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

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.

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.