

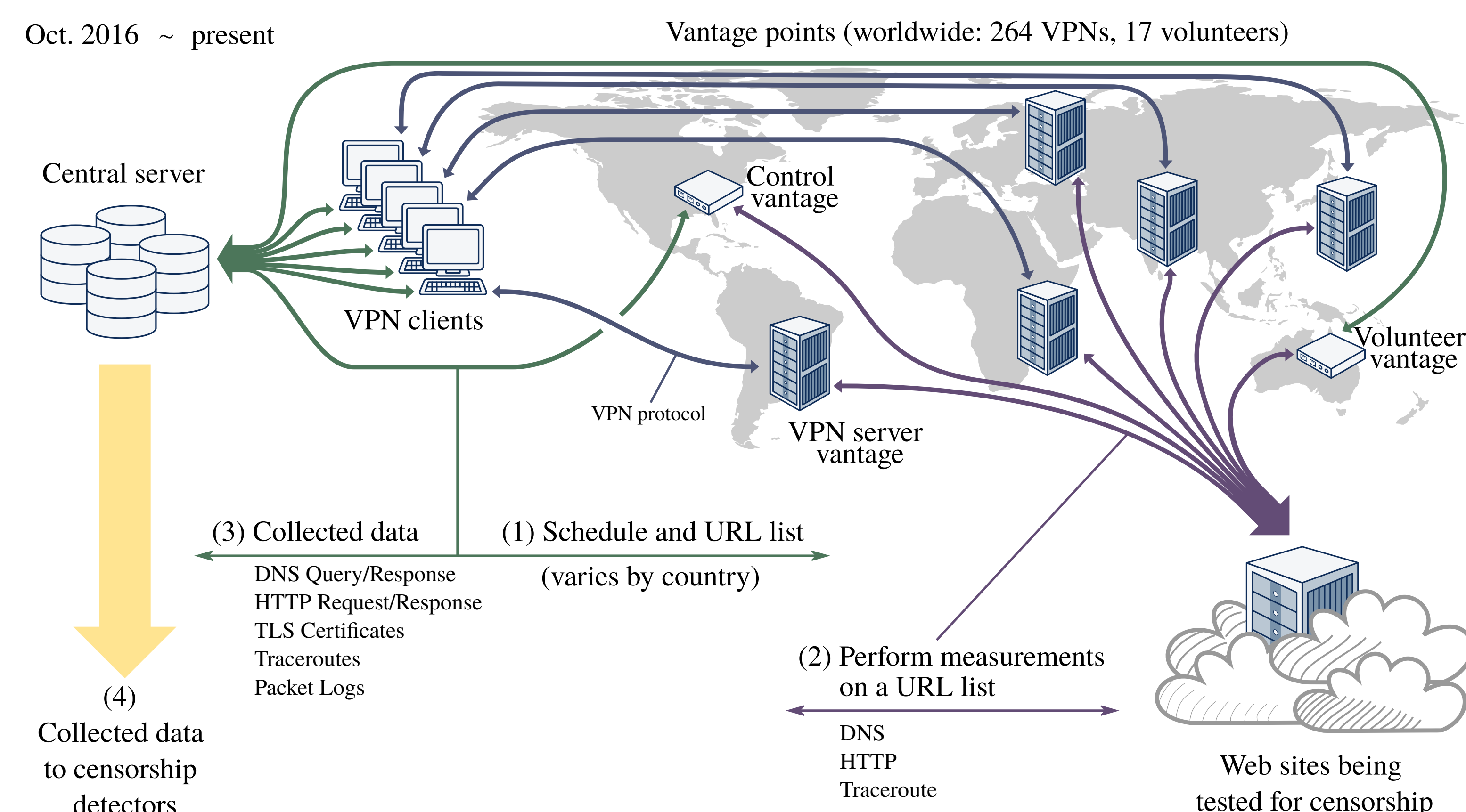
# ICLab: A Global, Longitudinal Internet Censorship Measurement Platform

To appear  
at IEEE S&P  
(Oakland)  
2020

Arian Akhavan Niaki, Shinyoung Cho, Zachary Weinberg  
Nguyen Phong Hoang, Abbas Razaghpanah, Nicolas Christin, Phillipa Gill

## Measurement platform specialized for censorship research

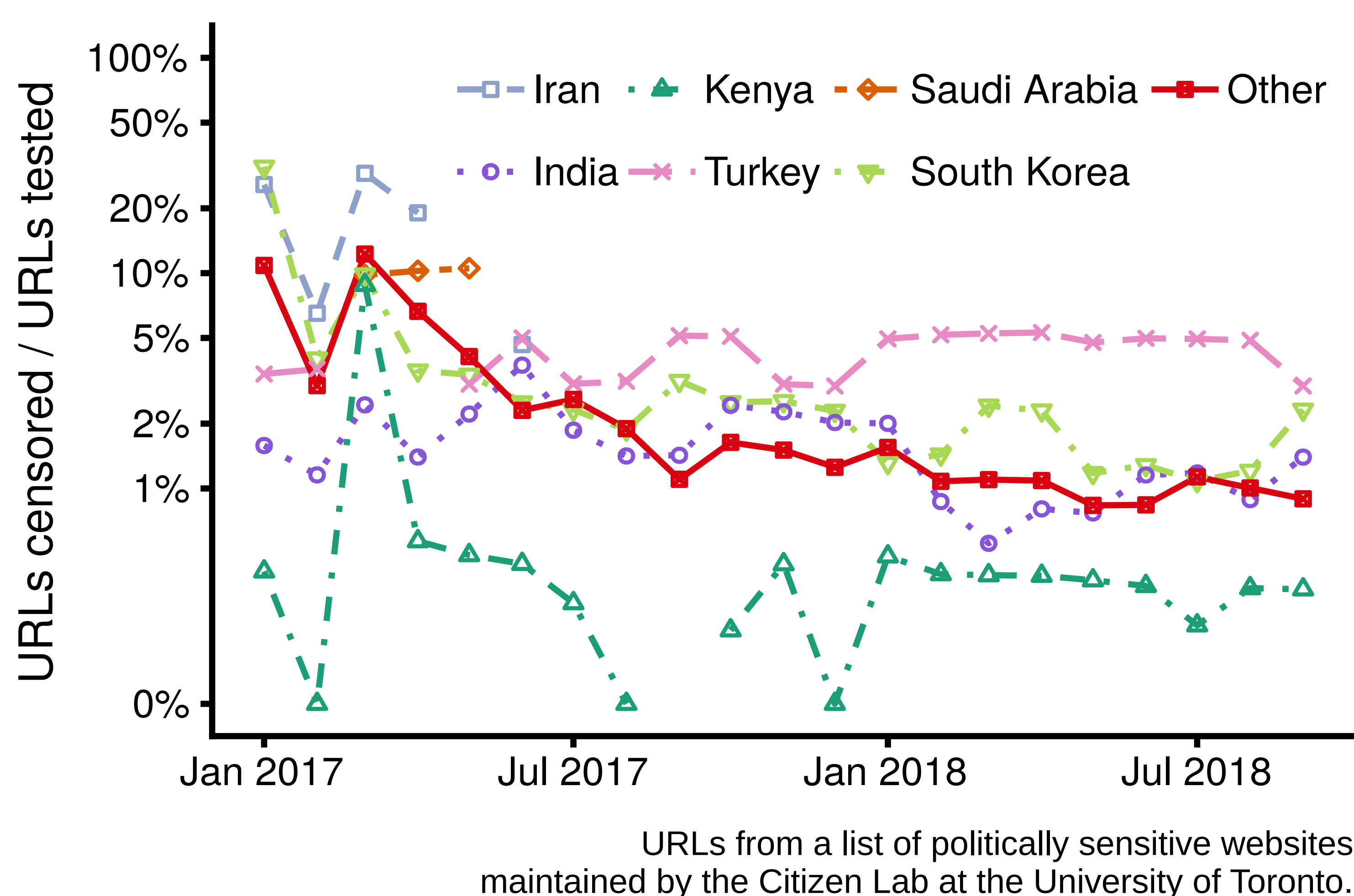
- Global, continuous monitoring
  - 234 ASes, 62 countries, 43,000 unique URLs
  - Ongoing data collection since 2016
- Avoid risk to volunteers
  - Use commercial VPNs where possible
  - Volunteer-operated devices only where safe
- Reliable detection of network interference
  - Data collected at all levels of network stack
  - False positives minimized
  - Raw data archived for future reanalysis
- Semi-automated discovery of new phenomena
  - Machine clustering of injected packets
  - Heuristic scoring of clusters, manual review



## Key findings

- Slow decline in # of censored websites
  - Probably due to increased use of HTTPS
  - No decline in the countries with the most aggressive policies
- Different methods used for different material
  - May be an attempt to conceal political censorship
  - Or may be two independent censors (e.g. local ISP, national backbone) going after different things
- Simple detectors have too many false positives
  - Must design detectors carefully
  - Packet-level logging helps
  - Manual verification is unavoidable
- We can detect other network attacks too
  - Surveillance for ad targeting
  - Cryptomining malware

## Observed censorship rates



## Example packet cluster

HTML structure

```
ACK+PSH
HTTP/1.1 200 OK
Connection: close
Content-Length: nnnn
Content-Type: text/html; charset="utf-8"
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN">
<html>
<head<title></title></head>
<body><h0><font color="black">
visible message
</font></h0></body></html>
```

Visible message

```
This URL has been blocked under instructions of a competent
Government Authority or in compliance with the orders of a Court
of competent jurisdiction.
***This URL has been blocked under Instructions of the Competent
Government Authority or Incompliance to the orders of Hon'ble
Court.*** [sic]
**"Error 403: Access Denied/Forbidden"**
404. That's an error.
HTTP Error 404 - File or Directory not found
HTTP Error 404 - File or Directory not found = http://...
```