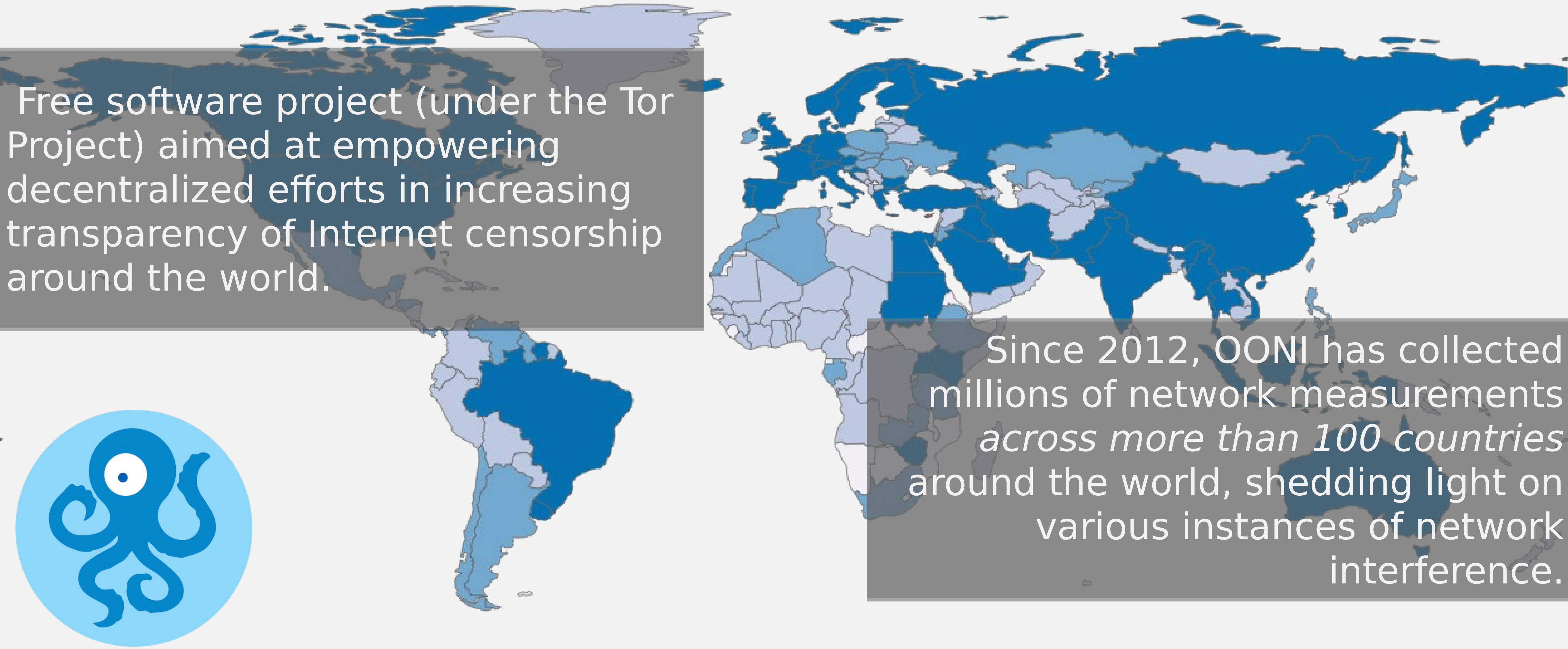
Investigating Internet Controls with OONI

Internet Freedom Festival, 7th March 2017
Arturo Filastò & Maria Xynou

OONI: Open Observatory of Network Interference



Free software project (under the Tor Project) aimed at empowering decentralized efforts in increasing transparency of Internet censorship around the world.

Since 2012, OONI has collected millions of network measurements *across more than 100 countries* around the world, shedding light on various instances of network interference.

https://ooni.torproject.org

Blocking of websites

Blocking of instant messaging apps

Blocking of censorship circumvention tools

Detection of middle boxes

Measurement of network speed & performance

OONI Software Tests

Recent cases

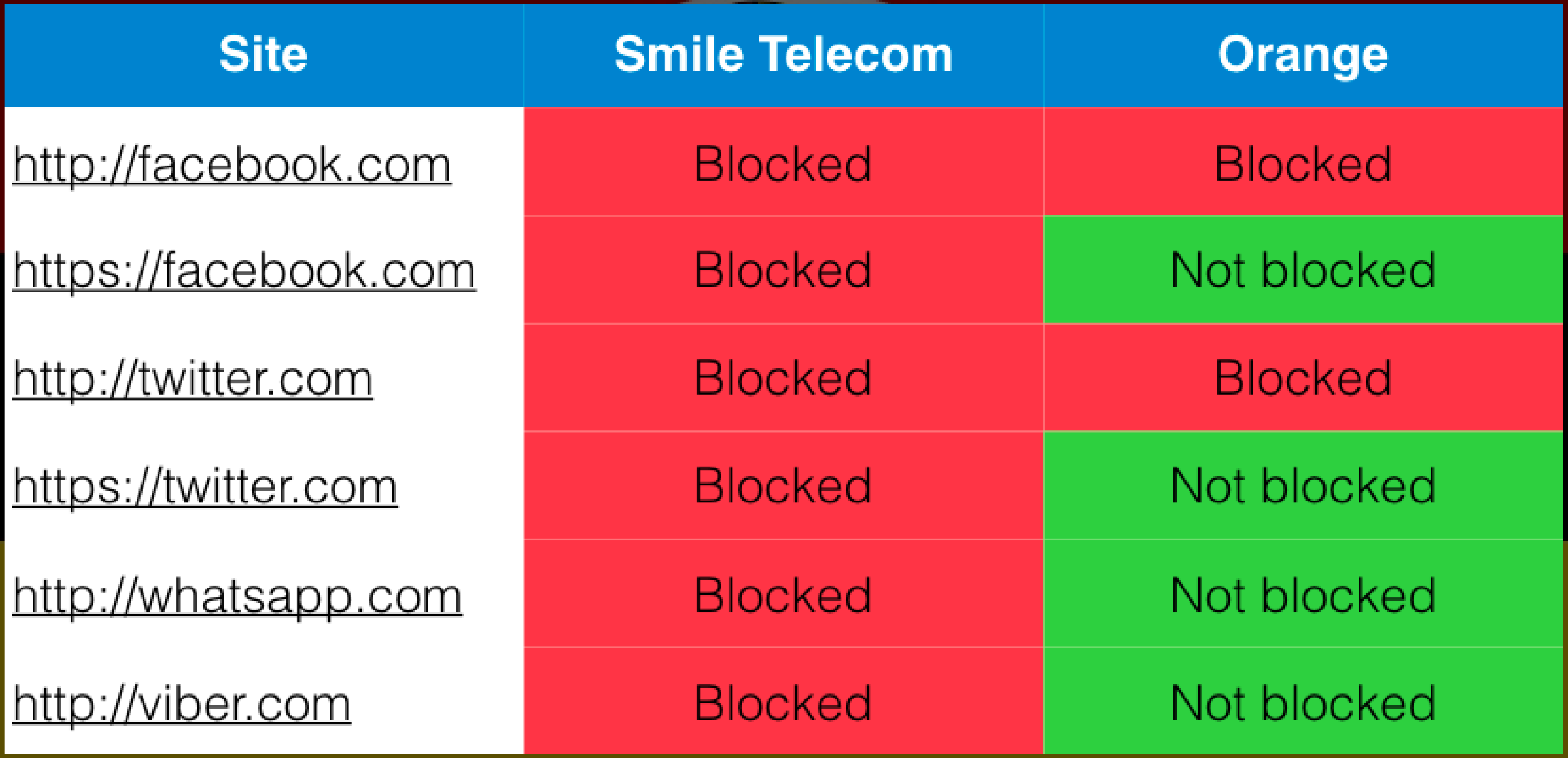
WhatsApp blocked in Brazil

May 2016

https://ooni.torproject.org/post/brazil-whatsapp-block/

Social media blocked in Uganda

May 2016



Site	Smile Telecom	Orange
http://facebook.com	Blocked	Blocked
https://facebook.com	Blocked	Not blocked
http://twitter.com	Blocked	Blocked
https://twitter.com	Blocked	Not blocked
http://whatsapp.com	Blocked	Not blocked
http://viber.com	Blocked	Not blocked

https://ooni.torproject.org/post/uganda-social-media-blocked/

Internet censorship events in Ethiopia

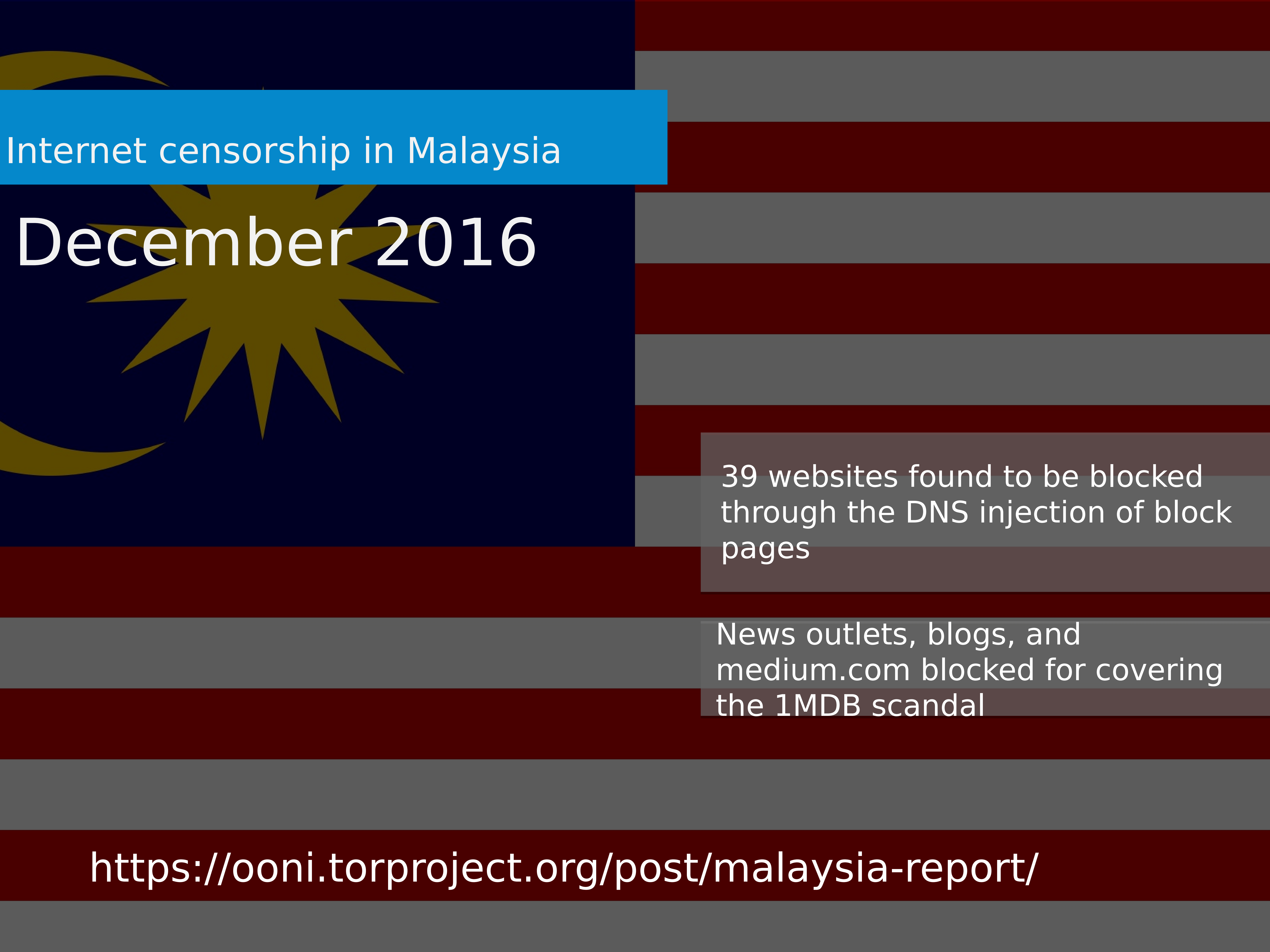
December 2016

WhatsApp found to be blocked

Deep Packet Inspection (DPI) detected

Media outlets, LGBTI sites, human rights websites, political opposition sites & circumvention tool sites found to be blocked

https://ooni.torproject.org/post/ethiopia-report/



Internet censorship in Malaysia

December 2016

39 websites found to be blocked through the DNS injection of block pages

News outlets, blogs, and medium.com blocked for covering the 1MDB scandal

https://ooni.torproject.org/post/malaysia-report/

Running ooniprobe

Linux or macOS

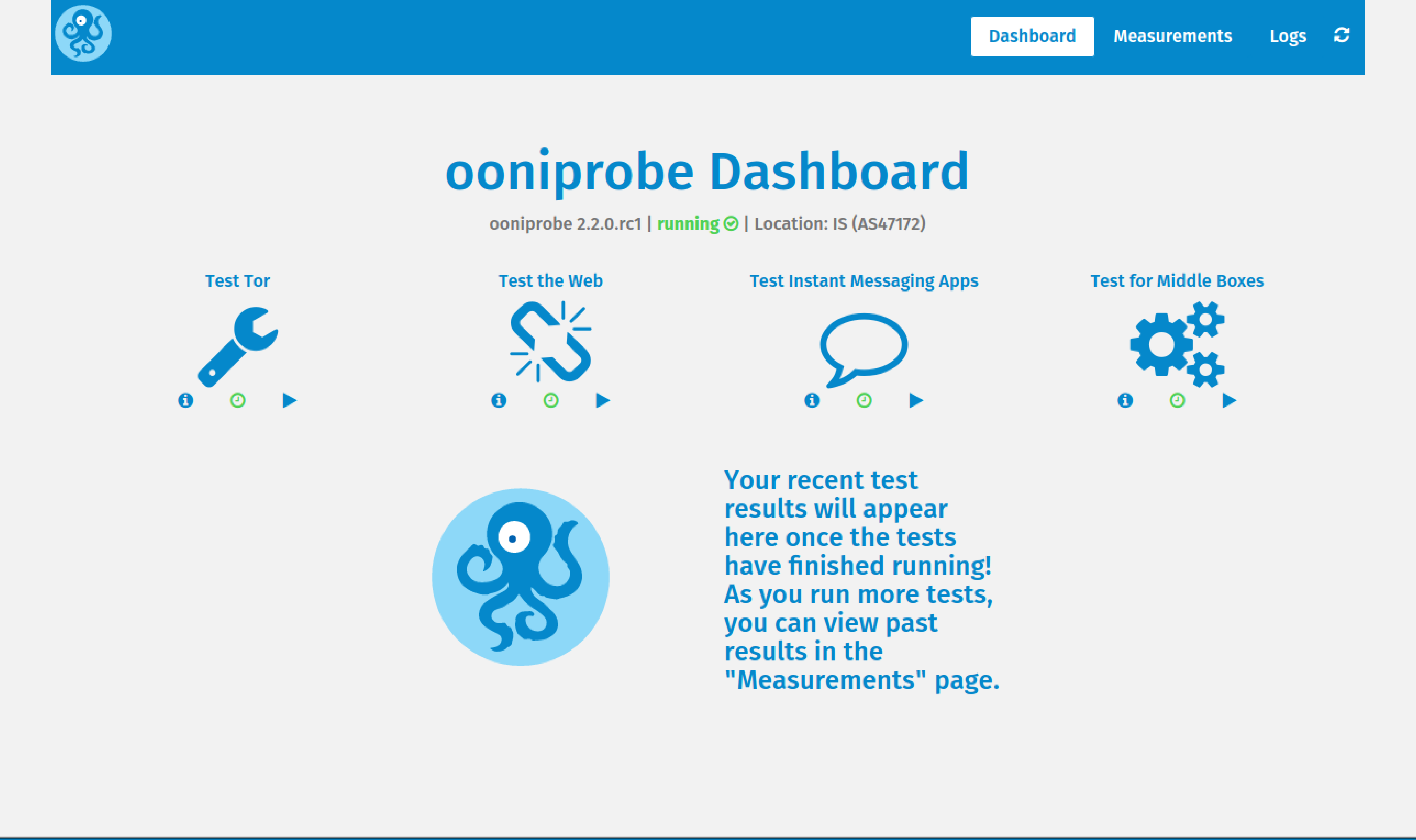
Android

GET IT ON
Google Play

iOS

Download on the
App Store

Raspberry Pi



ooniprobe Dashboard

ooniprobe 2.2.0.rc1 | running ✓ | Location: IS (AS47172)

Test Tor

Test the Web

Test Instant Messaging Apps

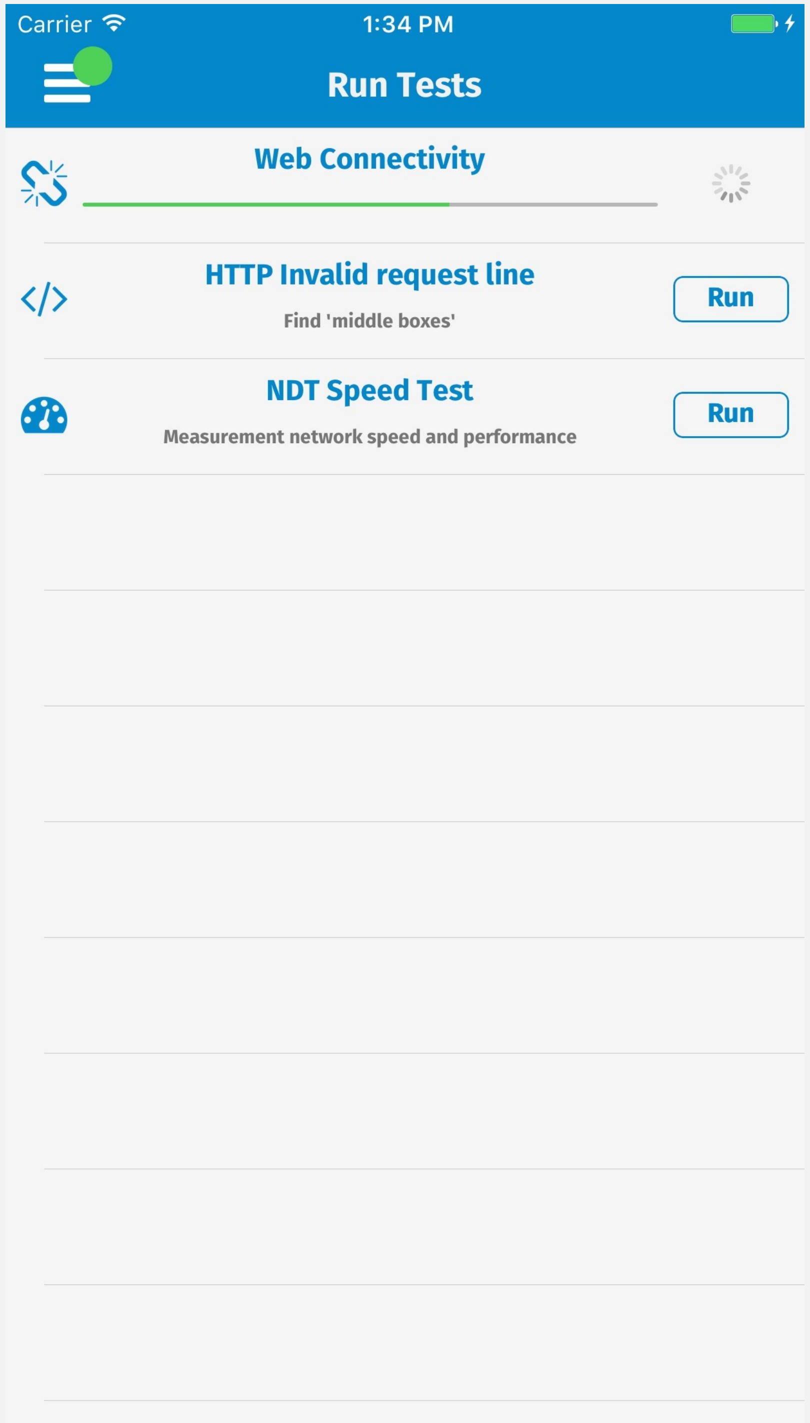
Test for Middle Boxes

Your recent test results will appear here once the tests have finished running! As you run more tests, you can view past results in the "Measurements" page.

ooniprobe web user interface

OONI
Getting Started
For information on how to download the latest
the Getting Started Guide, please visit

ooniprobe on RaspberryPi



Run Tests

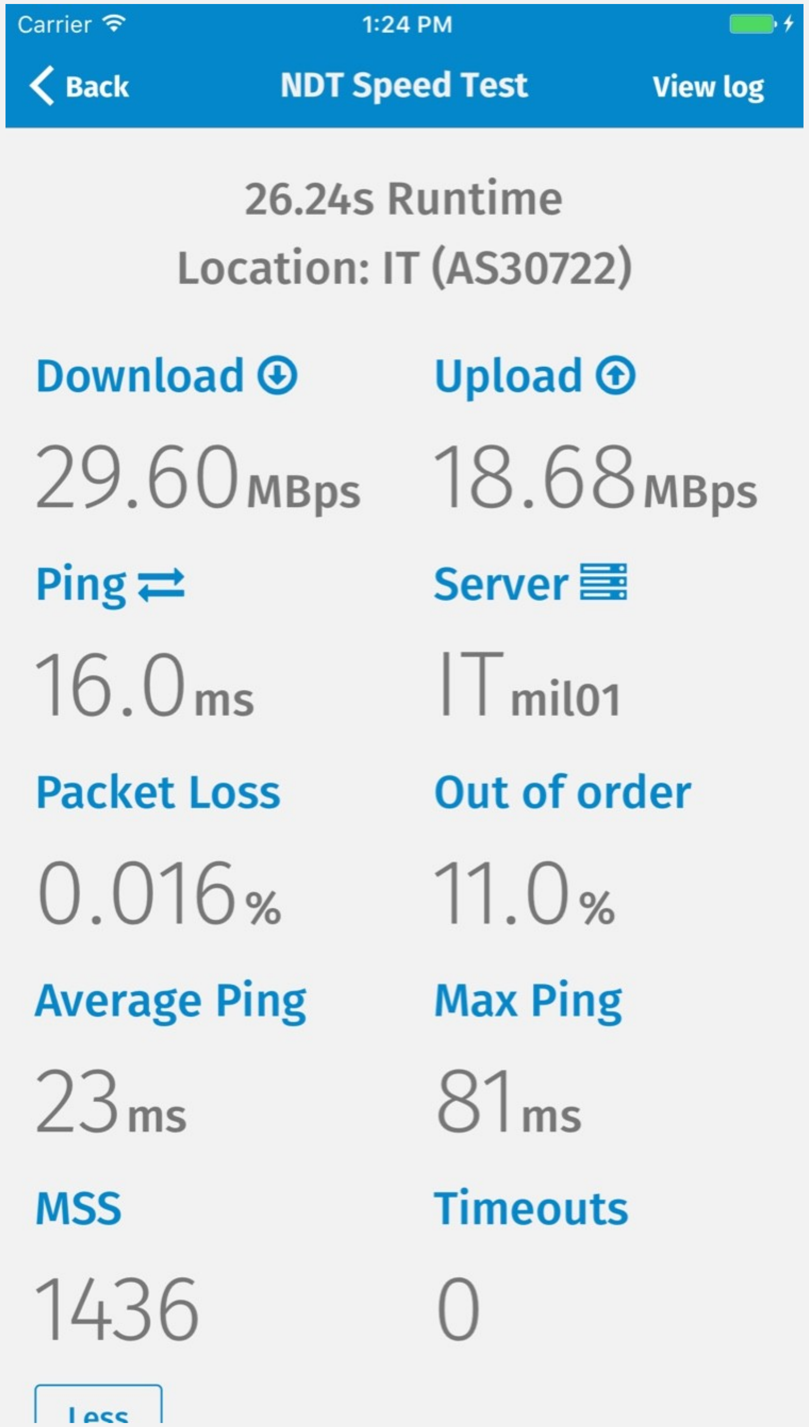
Web Connectivity

HTTP Invalid request line

Find 'middle boxes'

NDT Speed Test

Measurement network speed and performance



NDT Speed Test

26.24s Runtime
Location: IT (AS30722)

Download

29.60MBps

Upload

18.68MBps

Ping ⇄

16.0ms

Server

ITmil01

Packet Loss

0.016%

Out of order

11.0%

Average Ping

23ms

Max Ping

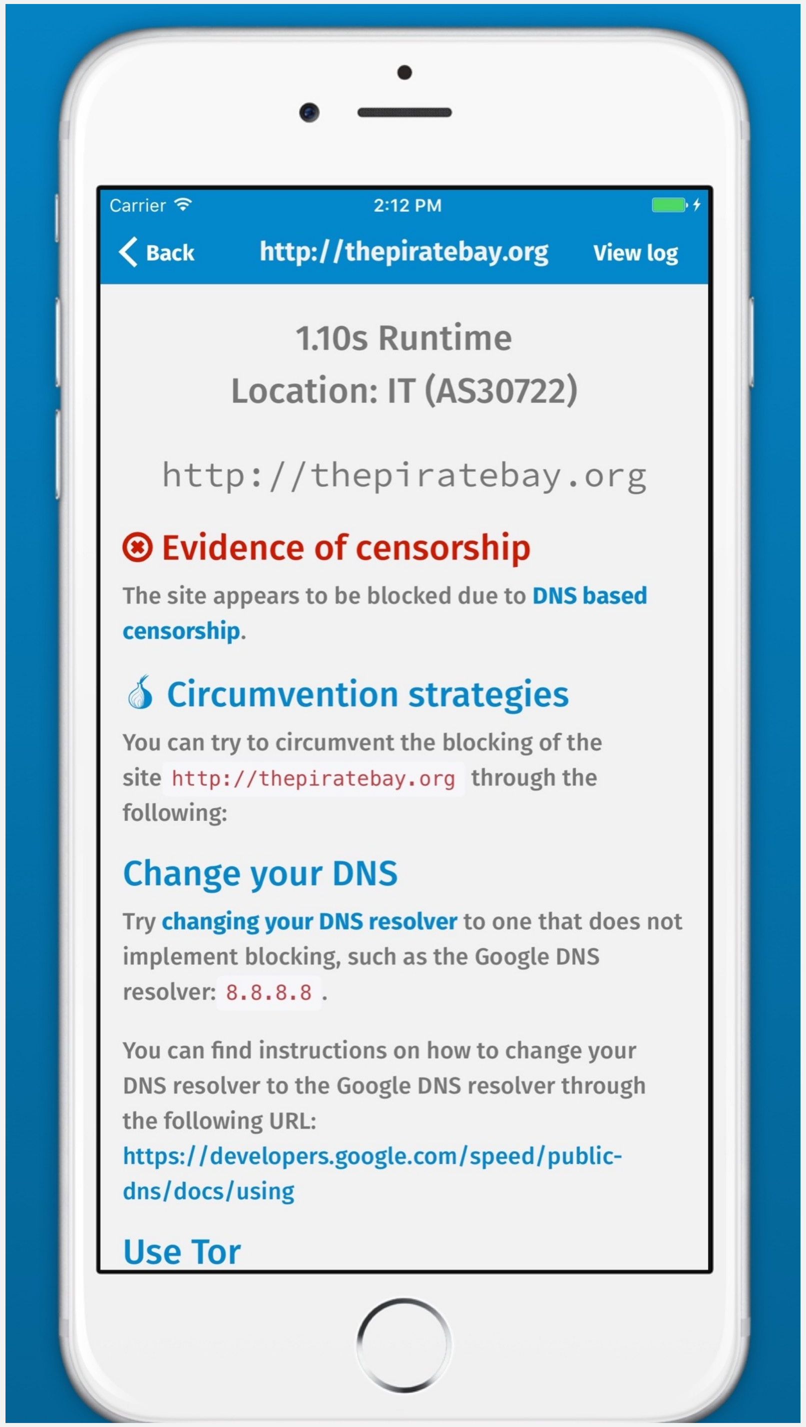
81ms

MSS

1436

Timeouts

0



http://thepiratebay.org

1.10s Runtime
Location: IT (AS30722)

```
http://thepiratebay.org
```

Evidence of censorship

The site appears to be blocked due to DNS based censorship.

Circumvention strategies

You can try to circumvent the blocking of the site `http://thepiratebay.org` through the following:

Change your DNS

Try changing your DNS resolver to one that does not implement blocking, such as the Google DNS resolver: `8.8.8.8` .

You can find instructions on how to change your DNS resolver to the Google DNS resolver through the following URL: https://developers.google.com/speed/public-dns/docs/using

Use Tor

ooniprobe mobile app

Risks: ooniprobe is a tool for investigations!

- Anyone monitoring your internet activity (e.g. ISP) will know that you are running ooniprobe.
- Types of URLs tested include provocative or objectionable sites (e.g. pornography).
- OONI's “HTTP invalid request line” test could be viewed as a form of “hacking”.
- The use of ooniprobe might potentially be viewed as illegal or anti-government activity.

https://ooni.torproject.org/about/risks/

Choices you can make

Contribute to test lists

Types of test to run

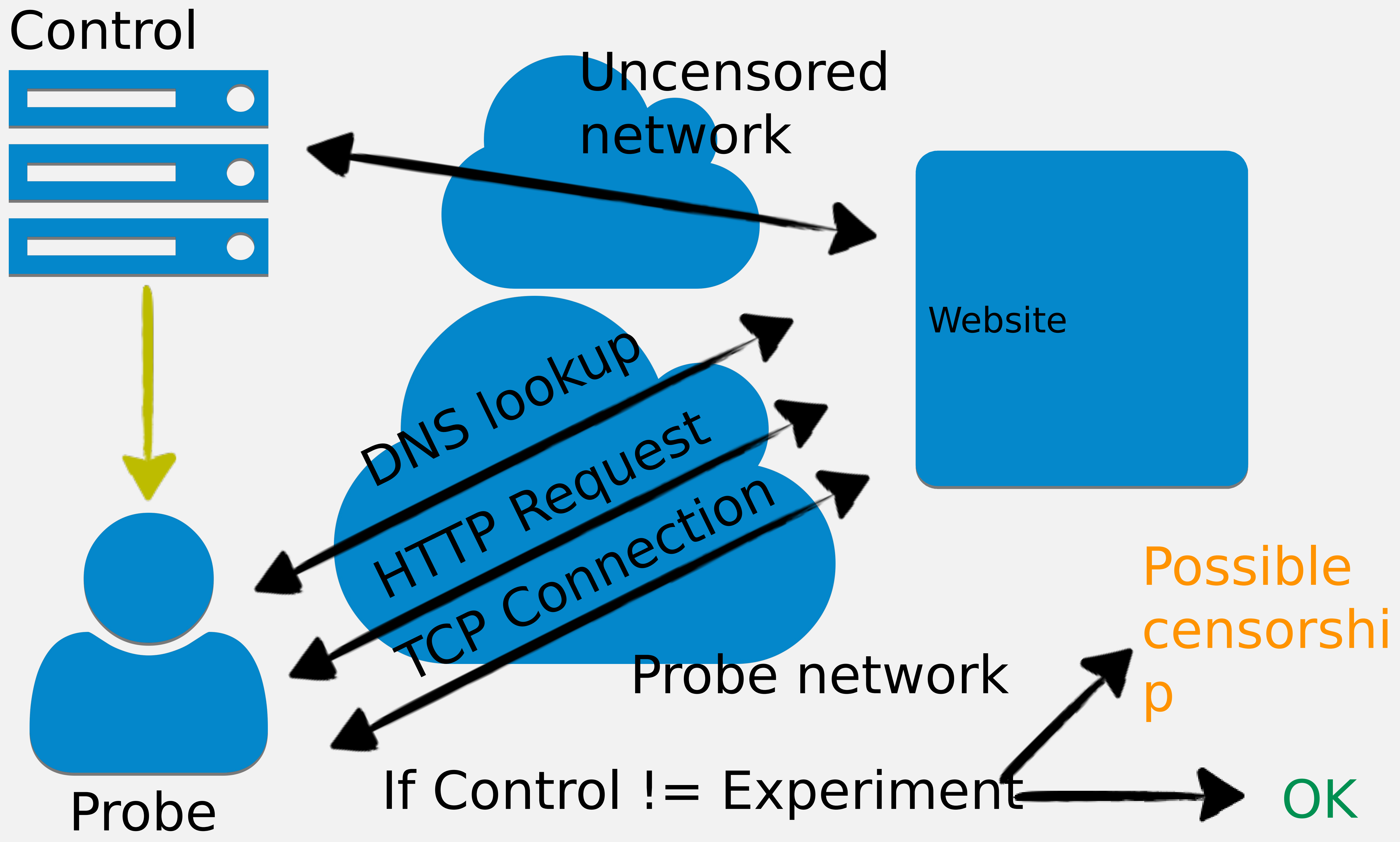
Privacy settings

How you upload data

Platform for running ooniprobe

Test lists: Determining which sites to test for censorship

- Global list: Internationally relevant websites
- Country-specific lists: Websites that are relevant to a specific country
- How to contribute to test lists: https://ooni.torproject.org/get-involved/contribute-test-lists/
- Citizen Lab github repo: https://github.com/citizenlab/test-lists



Web Connectivity

- DNS based blocking: If the DNS responses from the probe are inconsistent with those from the control

- TCP/IP blocking: If TCP connections to the resolved IPs fail

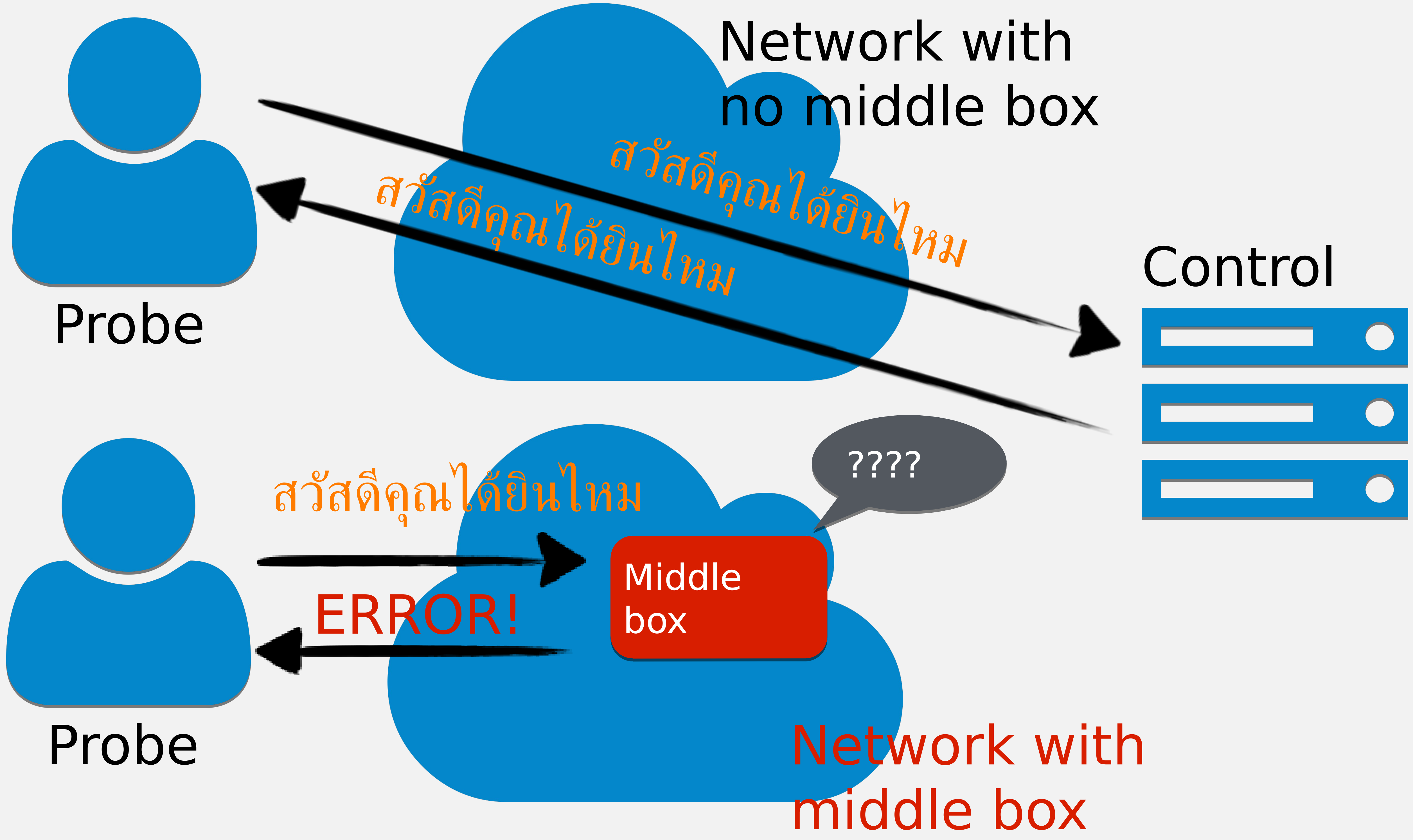
- HTTP based blocking: If only the HTTP request fails OR the pages does not match by looking at:
  - HTML Title tag
  - Body length
  - Response headers
  - HTTP status code

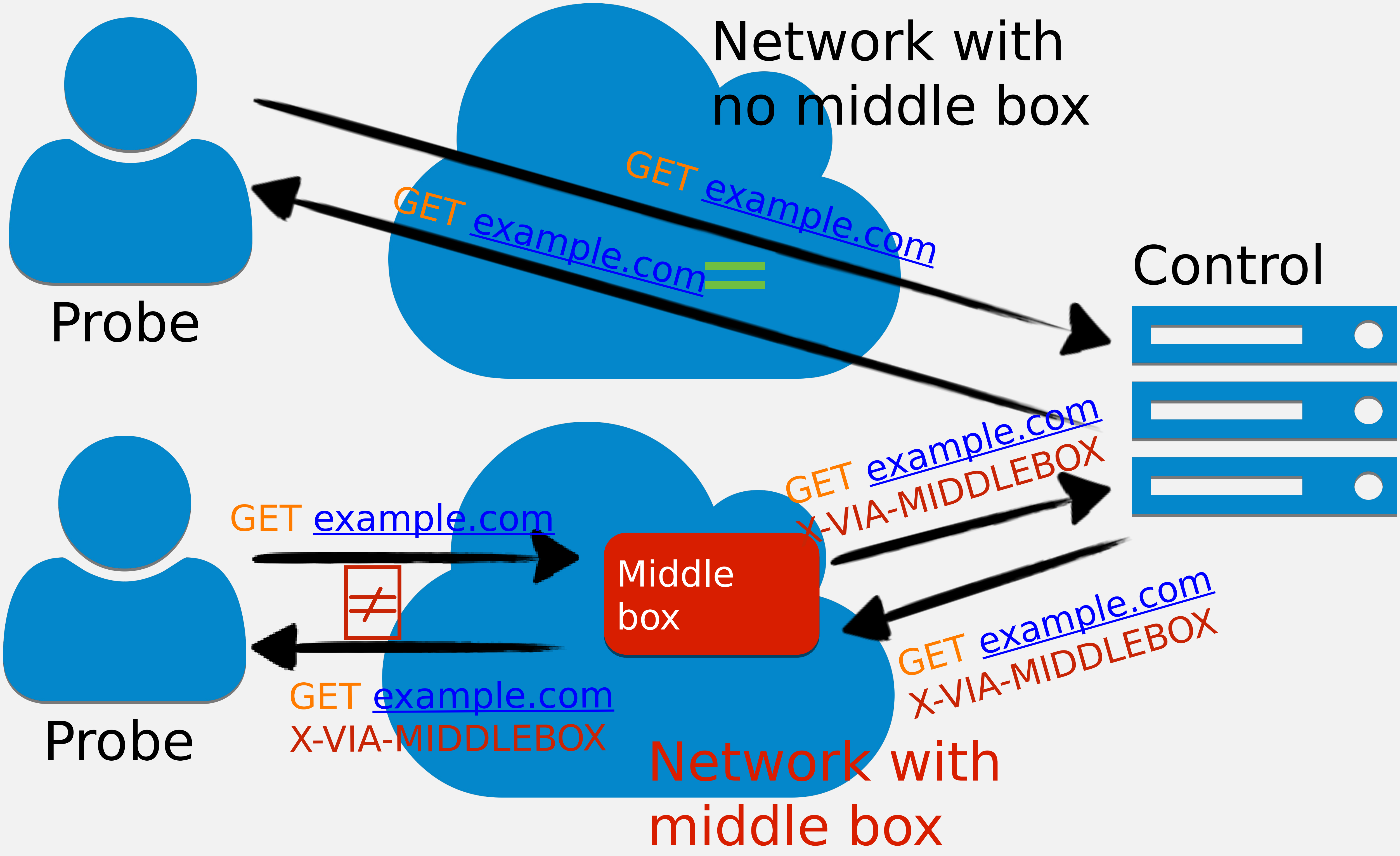
Web Connectivity

- False positives occur due to:
  - DNS resolvers (such as Google or your local ISP) often provide users with IP addresses that are closest to them geographically so that they can have faster access to sites
  - Some sites serve different content depending on the country that the user is connecting from
  - Sometimes it's hard to distinguish a network failure from a censorship event

Web Connectivity

HTTP Invalid Request Line





HTTP header
field manipulation

Middle boxes: Good or Bad?

- OONI has detected the presence of filtering technology across various countries around the world.

- However, not all proxy technologies are used for censorship and/or surveillance. Often, proxy technologies are, for example, used for caching purposes.

Data ooniprobe collects

- Country code (e.g. BR for Brazil)
- Autonomous System Number (ASN)
- Date & time of measurements
- Network measurement data (depending on the type of test)
- Note: IP addresses & other potentially identifying information might unintentionally be collected.
- OONI Data Policy: https://ooni.torproject.org/about/data-policy/

- Tor hidden services (recommended!)
- HTTPS collectors
- Cloud-fronting

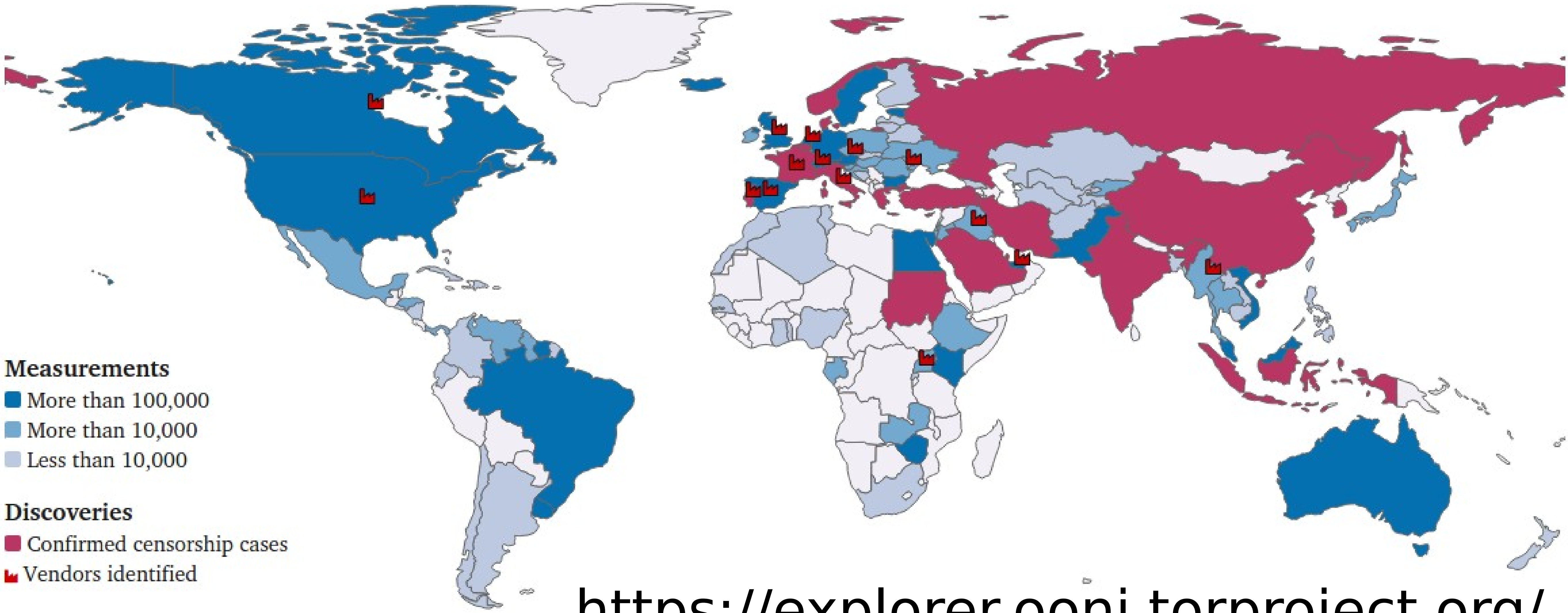
Uploading data to OONI servers

- Evidence of censorship events
- Transparency of global internet controls
- Allows researchers to conduct independent studies & to explore other research questions
- Allows the public to verify OONI's findings

Open Data

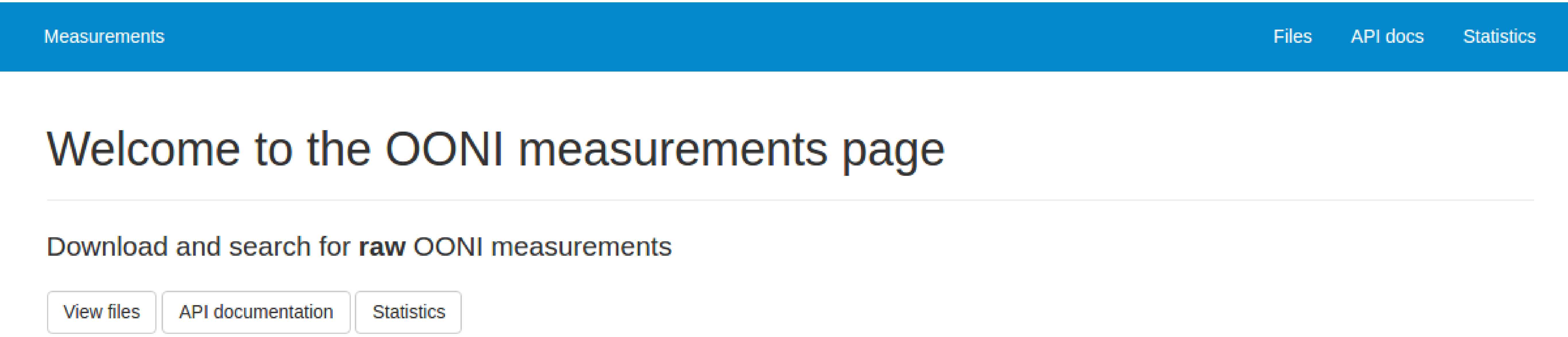
- Legality: Can the blocking of specific types of sites and services be legally justified?
- Circumvention tool strategies: When and where should censorship circumvention tools be promoted the most?
- Story-telling & Advocacy: Where are censorship events occurring and what is their impact on human rights?

Open Data



https://explorer.ooni.torproject.org/

OONI Explorer



Welcome to the OONI measurements page

Download and search for **raw** OONI measurements

https://measurements.ooni.torproject.org

Measurement API

- “Normal” and “anomalous” measurements.
- “Anomalous” measurements MIGHT contain evidence of censorship, but not necessarily (i.e. false positives).
- We only confirm a case of censorship when we have detected a block page.

Interpreting the data

Get involved!

- OONI Partnership Program
- Monthly community meetings on https://slack.openobservatory.org
- Run ooniprobe
- Contribute to test lists
- Analyze the data
- Tell stories
- Host an OONI workshop, spread the word! :)

- OONI: https://ooni.torproject.org/
- OONI Explorer: https://explorer.ooni.torproject.org/
- Download raw measurements: https://measurements.ooni.torproject.org/
- Software: https://github.com/TheTorProject/ooni-probe
- Contact the OONI team:
  contact@openobservatory.org
  Twitter: @OpenObservatory
  IRC: #ooni (irc.oftc.net) -
  https://slack.openobservatory.org/

Resources & contacts