OMG! Summary of the 3rd Open Measurement Gathering (OMG) Ask Me Anything (AMA) event

On June 25, 2025, the Open Measurement Gathering (OMG) held a public event, "*Open Measurement Gathering AMA",* featuring Censored Planet, IODA, OONI, and Measurement Lab. This was a chance for the OMG group to share project updates, future plans, and gather questions and feedback from the Internet freedom community. Each measurement group presented for 30 minutes followed by Q&A.

Summaries and links to each group's presentation:

- **Full OMG AMA Playlist**
- **Censored Planet** Summary, Slides and Recording
- **Measurement Lab** Summary, Slides and Recording
- **OONI** Summary, Slides and Recording
- **IODA** Summary, Slides and Recording
- Key Community Questions

This public virtual event was inspired by the past two OMG convenings (public reports 1 and 2) at which OMG groups have shared exciting updates to their platforms, tools, and/or datasets before sharing with the broader Internet freedom community. For the third OMG convening, the groups decided to share previewing updates publicly to encourage community feedback.

During the event, OMG groups gathered feedback and answered questions from the Internet freedom community directly. At the end of this post, find some key questions from the community and our answers. You can also watch the presentations and listen to the full Q&A for each session.

The OMG AMA event was especially intended for advocacy organizations, digital rights researchers, anti-censorship tool developers, journalists, lawyers, activists, policy makers, and funders. At its peak, we had about 60 folks joining us from around the world. The OMG groups truly appreciate those who could attend, and we hope to host more joint events in the future!

Presentation Summaries

🛰️What Censored Planet Does:

- Censored Planet is a research team at the University of Michigan building scalable systems and novel techniques to protect users from online censorship, surveillance, and the digital divide. Our work lies at the intersection of Networking, Security & Privacy, and Internet Measurements. We take a data-driven approach to detect and defend against powerful network intermediaries and government threat actors. Our observatory runs daily remote measurements to monitor which domains are blocked across over 200 countries, collecting longitudinal, ethically gathered data.

🆕 Recent and Upcoming Features:

- **Censored Planet Analysis Pipeline v2:** We released **a new analysis pipeline**, marking a major shift from batch-based cloud processing on Google Cloud to a self-hosted, real-time infrastructure. Previously, all global measurements were processed once per day, introducing a delay between data collection and availability. The new pipeline processes results **immediately after each measurement** finishes, allowing us to provide **real-time visibility** into ongoing censorship events. This architecture not only **boosts performance** but also **improves sustainability and data control** by eliminating dependencies on commercial cloud services. As a result, we can now better support real-time research and rapid response efforts.

- **Censored Planet API:** Alongside the infrastructure upgrade, we launched our first public API, available at data.censoredplanet.org. The API is built using GraphQL and provides:
    - A graphical interface for exploring and querying the dataset interactively
    - A programmatic endpoint at /query for researchers and developers
    - **Access to every measurement collected since 2018**, including all tested protocols, domains and countries.

  This API is a major milestone in our mission to make the Censored Planet data open, accessible, and actionable. It empowers the community to build custom dashboards, perform time-series analysis, and automate censorship detection pipelines.

- **Censored Planet Dashboard v2**: We also released a completely redesigned self-hosted dashboard, now available at dashboard.censored planet.org. Unlike our earlier dashboard, this version is fully maintained in-house and built for long-term scale and customization. Whereas the old dashboard only displayed the last 6 months of measurements to reduce cloud hosting costs, Dashboard v2 now serves **the entire dataset dating back to 2018.** This enables users to perform historical, longitudinal analysis of censorship patterns directly through the dashboard. The landing page of the new dashboard displays a global 3D visualization of country-level interference rates over

the past 30 days, shown on an interactive globe. To ensure these statistics are accurate and fairly represent countries with sparse measurement coverage, we apply a Bayesian estimation with a prior. For each country, we use recent measurements along with a carefully chosen prior to calculate a posterior distribution for the probability of interference. This approach helps avoid both overestimating and underestimating interference rates in countries where only a small number of measurements are available. Rather than reacting strongly to limited data, the Bayesian model smooths the estimate by incorporating statistical uncertainty, allowing high-confidence rates in well-measured countries to be balanced with more cautious projections in regions with less coverage.

This statistical fairness is essential for presenting global censorship patterns responsibly—especially in regions where measurement coverage is still limited.

The new dashboard also features an Explore page that gives users direct control over the data they want to analyze. The landing page of the dashboard leads the user to an Explore page, which gives users the possibility to interactively analyze the data. Users can select a specific country, define a time window (up to 6 months), choose the protocol of interest, and select up to 10 domains to focus on. The dashboard then fetches the relevant aggregated data from our GraphQL API and presents a series of detailed visualizations tailored to that selection.

A central part of the Explore page is a table showing each domain alongside its category, the network and subnetwork where it was tested, the number of probes performed, and the unexpected rate—that is, the percentage of probes that encountered some form of interference. To provide temporal context, the dashboard includes an Outcome Timeline, which visualizes how probe results change over time. For each day in the selected window, users can see how many measurements succeeded normally and how many were disrupted, along with a breakdown of the specific types of interference detected. The dashboard also offers a network-level view that breaks down probe outcomes by ASN and subnetwork, helping uncover whether censorship is uniform across providers or targeted to specific ISPs. Finally, we include a sunburst chart that provides a visual summary of how measurements break down proportionally across outcomes.

- **Censorship Early Warning System:** We are building a new alerting system that leverages Google Trends data to detect early signs of emerging censorship events. By analyzing spikes in public search interest for VPNs and other circumvention tools, the system surfaces signals that reflect user distress and potential access disruptions—particularly valuable in countries where traditional reporting channels are limited, restricted, or under threat. The system applies country-specific anomaly detection algorithms to daily search data and assigns each detected spike an impact factor, which quantifies the strength and urgency of public demand for circumvention. This impact-driven approach helps prioritize where attention and resources should be focused. In a multi-year evaluation across 76 countries (2011–2024), the system identified 149 confirmed censorship events, including 62 incidents that had not previously been reported by the internet freedom community. Most of these events were detected within 24 hours of their onset, making the tool highly suitable for real-time

monitoring and rapid response. A public release is planned in the coming months, which will include both an API and an interactive dashboard interface.

- **Launching Custom Measurements:** We are developing a new interface that will allow external researchers and digital rights organizations to request custom censorship measurements using our infrastructure.

- **Research:**
    - Our recent research has focused on strengthening the technical foundations of censorship detection and circumvention. In our work "CenPush: Blocking-Resistant Communication Using Push Notifications", we explore the untapped potential of push notification services as resilient control channels for censorship circumvention tools. By leveraging their indirect server-to-client communication model and the high collateral damage associated with blocking them, push notifications offer a robust and sustainable channel for the automatic delivery of client configuration updates, such as new proxy IP addresses to replace blocked ones, without requiring user intervention. Through measurement-based analysis, we demonstrate that these systems offer strong availability and fingerprint-resistance, even under IP-level blocking. We have integrated support for a push notification-based control channel into Orbot, the Tor client for Android.
    - In our FOCI 2025 paper "Is Custom Congestion Control a Bad Idea for Circumvention Tools?", we examine how aggressive congestion control algorithms (CCAs), such as those used in Hysteria and TCP-Brutal, trade performance for detectability. While designed to perform better under lossy cross-border connections, these custom CCAs deviate significantly from standard TCP/QUIC behaviors, exposing them to easy classification and detection by censors. Using controlled experiments and a two-stage threshold-based classifier, we show that these protocols can be reliably fingerprinted, even under varying network conditions. Our findings underscore the importance of aligning circumvention tool behavior with standardized protocols to maintain traffic indistinguishability and avoid detection.
    - In our paper "The Discriminative Power of Cross-layer RTTs in Fingerprinting Proxy Traffic", we introduce a technique to remotely fingerprint censorship middleboxes based on the round-trip time (RTT) overhead they introduce. By measuring subtle RTT changes across thousands of vantage points, we demonstrate how this method can identify specific censorship equipment and their behaviors—even in opaque or hostile network environments. This approach allows us to infer the presence, type, and scope of middlebox interference without needing privileged access or in-country infrastructure, offering a new lens for remote censorship analysis at scale.

🌐 What Measurement Lab (M-Lab) Does:

M-Lab *measures the Internet*, *saves the data*, and *makes it universally accessible and useful*.

- M-Lab's platform consists of 500+ servers globally, in more than 40+ countries.
- M-Lab supports a suite of open-source tools and experiments that measure Internet speed and performance (NDT), routing paths, and application layer performance
- M-Lab provides the measurement results as open data in BigQuery

🆕 Recent and Upcoming Features:

- **The Giga / UNICEF use case:** Giga is using the M-Lab platform to monitor school connectivity worldwide. Giga Meter runs periodic tests monitoring Internet performance, and since 2024 has conducted more than 1.5M measurements from more than 10K schools in 27 countries. All data are provided in Giga maps

- **The IP Route Survey (IPRS)**: A new dataset, by the Dioptra research group at Sorbonne University, is published by M-Lab. The dataset contains regular traceroute-style measurements from 10 vantage points to all routable IPv4 prefixes. Find out more at our blog post.

- **Host Managed Deployments**: M-Lab is evolving its platform, by enabling a new type of servers, aiming to measure more of the Internet from new network locations, diversify platform servers and costs, and have a larger geographical footprint.

- **Internet Quality Barometer (IQB)**: M-Lab has designed the IQB framework to redefine Internet quality beyond "speed". IQB considers multiple use cases in the Internet and multiple datasets to characterize the Internet Quality. Find out more at our blog post.

🐙 What OONI Does:

- The Open Observatory of Network Interference (OONI) is a nonprofit organization that builds free and open source network measurement tools that anyone can use to measure and detect various forms of internet censorship. OONI publishes network measurements collected from around the world as open data in real-time.

🆕 Recent and Upcoming Features:

- **New Software Releases:**
  - **Launched OONI Run v2.** In October 2024, OONI launched OONI Run v2: the next generation version of OONI Run for community-driven censorship testing. OONI Run v2 is a major revamp that addresses key community feedback and needs.
  - **Launched OONI Probe multiplatform app for Android and iOS.** In March 2025, OONI launched an OONI Probe multiplatform app for Android and iOS. This is an important milestone for the long-term sustainability of the OONI Probe apps, as it will enable OONI to ensure feature parity and to ship new features faster and more effectively across platforms.
  - **Launched News Media Scan app for iOS.** In 2024, OONI launched the News Media Scan app for iOS (their first multiplatform app in production). This is an OONI Probe-based app developed in collaboration with Deutsche Welle (DW) to measure the blocking of news media websites. Similarly to OONI Probe, OONI publishes News Media Scan app test results as open data in real-time. OONI previously launched the Android version of the News Media Scan app in October 2023.
  - **Launched new OONI Explorer thematic censorship pages.** In April 2025, OONI launched new OONI Explorer thematic censorship pages. These new pages include charts and reports documenting the blocking of social media, news media, and circumvention tools around the world based on OONI data.

- **Experiments and Data Analysis:**
  - **Throttling methodology.** Over the past few years, OONI created a methodology for measuring targeted cases of throttling. As part of this methodology, OONI analyzes 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 Twitter/X). Specifically, OONI's methodology for measuring targeted cases of throttling involves the analysis of timing information during HTTPS requests in Web Connectivity data. This methodology has been successful in measuring various cases of throttling, such as those documented as part of their research reports on throttling cases in Kazakhstan, Russia, and Turkey. In 2024, OONI published a design document about their throttling methodology to support related research and future work.

- **OpenVPN experiment.** As part of their OTF Information Controls Fellowship with OONI, Ain Ghazal contributed a new OpenVPN experiment to OONI Probe. In 2024, OONI shipped this experiment as part of the OONI Probe apps and they started publishing OpenVPN measurements as open data in real-time.
- **Encrypted Client Hello (ECH) experiment.** In November 2024, Russia blocked ECH. In response to this block, and in light of the risk that more countries may start blocking ECH over the next years, OONI designed a new "ECH Check" experiment which measures whether blocking is triggered by the presence of the Encrypted Client Hello (ECH) extension in the Client Hello during a TLS handshake. OONI shipped their new ECH Check experiment as part of the OONI Probe apps and they started publishing ECH measurements as open data in real-time.
- **OONI Pipeline v5.** Over the past two years, OONI have been advancing their data analysis methods through their latest data processing pipeline: OONI Pipeline v5. With this pipeline, OONI are moving beyond the concept of "anomalies" to instead characterize tested services as "blocked", "down", or "OK". The pipeline specifies the blocking details, fully characterising a block based on all the methods through which it is implemented. The data analysis capabilities of the new OONI Pipeline v5 supported all of OONI's latest research reports, such as those on internet censorship in Kazakhstan, Russia, Tanzania, Jordan, Senegal, Brazil, and Azerbaijan. The OONI Pipeline v5 also enabled OONI to analyze TLS handshakes and apply their throttling methodology to investigate targeted cases of throttling in Kazakhstan, Russia, and Turkey. As anyone can run the OONI Pipeline v5, third party researchers have already made use of its data analysis capabilities. Sinar Project, for example, used the OONI Pipeline v5 in support of their 2024 iMAP research reports on internet censorship in 9 Asian countries.

- **Research and Reporting on Internet Censorship:**
  - **Research on internet censorship.** Over the last year, OONI published several research reports based on the analysis of OONI data. These include reports documenting a surge in online LGBTQI website blocks in Tanzania, TLS man-in-the-middle (MITM) attacks and news media blocks in Kazakhstan, extensive news media censorship in Russia, and the blocking of Telegram in Kenya during the country's 2023 and 2024 KCSE national exams. Notably, Russia started blocking OONI Explorer – which OONI documented with OONI data.
    - **Third party use of OONI data.** Similarly to previous years, OONI data continued to support third party research efforts. This includes a FOCI paper that applies supervised and unsupervised models to OONI global DNS measurement data, a USENIX paper on measuring the Great Firewall's web censorship at scale, the Tehran E-Commerce Association report on the "Quality of Internet in Iran", and a Cloudflare blog post which provides a global assessment of third-party connection tampering by

comparing Cloudflare TCP connection anomalies with OONI reports of connection tampering. Notably, the iMAP project published 9 research reports on internet censorship in Cambodia, Hong Kong (China), India, Indonesia, Malaysia, Myanmar, Philippines, Thailand, and Vietnam based on OONI data. More examples of third party use of OONI data in 2024 are available here.

- **Rapid reporting on internet censorship.** In response to emergent censorship events around the world, OONI published numerous short reports on their OONI Explorer Censorship Findings page documenting blocks based on OONI data. In 2024, OONI published 12 new censorship reports. Within the first 6 months of 2025, OONI has published 18 new censorship reports so far.

- **Global Community Engagement in Internet Censorship Research:**
  - **New partnerships.** Over the past year, OONI established 6 new partnerships with Digital Rights Foundation (Pakistan), SAFEnet (Indonesia), Digital Rights Nepal, CyberHUB Armenia, EngageMedia (Philippines), and 7amleh – The Arab Center for the Advancement of Social Media (Palestine). Now, OONI's global partner network includes 55 digital rights organizations!
  - **OONI Partner Gathering 2024 in Malaysia.** In May 2024, OONI hosted an in-person OONI Partner Gathering in Kuala Lumpur, Malaysia. As part of this 2-day event, they brought OONI partners (primarily from Asia and the Middle East) together to exchange skills and knowledge on internet censorship research. The goal of the event was to strengthen global and regional collaborations on censorship measurement research and advocacy. Learn all about the event through OONI's report and animation.
  - **New OONI Community Interview videos.** To highlight the important work of their community and the interesting ways that community members make use of OONI tools and data, OONI started an "OONI Community Interviews" video series on their YouTube channel several years ago. In 2024, OONI published 2 new OONI Community Interviews with Chido Musodza from the Localization Lab and Tawanda Mugari from the Digital Society of Africa (DSA).
  - **Localization of OONI tools and resources.** Thanks to the Localization Lab community, OONI tools and resources are available in multiple languages. Localization highlights from the past year include the release of the Test Lists Editor in 9 languages, and the publication of the OONI Outreach Kit in Arabic and Farsi.
  - **OONI workshops.** In 2024, the OONI team facilitated multiple (online and in-person) OONI workshops for **484 participants** from around the world. Many additional OONI workshops were also facilitated by their partners and broader community (for example, in Pakistan, Sudan, Senegal, and Tanzania).

🔄 In Development / Future Plans:

- **Software Development:**
  - Release OONI Probe Desktop Multiplatform App
  - Refactor and streamline the OONI measurement engine
  - OONI Pipeline v5 improvements
  - Release the Social Media Censorship Alert System
  - Create an anonymous credential system for use in OONI Probe
- **Research:**
  - Publish more research reports documenting internet censorship around the world based on the analysis of OONI data
  - Publish more censorship findings on OONI Explorer (ongoing basis)
- **Community:**
  - Expand & strengthen the OONI partner network
  - Facilitate OONI workshops to enable the community to independently make use of OONI data
  - Coordinate ongoing localization and censorship rapid response efforts

🔍 What IODA Does:

- IODA provides a **public dashboard** showing internet **connectivity measurements** to monitor Internet infrastructure connectivity and detect Internet **outages**. IODA is hosted by the **Internet Intelligence Lab** at Georgia Tech. Users across the globe rely on IODA to track and monitor Internet connectivity. IODA also provides a valuable open-data source for the technical research community that inspires collaboration and spurs researchers to publish scientific literature in the Internet measurement space.

🆕 Recent and Upcoming Features:

- **Greater Granularity in Signal Data -** IODA released an update that provides greater granularity of data. Specifically, ASN/ISP signals are now localized to the country or region they operate in, providing a more localized view of connectivity. In this presentation we walk through examples in **Sumy, Ukraine** and **Bocas del Toro, Panama**. This update is particularly powerful for identifying outages within ASNs/ISPs that operate across regions. Read more in our blog post.
- **Active Probing: Latency & Loss Signals -** New signals detect our Active Probing **Probe/Response loss** and **latency spikes** to infer **generalized throttling** or degraded performance. An example from **Gaza** shows probe/response loss corresponding with recent fiber cuts. This new data will be released July 2025.
- **New User Resource Hub -** Includes tutorials, research papers, glossary, and data repositories. We aim to make the tools more understandable and accessible. Keep looking for more content to be added in the future. Read more in our blog post.
- **Dashboard Redesign - I**mproved UI based on user feedback and user-centered design. The redesign provides easier access to visualizations and signals previously hidden behind buttons.
- **Upstream Delay/ Traceroute Analysis -** Uses **traceroute data** to track **routing path changes** and measure delay or the penultimate or last hop ASN/ISP. Helpful for identifying networks that are upstream, as shown with examples from **Rwanda (MTN)** and **Venezuela (post-election unrest)**. This is only available at the ASN/ISP level in IODA and will be released July 2025.

🔄 In Development / Future Plans:

- Integration of Mozilla telemetry data.
- Global power outage dataset being compiled.
- Localization support (beyond browser-based translation).
- Semi-automated system for documenting outages (to improve efficiency of manual verification).
- Animated explainer videos to clarify measurement methods.

Some Key Questions From Community

Q: Are there efforts to measure the broader impacts of internet interference (economic, social, political)?

A: For economic impact, we refer you to the methodology implemented in this study from Brookings Institute. There is interest to build upon existing work, however, deeper analysis will likely require collaboration with experts in other fields.

Q: How is AI being used in internet measurement work?

IODA: The Internet Intelligence Lab at Georgia Tech is using AI to classify networks (e.g., identifying government or residential ASNs). Potentially, AI agents could be employed on our dashboard that would allow users to query and interact with measurement data directly. We have also considered using LLMs to help identify potential causes of Internet outage.

M-Lab: One potential use of AI is to help non-technical users to have better access and analysis of Internet measurement data. It is something we would be interested in exploring with partners.

Q: For funding, is there any possibility of becoming for-profit to reduce reliance on support from specific governments?

A: It's important to OMG groups to maintain their non-profit status, whether as part of a larger entity or independently, due to the nature of their work to make data publicly available, trustworthy, and actionable, especially for the Internet freedom community. In addition, some open Internet measurement tools rely on their communities to collect the data, and we would not want our user community to worry about data being monetized. However, there are options OMG groups could pursue to generate revenue such as data analysis services.

Links to donate:

- Donate to the Internet Intelligence Lab at Georgia Tech which runs and maintains IODA.
- Contribute the Measurement Lab platform
- Donate to OONI or become an OONI supporter

Q: Is it feasible to predict internet outages/censorship events?

CP: Not really — forecasting outages or censorship in advance remains out of reach. However, Censored Planet is developing an early censorship warning system that leverages spikes in

Google Trends VPN search terms to flag emerging censorship within a day of onset, even though it cannot predict events ahead of time.

IODA: In our recent paper, Destination Unreachable, we conducted a longitudinal and interdisciplinary study of shutdowns compared to outages and identified political and technical signatures of each. Potentially, these findings could be used to provide an early indicator of an outage demonstrating the signatures of a shutdown versus a spontaneous outage. Read more about the study here.

Q: Can users subscribe for updates?

A: Join the *Keep It On* and *OTF-Talk* listservs for updates in the internet freedom community. To join *OTF-Talk,* go to https://www.opentech.fund/ and scroll to the bottom of the website to request. To join *Keep It On,* email keepiton-request@lists.riseup.net and request to join.

OONI: You can subscribe to the ooni-talk mailing list for regular OONI updates.

M-Lab: Join our Discuss Google group to get access to M-Lab data, receive updates, and be part of M-Lab community discussions.

Q: Can users define custom alerts for Internet disruptions or censorship events?

A: Yes.

IODA: IODA has an outage detection system that produces alerts for abnormal drops in connectivity signals. You can read more about this outage system in our User Resource Hub. These alerts and outage summaries are visible in our dashboard and accessible via the API.