Studying Transnational Routing Detours

Annie Edmundson, Roya Ensafi, Nick Feamster, Jennifer Rexford
Princeton University

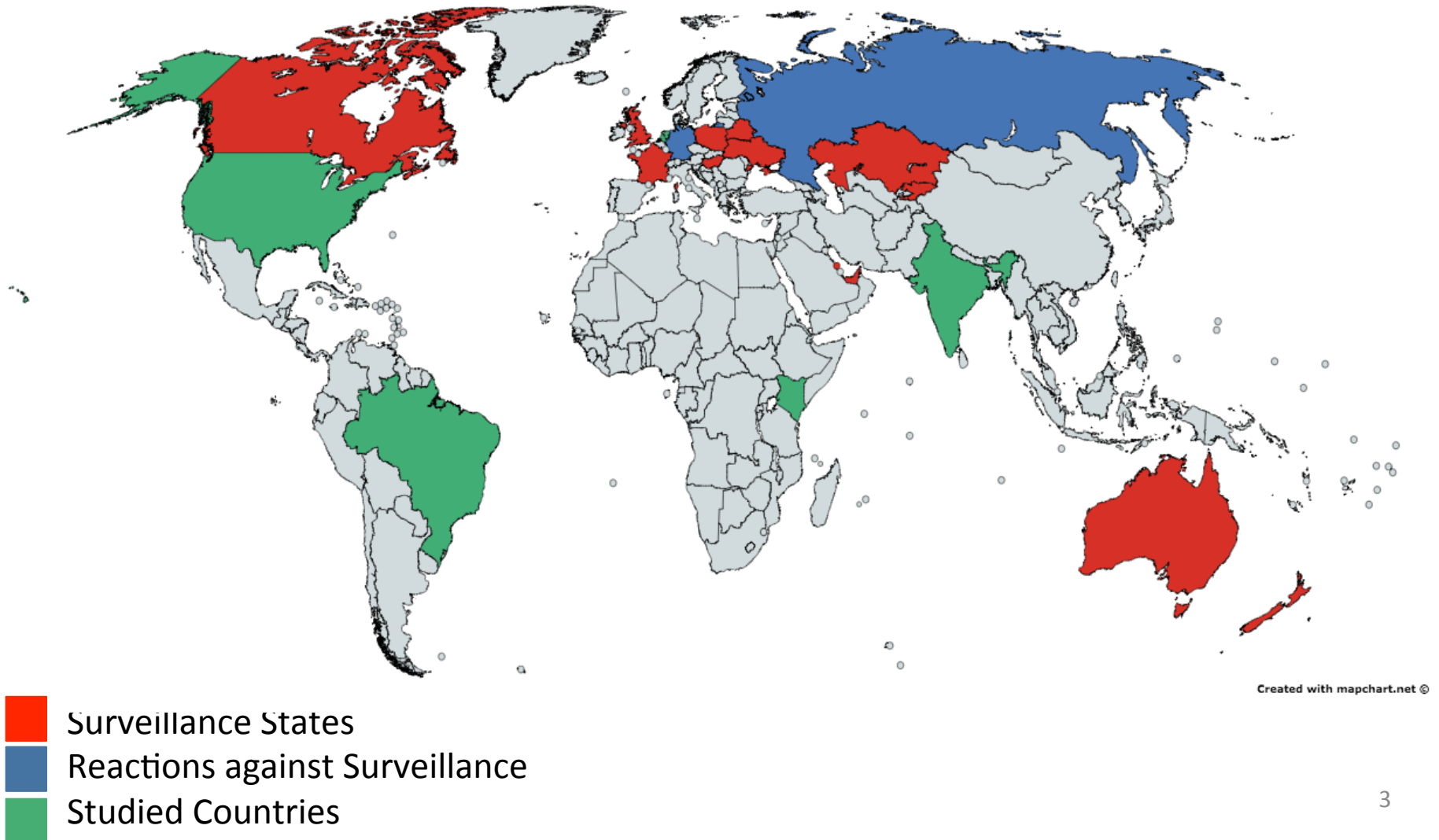# Characterizing and Avoiding Routing Detours

Characterizing detours

- Which countries are Internet paths to popular destinations currently traversing?
- Does local traffic leave the country? To where?

Avoiding detours

- Can end-users avoid certain countries to popular destinations?
- Can end-users keep more local traffic local?

Current State of Surveillance

Surveillance States

Reactions against Surveillance

Studied Countries

3

Characterizing and Avoiding Routing Detours

Characterizing detours

- Which countries are Internet paths to popular destinations currently traversing?
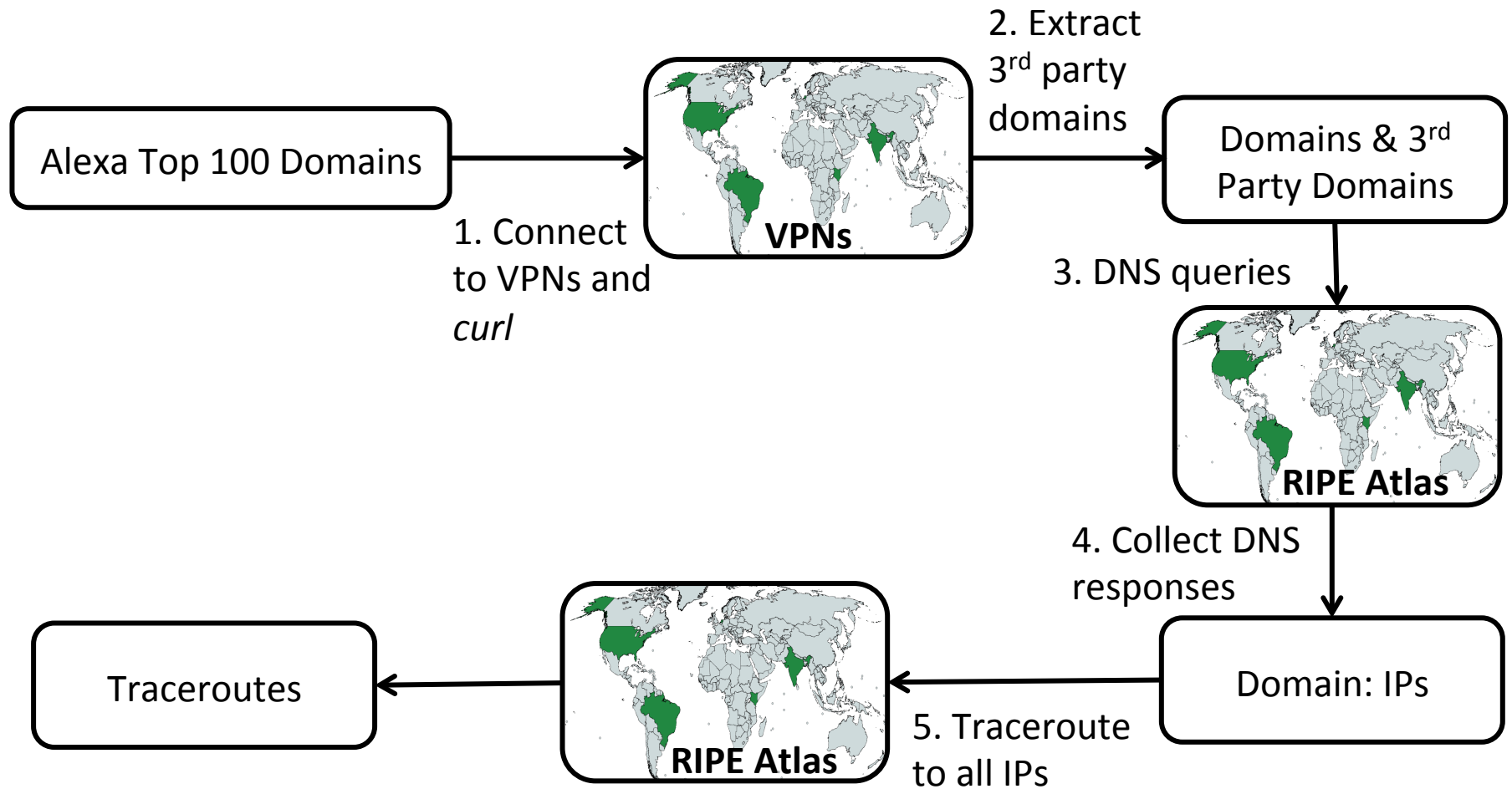- Does local traffic leave

The most common destination and transit country among all five countries studied is the United States.

Avoiding detours

- Can end-users avoid certain countries to popular destinations?
- Can end-users keep more local traffic local?

Measurement Study: Experiment

Alexa Top 100 Domains

1. Connect to VPNs and *curl*

VPNs

2. Extract 3rd party domains

Domains & 3rd Party Domains

3. DNS queries

RIPE Atlas

4. Collect DNS responses

Domain: IPs

5. Traceroute to all IPs

RIPE Atlas

Traceroutes

Where are popular domains hosted?

Terminating in Country	Brazil	Netherlands	India	Kenya	United States
Brazil	.169	-	-	-	-
Canada	.001	.007	.015	.006	-
United States	.774	.454	.629	.443	.969
France	.001	.022	.009	.023	.001
Germany	.002	.013	.014	.028	.001
Great Britain	-	.019	.021	.032	.002
Ireland	.016	.064	.027	.108	.001
Netherlands	.013	.392	.101	.200	.024
Spain	.001	-	-	-	-
Kenya	-	-	-	.022	-
Mauritius	-	-	-	.004	-
South Africa	-	-	-	.021	-
United Arab Emirates	-	-	-	.011	-
India	-	-	.053	.002	-
Singapore	-	.002	.103	.027	-

77.4% of paths that start in Brazil terminate in the United States

6

Which countries are on the path to popular domains?

Transiting Country	Brazil	Netherlands	India	Kenya	United States
Brazil	1.00	-	-	-	-
Canada	.013	.007	.016	.008	.081
United States	.844	.583	.715	.616	1.00
France	.059	.102	.104	.221	.104
Germany	.005	.050	.032	.048	.008
Great Britain	.024	.140	.204	.500	.006
Ireland	.028	.106	.031	.133	.006
Netherlands	.019	1.00	.121	.253	.031
Spain	.176	.004	-	-	-
Kenya	-	-	-	1.00	-
Mauritius	-	-	-	.322	-
South Africa	-	-	-	.334	-
United Arab Emirates	-	-	-	.152	-
India	-	-	1.00	.058	-
Singapore	-	.002	.270	.040	.003

84.4% of paths that start in Brazil have the United States on the path

Characterizing and Avoiding Routing Detours

Characterizing detours

- Which countries are Internet paths to popular destinations currently traversing?
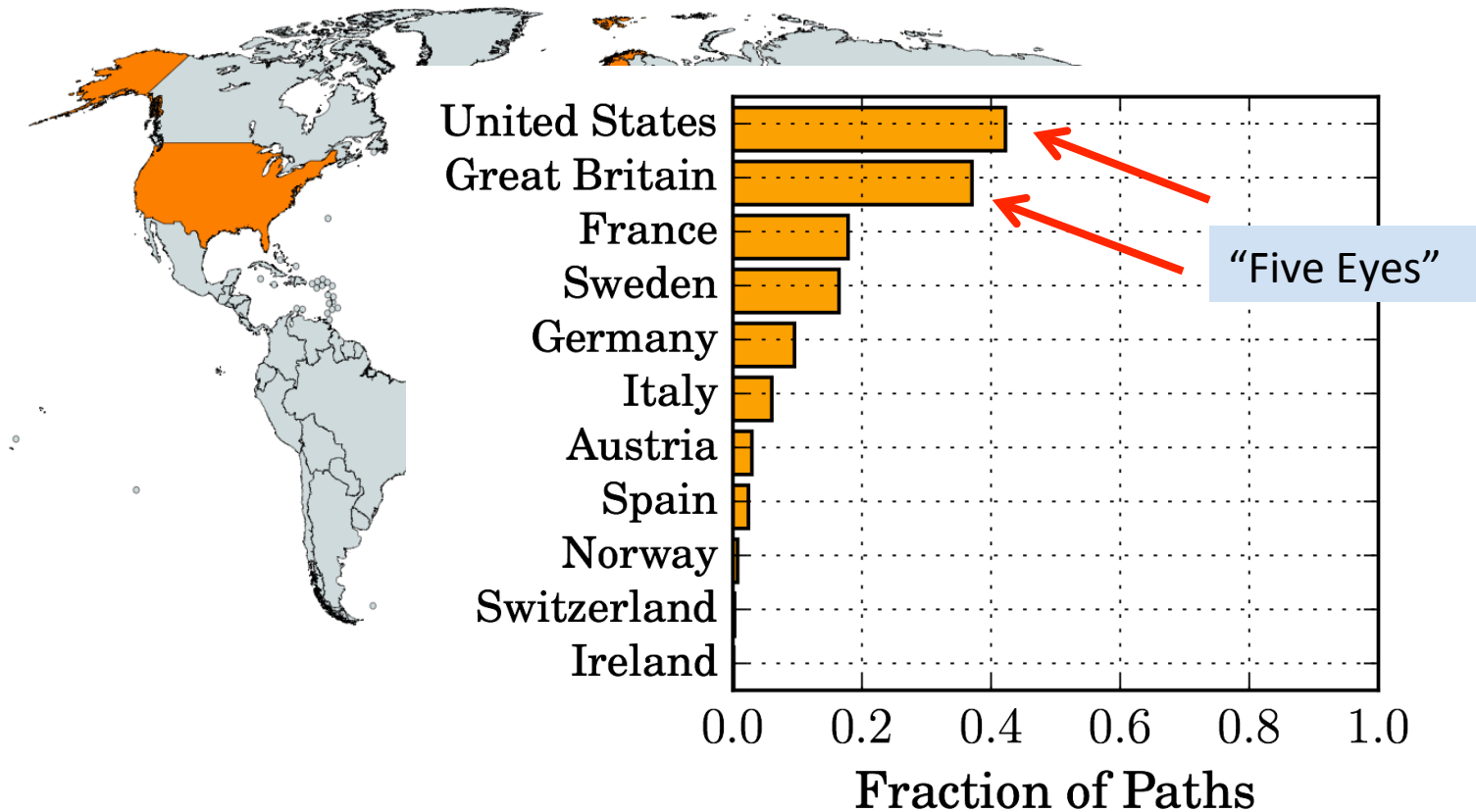
- Does local traffic leave the country? To where?

Despite having large IXPs, Brazil and Netherlands paths often trombones to the United States.

Avoiding detours

- Can end-users avoid certain countries to popular destinations?
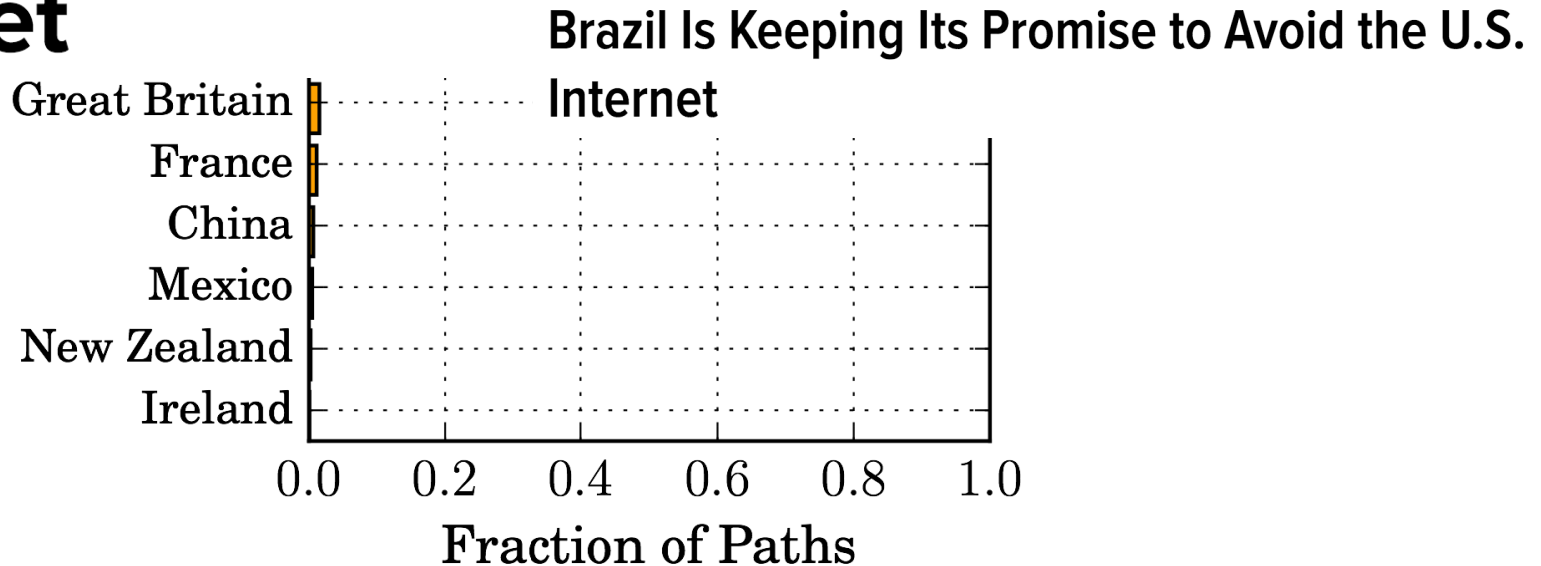- Can end-users keep more local traffic local?

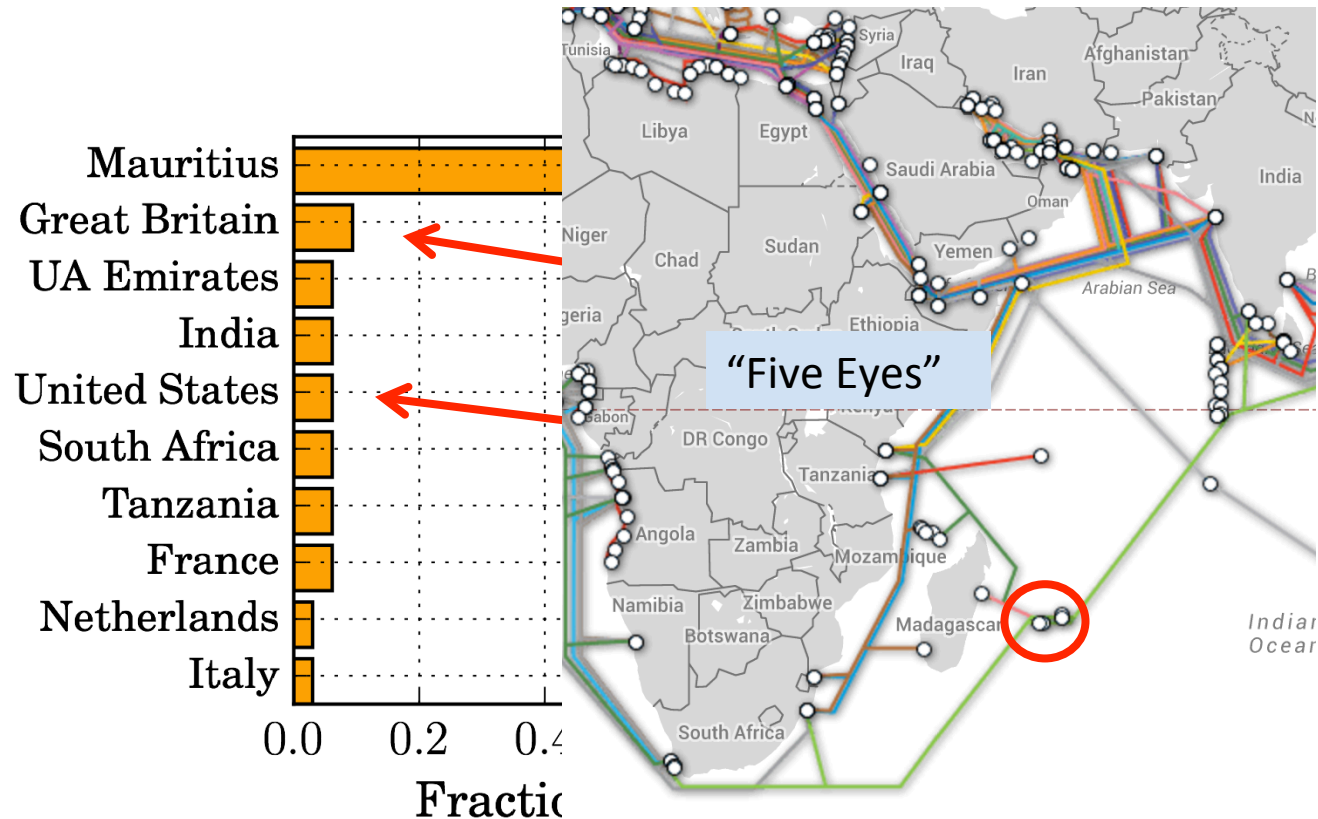# Netherlands: Where is local traffic going?

"Five Eyes"

Brazil: Where is local traffic going?

Brazil begins laying its own Internet cables to avoid U.S. surveillance

Brazil looks to break from US-centric Internet

Brazil Is Keeping Its Promise to Avoid the U.S. Internet

Kenya: Where is local traffic going?

Characterizing Routing Detours: Summary

- Routing detours often transit surveillance states – especially the United States

- Local traffic doesn't always stay local

- **Is it possible to avoid certain countries by tunneling traffic through relays?**

Characterizing and Avoiding Routing Detours

Characterizing detours

- Which countries are Internet paths to popular destinations currently traversing?
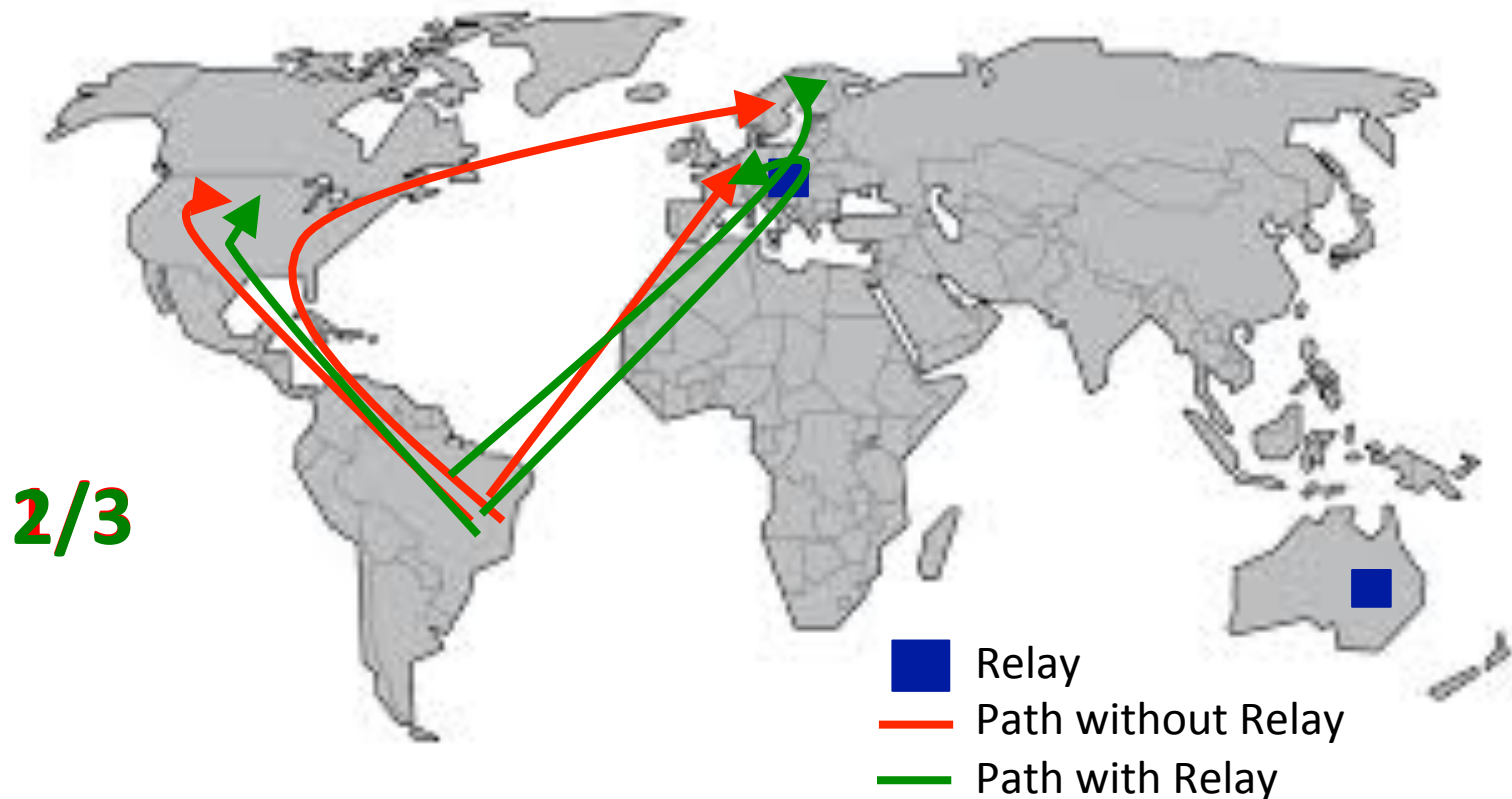- Does local traffic leave the country? To where?

Yes, but it's more difficult to avoid the United States than it is to avoid any other country.

Avoiding detours

- Can end-users avoid certain countries to popular destinations?
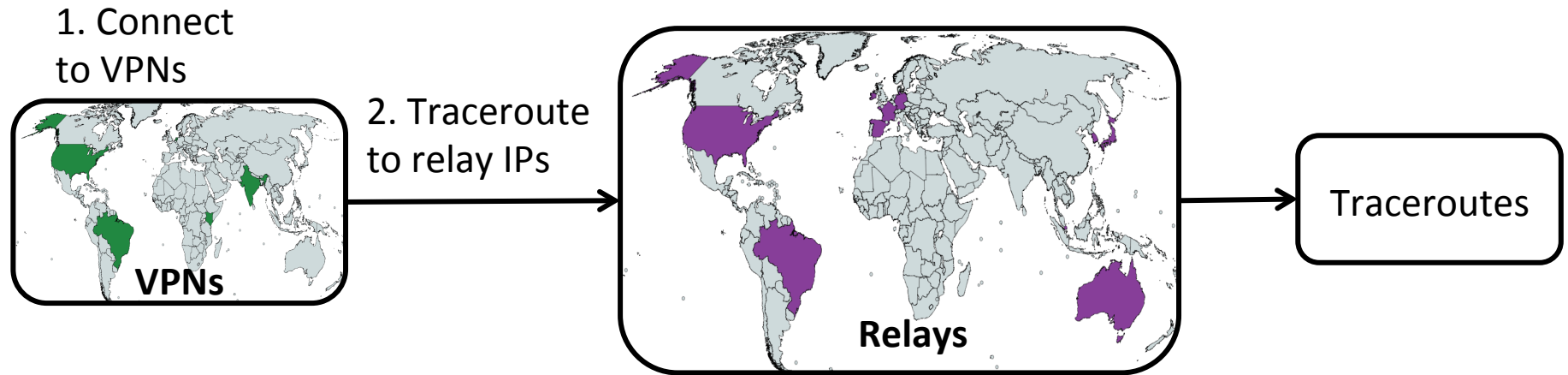- Can end-users keep more local traffic local?

Country Avoidance

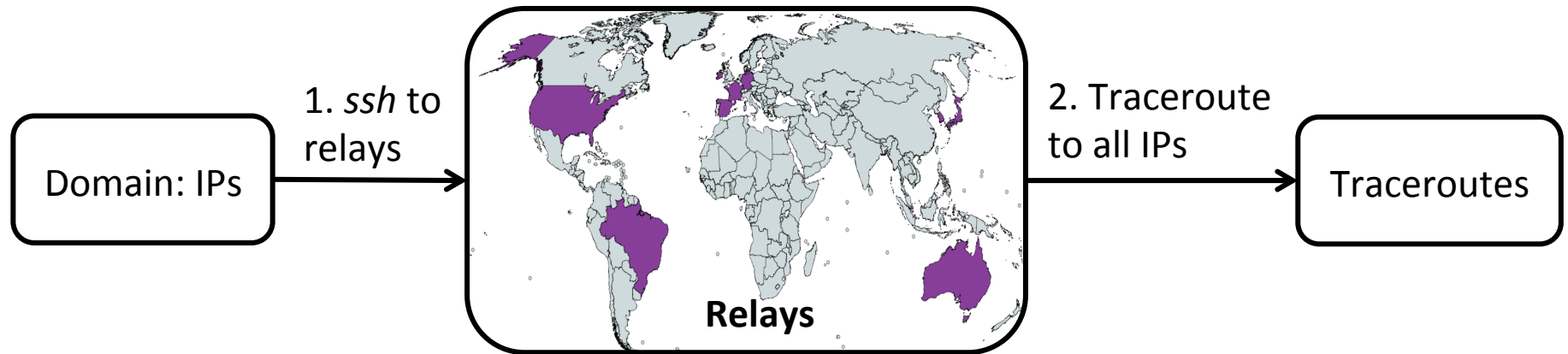- *Country Avoidance* = fraction of paths that do not pass through Country X

2/3

Relay
Path without Relay
Path with Relay

14

Avoidance Study: Experiment

1. Connect
to VPNs

2. Traceroute
to relay IPs

VPNs

Relays

Traceroutes

Relay to Server Path:

Domain: IPs

1. *ssh* to
relays

Relays

2. Traceroute
to all IPs

Traceroutes

15

Can clients avoid countries more often?

Yes – many countries are almost completely avoidable for the top 100 domains

Country to Avoid	Brazil		Netherlands		India		Kenya		United States	
	No Relay	*Relays*	*No Relay*	*Relays*	*No Relay*	*Relays*	*No Relay*	*Relays*	*No Relay*	*Relays*
Brazil	0.00	0.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Canada	.98	1.00	.99	1.00	.98	.98	.99	.99	.92	1.00
United States	.15	.62	.41	.63	.28	.65	.38	.40	0.00	0.00
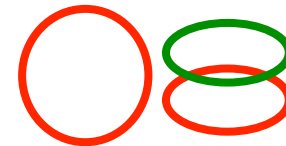
Characterizing and Avoiding Routing Detours

Characterizing detours

- Which countries are Internet paths to popular destinations currently traversing?
- Does local traffic leave the country? To where?

Tromboning Brazilian paths decreased from 13.2% to 9.7%.

Avoiding detours

- Can end-users avoid certain countries to popular destinations?
- Can end-users keep more local traffic local?

Avoiding Routing Detours: Summary

- It is more difficult to avoid the United States than it is to avoid any other country

- Tromboning Brazilian paths decreased from 13.2% to 9.7%

Future Work

- Connectivity within a country

- Relationship between IXPs and nation state routing

- Country avoidance based on IPv4 vs. IPv6 connectivity

Conclusion

- Paths commonly traverse known surveillance states – 84% of paths from Brazil traverse the United States

- Relays can help prevent routing detours, but some of the more prominent surveillance states are the least avoidable

- Tromboning Brazilian paths decreased from 13.2% to 9.7% with relays.

Full write-up and more data at:

ransom.cs.princeton.edu

Relays as Proxies

- Relays act as proxies
- Modify Proxy Auto-Configuration (PAC) file

```
function FindProxyForURL(url, host) {
    if (dnsDomainIs(host, "www.google.com") ) {
        return "PROXY 4.5.6.7:8080";
    } else if (dnsDomainIs(host, "www.youtube.com") ) {
        return "PROXY 4.5.6.7:8080";
    } else if (dnsDomainIs(host, "www.twitter.com") ) {
        return "PROXY 7.8.9.10:8080";
    } else if (dnsDomainIs(host, "aws") ) {
        return "PROXY 1.2.3.4:8080";
    } else {
        return "DIRECT";
    }
}
```