HTTP responses from the network of the OONI Probe user and from the control vantage point will differ, potentially incorrectly indicating the presence of HTTP based interference.

When running the OONI Probe instant messaging app tests (WhatsApp, Facebook Messenger, Telegram, Signal), beyond the aforementioned issues, false positives may also occur when the instant messaging app vendor makes changes to their infrastructure that affect how OONI Probe tests run. When running the OONI Probe middlebox tests, false positives may occur due to issues with the OONI Probe backend infrastructure. When running any OONI Probe test, false positives may occur due to software bugs triggered by the user's particular device and network configuration, or due to bugs in OONI's systems.

Distinguishing false positives can often be tricky, even for engineers. It requires examining the network measurement data carefully, having a good understanding of how OONI Probe tests work, analyzing the data over a long period of time (to check whether the tested resource consistently presents the same failures on the same network), and evaluating and ruling out other possible reasons that could have triggered the anomaly (for example, by checking the global failure rates of a site).

In general, **we recommend looking at relevant measurements in aggregate over a timeline, rather than individually** (OONI enables this with their Measurement Aggregation Toolkit). For example, if you observe that a tested website presents the same failure (e.g. TLS connection reset error) every time it is tested on a specific network in a country, it's more likely the case

that access to it is being interfered with. If, however, a single measurement (for example) presents a TCP/IP anomaly, but all other measurements testing that website on the same network were successful, it's likely the case that that TCP/IP anomaly is a false positive.

IODA limitations include:

- IODA relies on geolocation datasets that can be inaccurate/ outdated.
- Limited to IPv4 (no IPv6).
- Less visibility into countries that heavily use private IP addresses (NAT).
- Less visibility into mobile networks.
- IODA cannot tell the cause of a disruption.

M-Lab limitations include:

- Tests are user-initiated, so measurement volume depends on user behavior and may vary significantly across regions and networks.
- Data availability in BigQuery has up to 24-hour delay, limiting real-time monitoring capabilities.
- Measurements are application-agnostic and cannot detect service-specific throttling (e.g., targeting YouTube or Facebook).
- Analysis requires sufficient test volume for statistical significance; regions or networks with few tests cannot be reliably analyzed.
- M-Lab does not have servers in every country; when servers are distant, attributing performance changes requires ruling out other causes along the network path (e.g., fiber cuts, interconnection congestion).

Censored Planet limitations include:

- **Limited visibility into user-proximal interference.** Because Censored Planet's measurement techniques rely on remote vantage points rather than user devices, they cannot reliably detect censorship occurring very close to the user, such as filtering by access networks or enterprise firewalls located only a few hops upstream. OONI's on-device measurements are better suited for capturing such localized interference.
- **Restricted coverage due to ethical constraints.** In line with strict ethical guidelines, Censored Planet only performs measurements targeting organizational web servers (for example, ISP-hosted or infrastructure servers) and avoids directly interacting with individual users or residential networks. As a result, measurement density varies across countries: in some regions, only a limited number of suitable vantage points exist, leading to sparser data and less comprehensive coverage.
- **Dependence on external geolocation data.** To map measurement results to specific countries or regions, Censored Planet depends on third-party IP geolocation datasets. These datasets may be incomplete or occasionally inaccurate, which can affect the precision of geographic attribution.

## Best practices for each tool

- Crossreference data sources! - Don't just rely on one dataset. If one dataset indicates there may be network interference, use this as a starting point to begin your investigation into several datasets. If one dataset indicates possible interference, use it to guide your investigation across several sources (OONI, Censored Planet, IODA, M-Lab, Cloudflare Radar).
- Reach out to the OMG teams! You can find us on the OMG Help Slack channel hosted by OONI.

M-Lab best practices:

- Analyze aggregate data over time rather than individual measurements to identify patterns and rule out transient network issues.
- Ensure sufficient test volume exists for the region or network of interest before drawing conclusions; sparse data limits reliability.
- Cross-reference M-Lab findings with other datasets (OONI, IODA, Cloudflare Radar) to distinguish network disruptions from natural congestion or infrastructure issues.
- When investigating performance degradation to specific M-Lab servers, verify server health by checking performance from other geographic regions to rule out server-side issues before attributing problems to the network or region under investigation.
- M-Lab data has up to 24-hour publishing delay; use it for follow-up analysis and confirmation when investigating disruptions happening in real time.

To get the full picture of website blocking, always analyze Censored Planet data together with OONI data. The two datasets are complementary, OONI's vantage points capture on-the-ground, user-side measurements, while Censored Planet provides large-scale remote observations across networks and countries.

If one dataset indicates potential interference, use it as a starting point and cross-check the finding in the other to validate or refine your interpretation. For deeper guidance on how to perform rigorous censorship data analysis, check out the paper Advancing the Art of Censorship Data Analysis, which proposes an open-source pipeline for cleaning, annotating, and interpreting Censored Planet data. The paper highlights several best practices, including:

- Remove false positives by comparing test and control measurements and applying fingerprints for known non-censorship cases (e.g., CDN localization, server-side blocking, bot protection).
- Add accurate metadata (e.g., AS, organization, and geolocation info) from multiple sources such as CAIDA, DB-IP, and Censys to contextualize blocking events.
- Account for unexpected interference like CDN configurations, geoblocking, or Internet shutdowns before attributing behavior to censorship.
- Use control measurements to distinguish true censorship from general connectivity failures or routing disruptions.
- Aggregate over time to detect persistent patterns and avoid misclassifying transient network errors.
- Keep analysis modular and iterative, so new fingerprints or metadata can refine past measurements.