Anonymity, Privacy, and Circumvention: Tor in the Real World

Jacob Appelbaum <jacob@torproject.org>
The Tor Project
https://www.torproject.org/

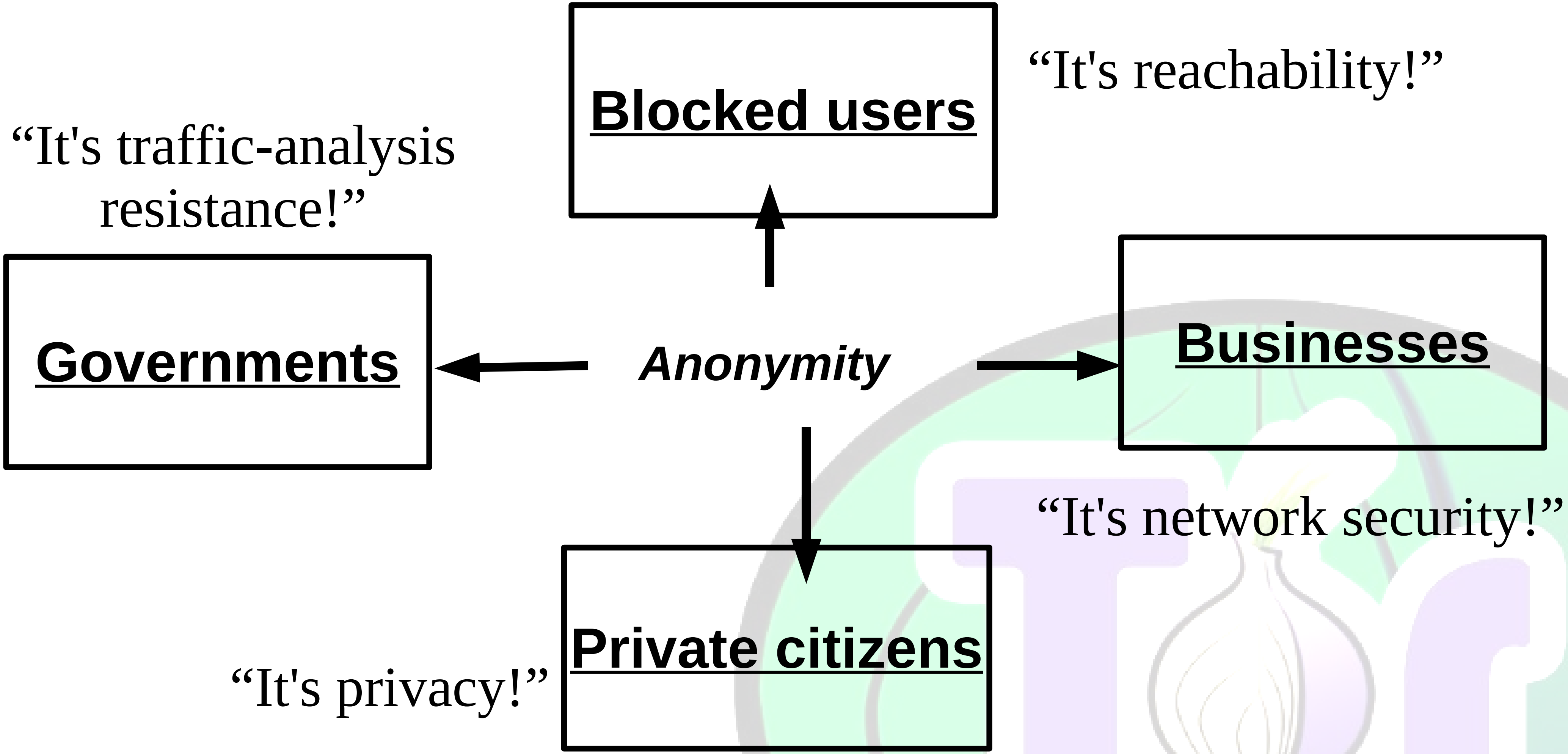
About me:

- Free software hacker (Tor, libmsr, blockfinder, etc)
- General human and other animal rights activist
- Founder of Noisebridge
- Cold Boot Attack
- MD5 Considered Harmful Now: Constructing a Rogue CA Certificate
- Cult of the Dead Cow member
- Chaos Computer Club supporter
- EFF supporter
- **Tor Project Developer**

Tor: Big Picture

- Freely available (Open Source), unencumbered.
- Comes with a spec and full documentation: Dresden, Aachen, Yale groups implemented their own compatible Java Tor clients; researchers use it to study anonymity.
- 2000 active relays, 250,000+ active users, >3Gbit/s.
- Official US 501(c)(3) nonprofit. Seven funded developers, dozens more dedicated volunteers.
- Funding from U.S. Naval Research Lab, Electronic Frontier Foundation, Voice of America, Human Rights Watch, NLnet, Google, ...you?

Anonymity serves different interests for different user groups.



Anonymity

Blocked users

“It's reachability!”

Governments

“It's traffic-analysis resistance!”

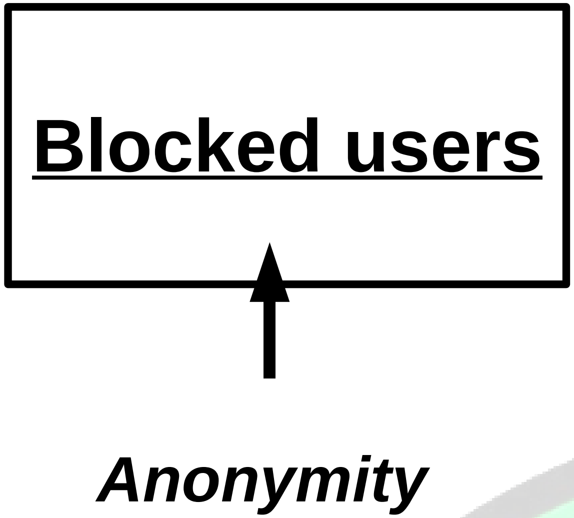
Businesses

“It's network security!”

Private citizens

“It's privacy!”

Anonymity in the context of a censored or blocked user?



Confidentiality of their requests.

Integrity of the data in transit.

Privacy from the source and destination networks.

Lets talk about censorship

Censorship in the form of **forced**, *non-democratic* network filtering is ever-present in the world.

Network filtering is as *pervasive* as it is *invasive:*

I've recently spent a few years traveling and training people to use Tor; I'd like to share some anecdotal information I've learned about censorship.

Lets talk about censorship

Censorship does not serve humanity and in fact humanity becomes a slave to the truth of its censors.

History should not be erased, voices should not be silenced; The solution to *subjectively* **bad** speech is objectively ***more speech***.

Most of my examples are about the current triumph of **bureaucratic authoritarianism** over fundamental rights of the individual.

Who ***really*** uses Tor?

People often wonder: “Who would use Tor?” Their feelings often come from a position of blindness of privilege or out of conjecture rooted in their own subjective experience. During my recent travels in the Middle East, I personally trained people from all over the Arab and Persian world. They generally came from the following groups:

- Bloggers & students
- Journalists and their audience members
- IT professionals
- Human rights activists and likely whistleblowers

A crash course in Tor

Tor is a peer to peer network with a focus on anonymity, privacy and security.

- Tor is used for *anonymous* TCP connections
- It has (limited) DNS query support
- Tor relays publish to directory authorities
- Directory authorities create a consensus
- Clients bootstrap by downloading the consensus
- Clients choose their own network path
- No logins, no passwords, no fees or costs

There's a lot more to this protocol.
Read our specifications or ask me!

Why bother with all of this?

A single hop proxy ***is*** a single point of failure. Its use allows for blocking, risks temptation of abuse untrusted operators, or worse: allows for wiretaps to surveil unsuspecting or even ***targeted*** users.

At best a single hop proxy is encrypted, not monitored and the administrator is trusted. Often these proxies are *blocked*, **not encrypted**, **monitored by multiple parties**, and the administrator is able to **target users**.

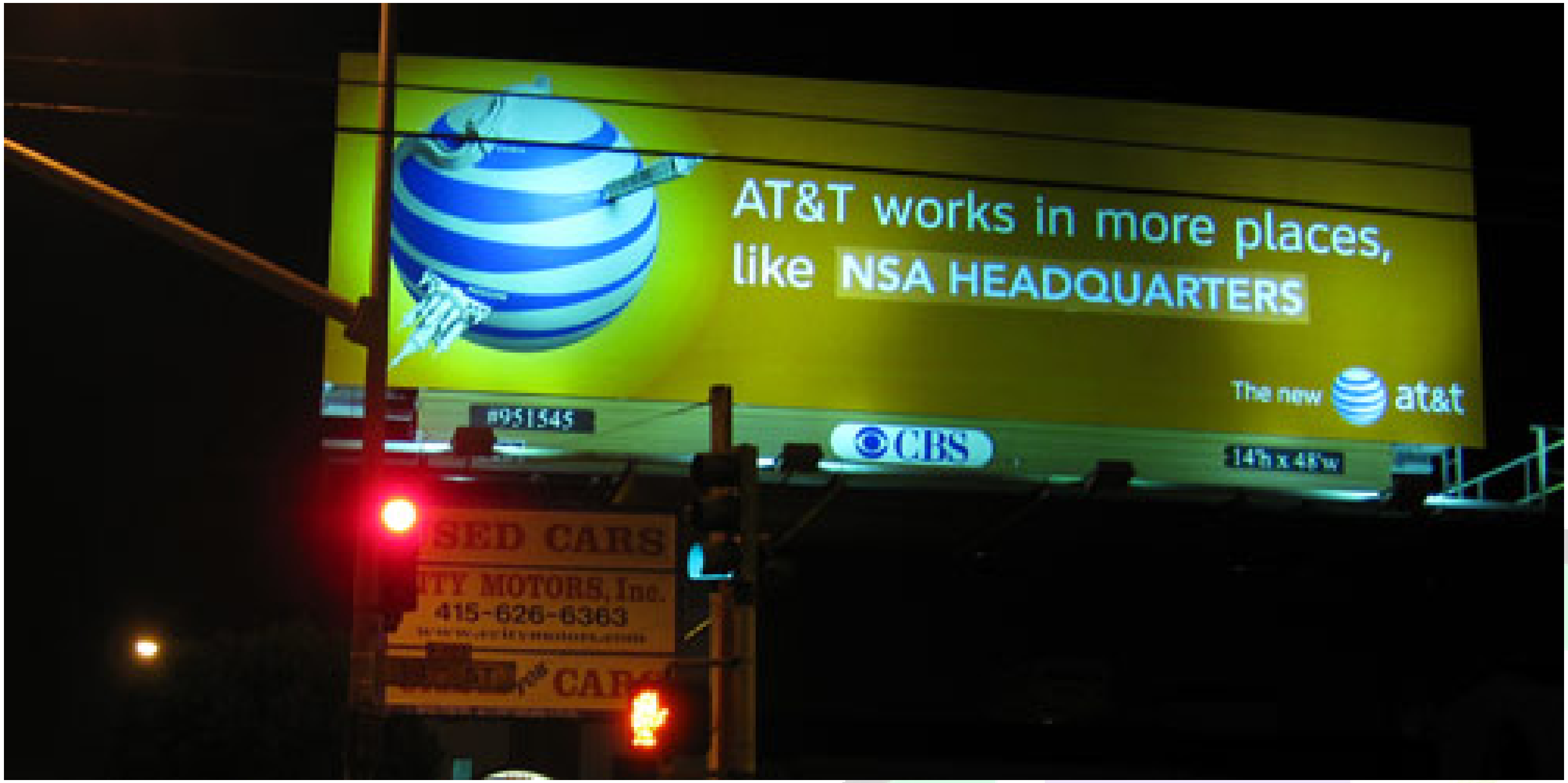
What's their threat model?

In January 2010, the Iranian National police chief Esmail Ahmadi-Moghaddam stated:

*"These people should know where they are sending the **SMS** and **email** as these systems are under control. They should not think using **proxies** will prevent their **identification**. If they continue ... those who organize or issue appeals (about opposition protests) have **committed a crime worse than those who take to the streets**"*

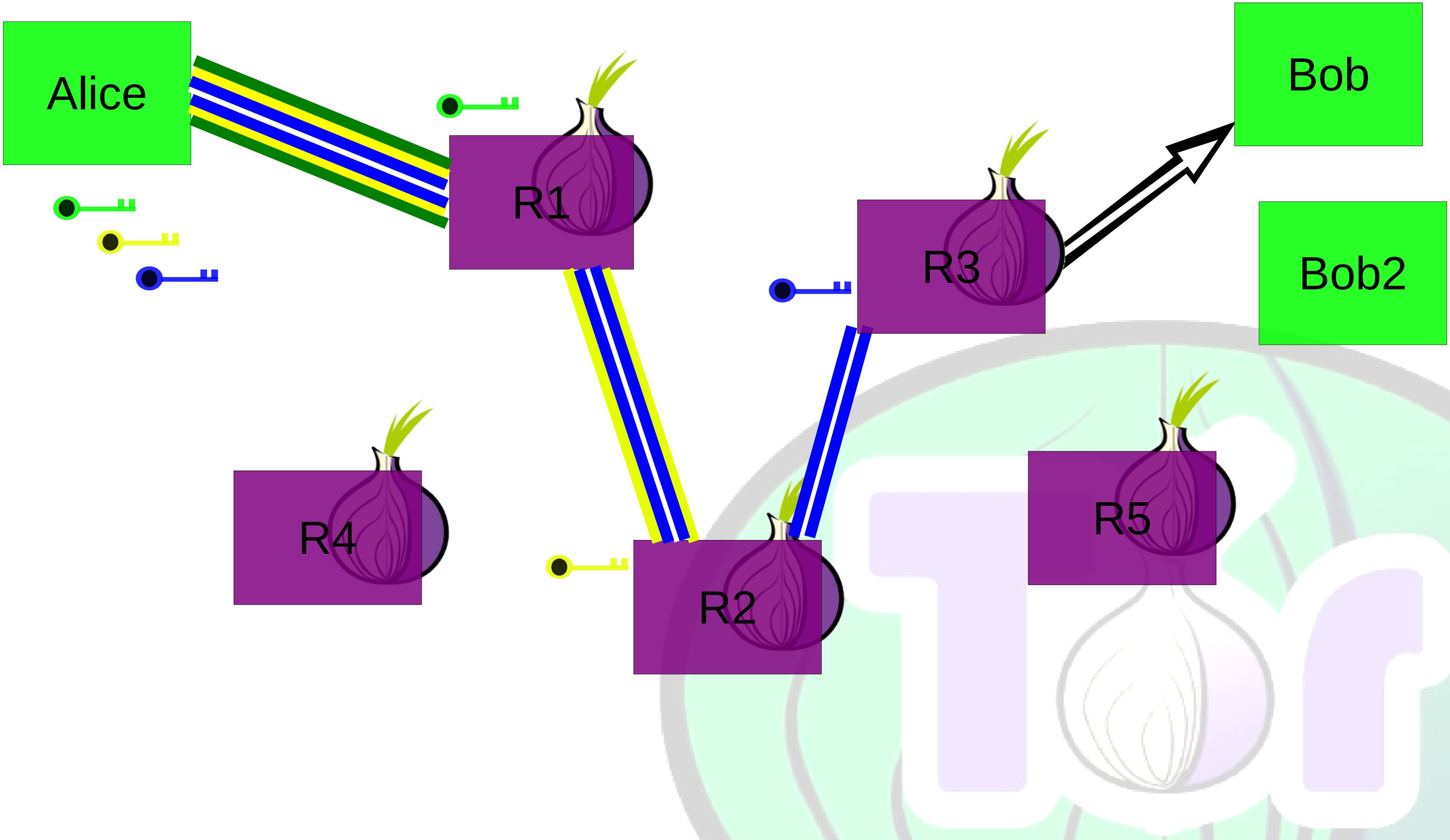
They're afraid and they're *hunting*. They've created a **Filternet**; An alternate view of reality as dreamed up by the authorities rather than the internet as it is **objectively**. This does not serve humanity in the short or long term.

Why are we any different?

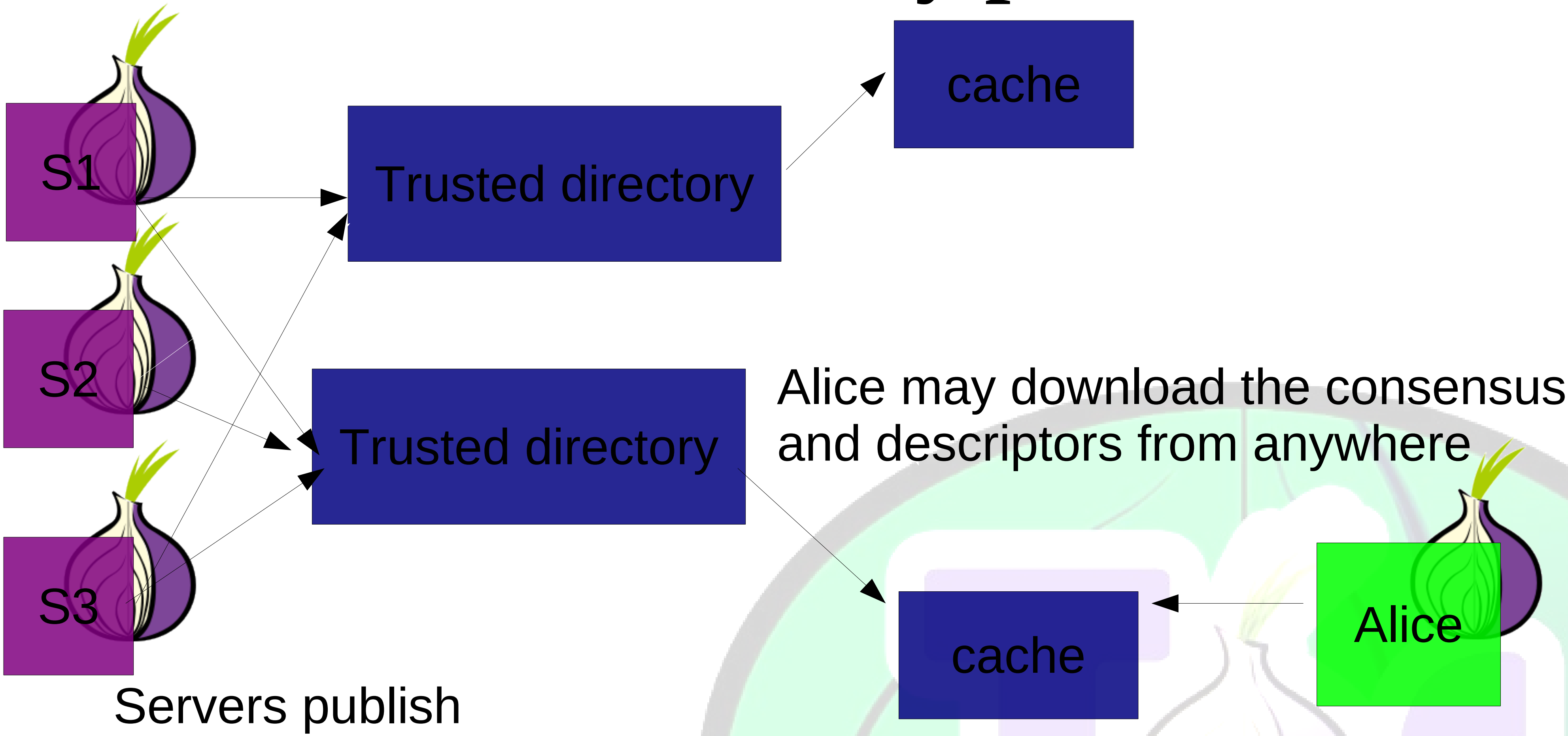


Is the government wiretapping in the United States substantially different? What stories will your log files tell about you in ten years' time? What about logs that tell a story that isn't yours?

Tor avoids the single hop paradigm;
This is Privacy by Design!



The basic Tor design uses a simple centralized directory protocol.

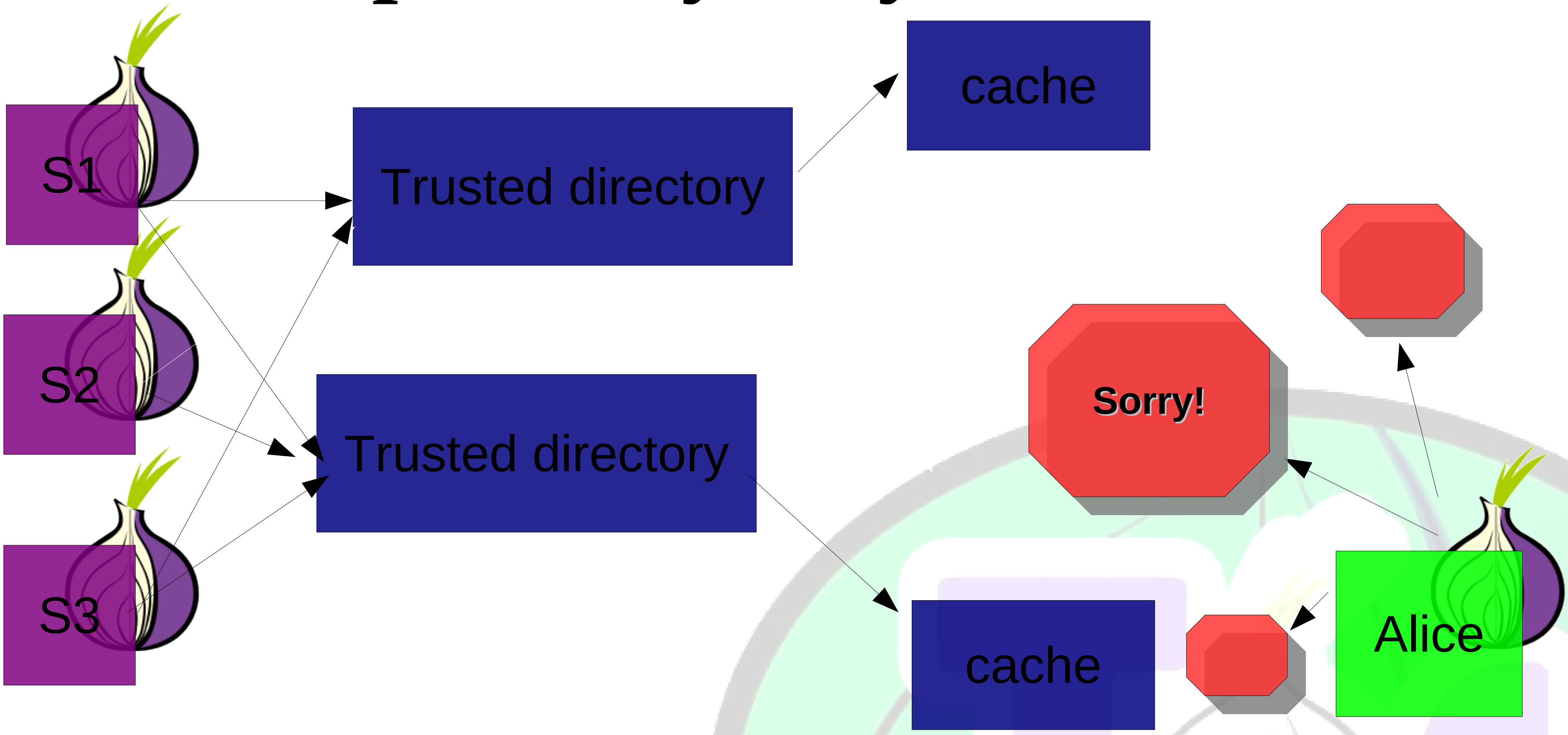


Alice may download the consensus and descriptors from anywhere

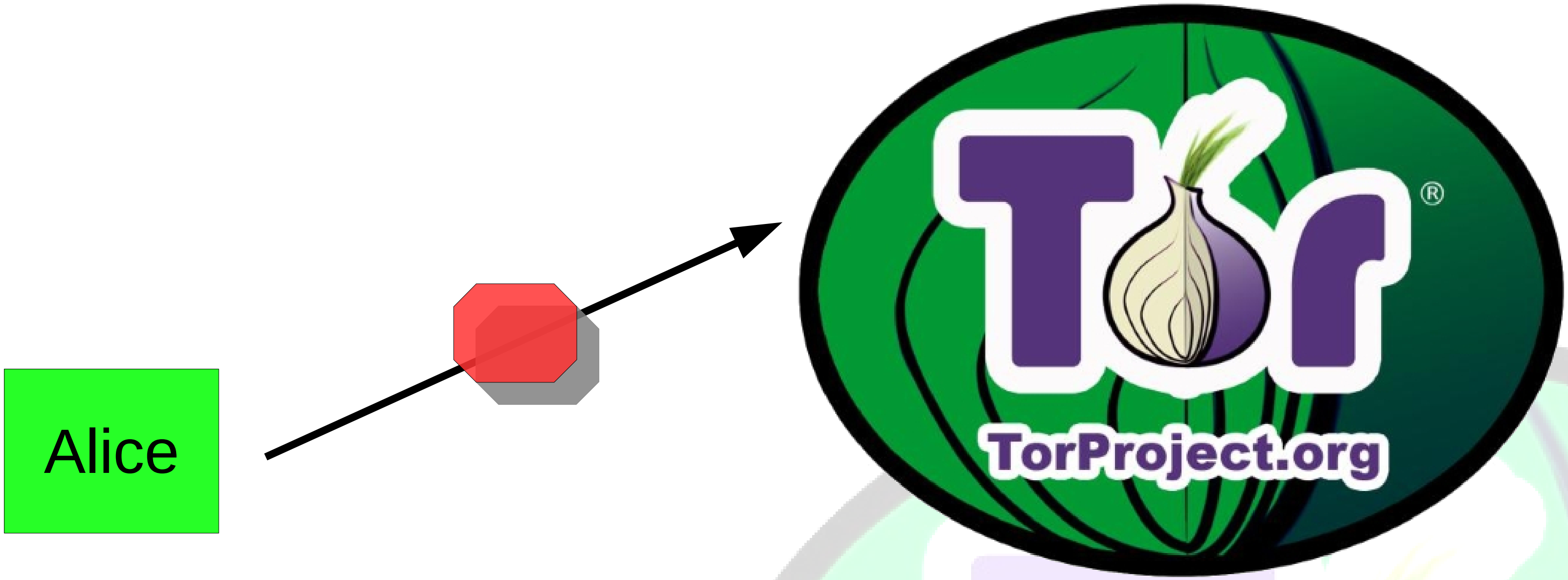
Servers publish self-signed descriptors.
We call these servers relays.

Authorities publish a signed consensus list of all relay descriptors

The basic Tor design is also exceptionally easy to block.



Many governments simply block attempts to download Tor



China, Iran, Lebanon, Qatar, etc;
The list is longer each day!

We deliver: Tor via email

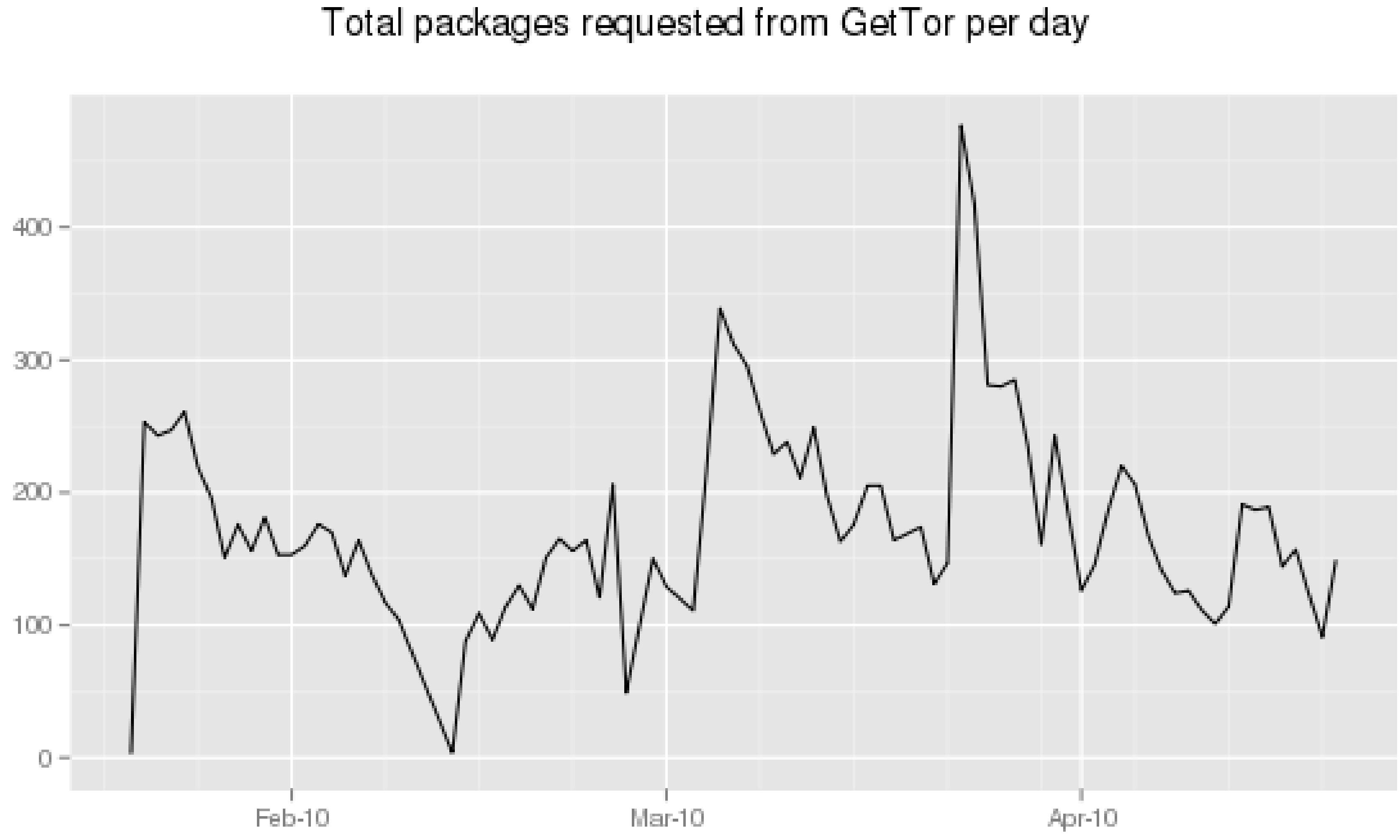
If the Tor Project website is blocked we offer Tor via an email robot that goes by the name GetTor.

Simply send an email to ***gettor@torproject.org*** and we'll send you whatever you'll need to bootstrap a Tor client.

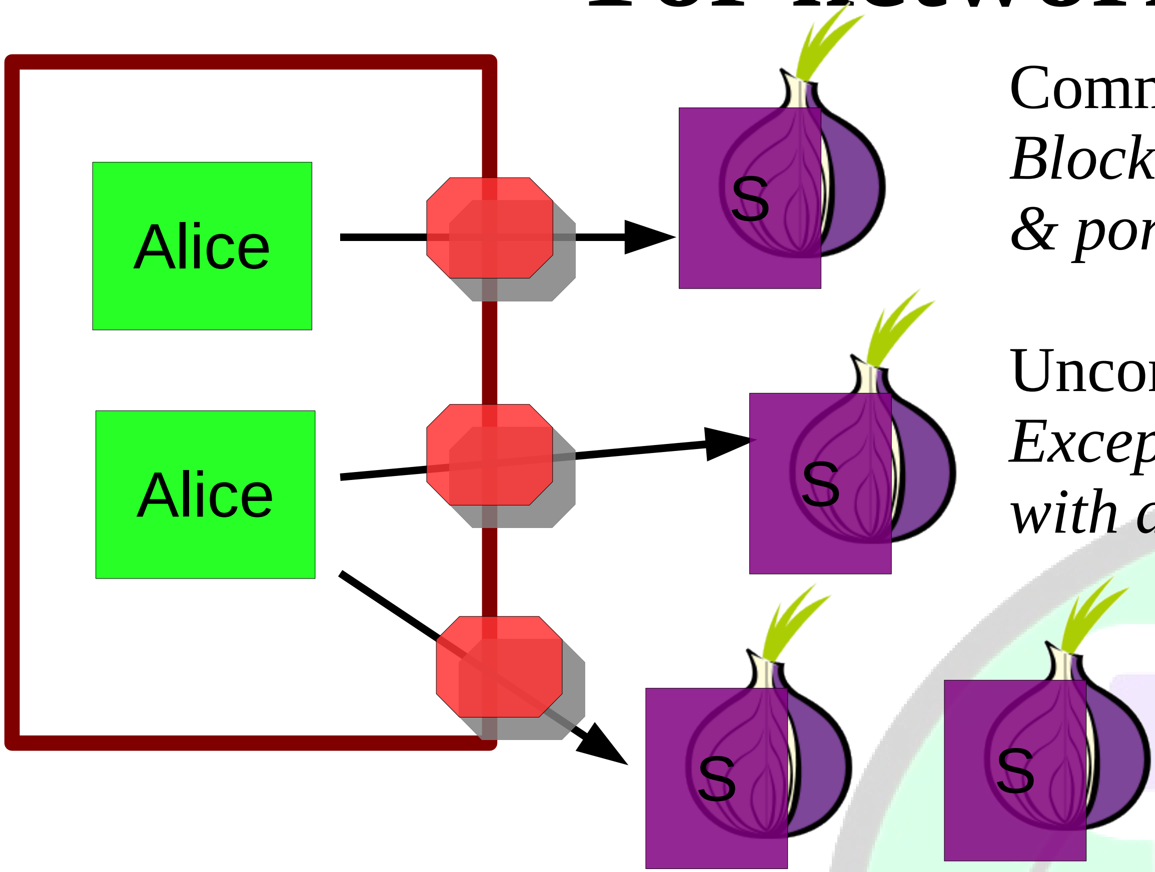
We have alternative methods too – contact us and we'll be happy to try to help you.

This is popular in many countries.

How many people are using GetTor?



Governments and other firewalls may block the whole publicly known Tor network.



Commonly we see:
Block lists including IP address & port number

Uncommonly we hear about:
Exception policy based networks with default deny policies

The directories *must* give clients a list of IP addresses and port numbers. This makes filtering connections to the Tor network very simple with the right firewall placement.

Is there a (blocking) resistance?

Of course.

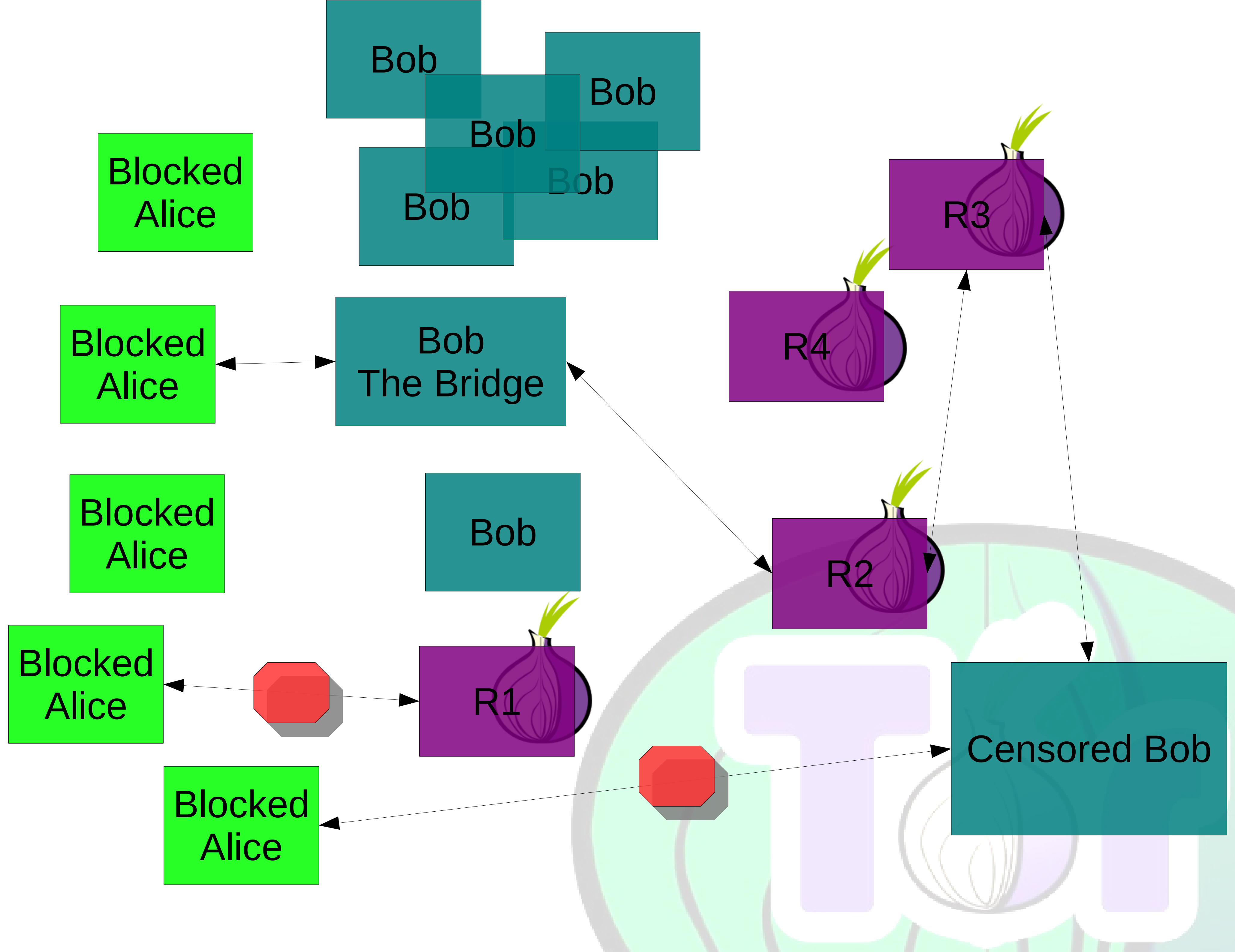
It's important to not lose hope. We simply need a layer of indirection between us and the public Tor network.

Mutual aid and solidarity provide methods for two kinds of solutions. We call the general solution a *bridge*.

Bridges are our partial darknet solution

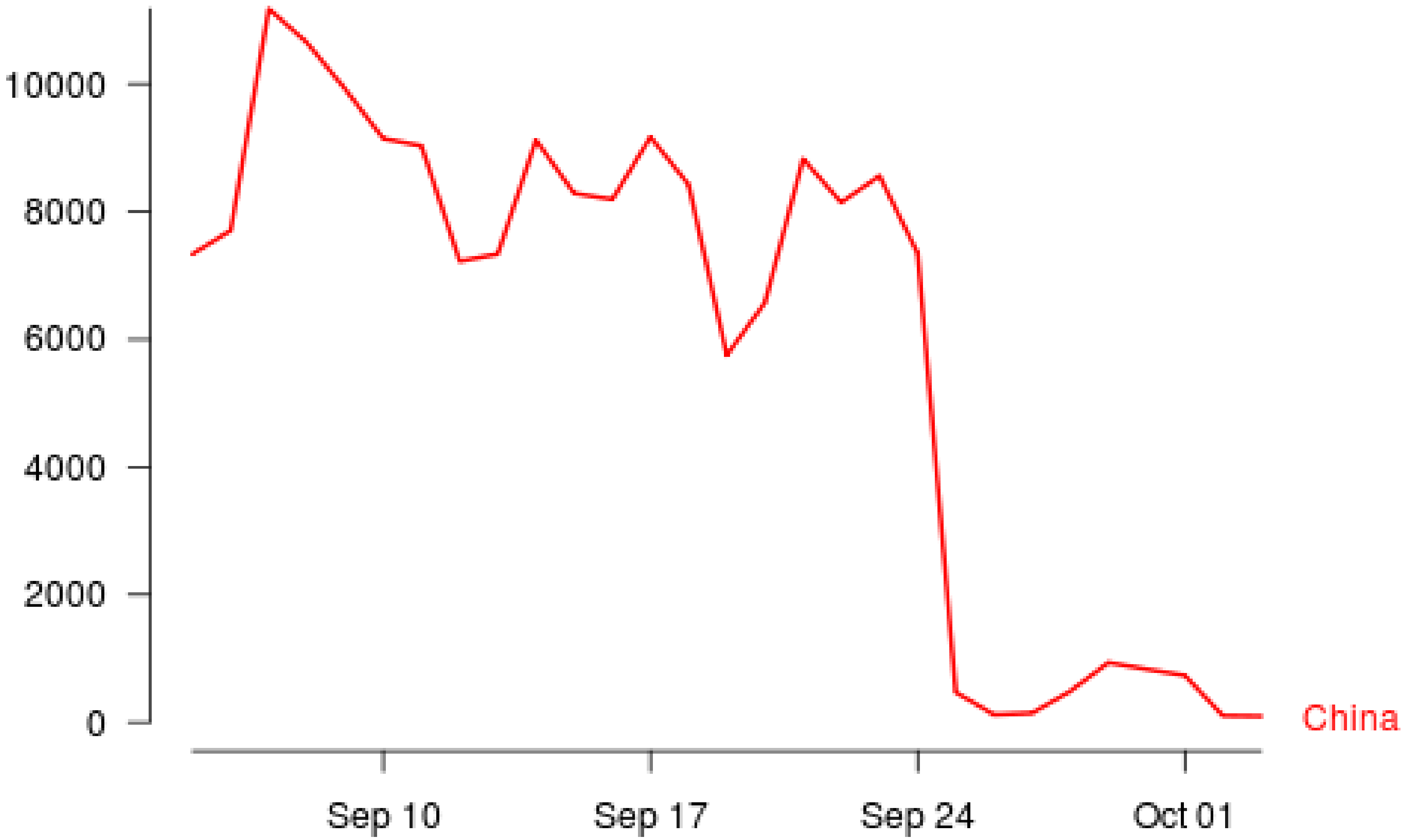
Bridges create connections between filtered clients and the blocked public Tor network. Bridges only have to be accessible – they don't have to be trusted. They can be public or private.

If you'd like a public bridge, simply email (gmail only) bridges@torproject.org and we'll send you one. If you can't find one that works, ask a friend to setup a private bridge that is much more difficult to block.


Bob
Bob
Bob
Bob
Bob
Blocked Alice
R3
R4
Blocked Alice
Bob The Bridge
Blocked Alice
Bob
R2
Blocked Alice
R1
Censored Bob
Blocked Alice

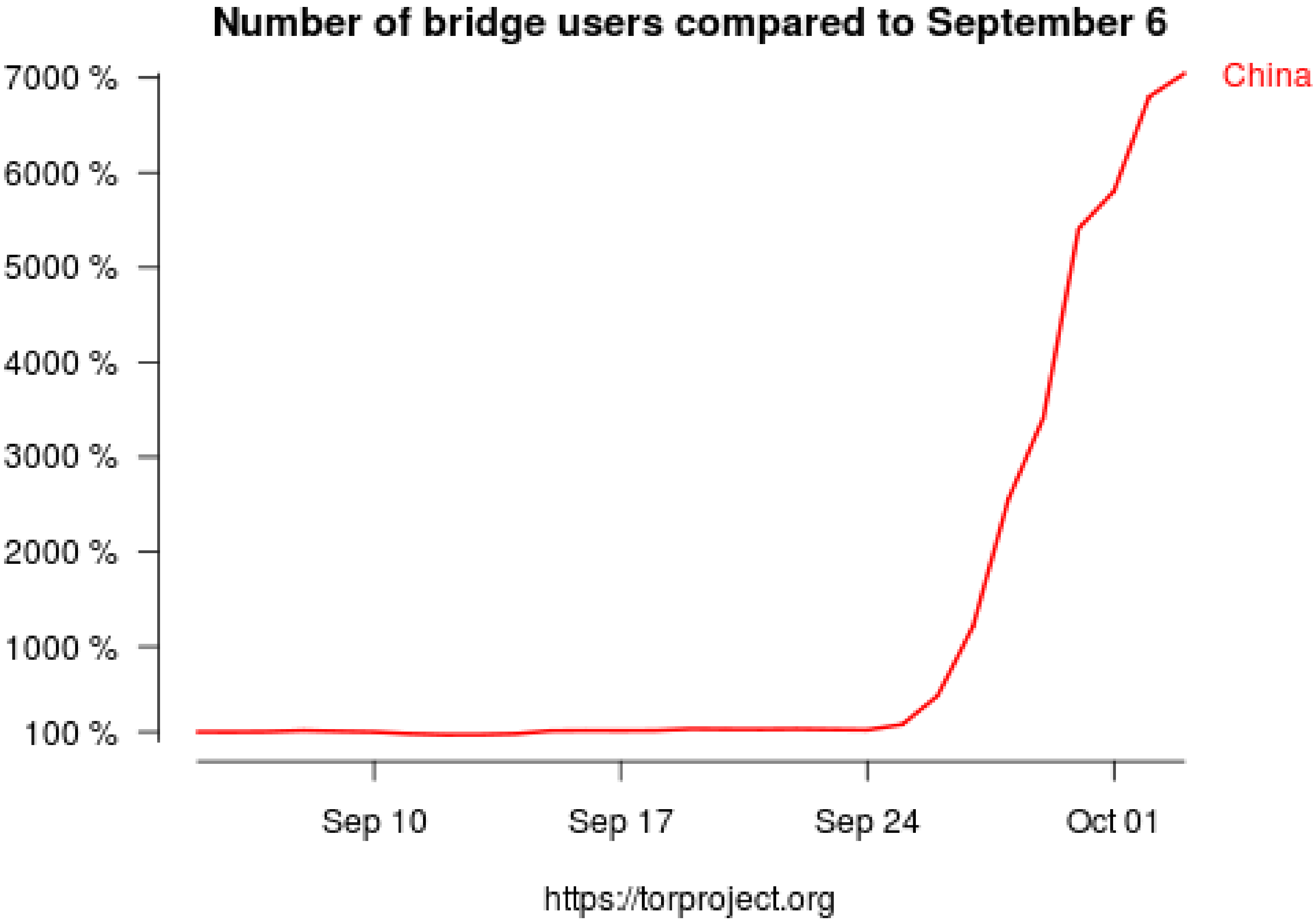
How's that working in practice?

Number of directory requests to directory mirror trusted



https://torproject.org

Reasonably well


Number of bridge users compared to September 6

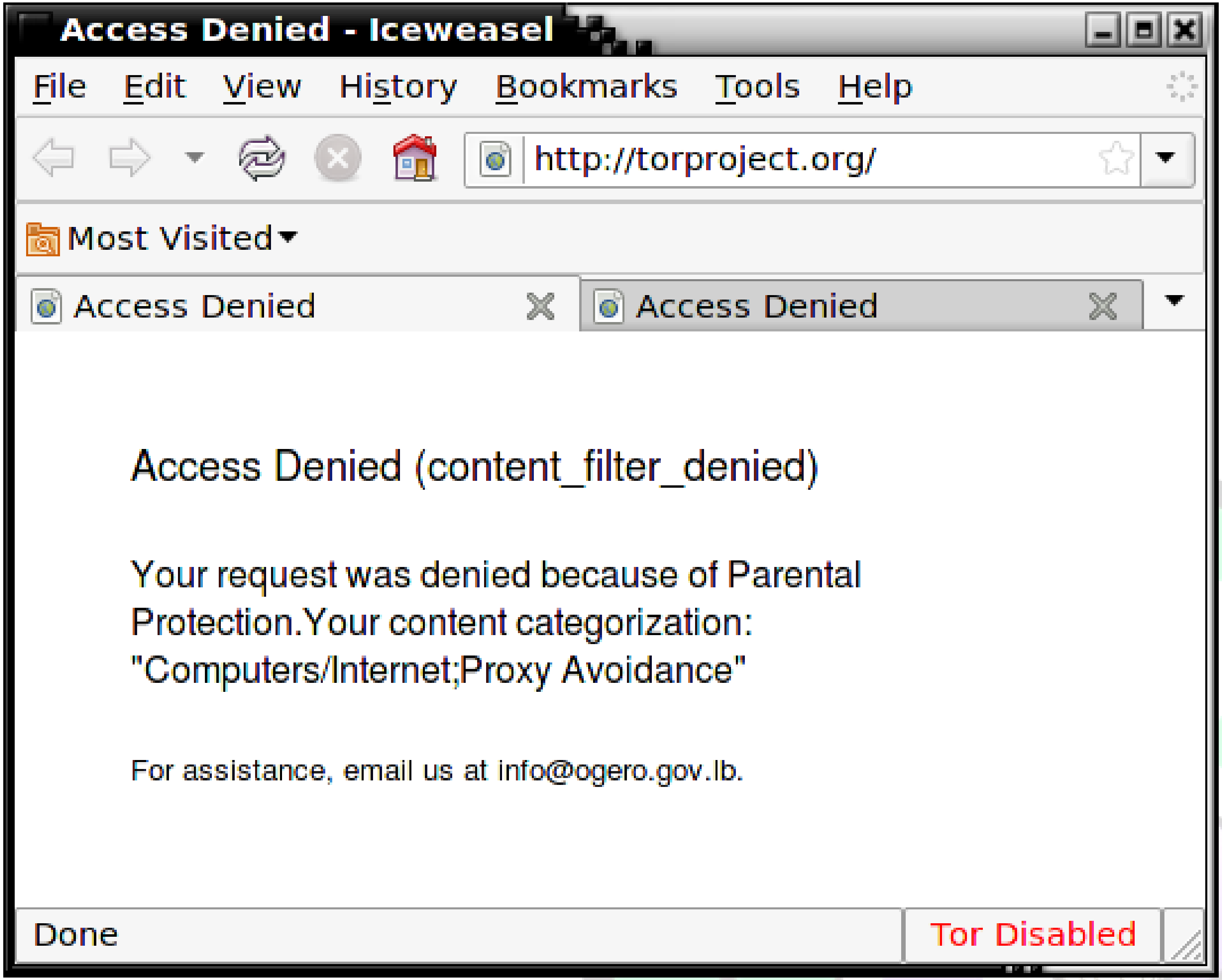
https://torproject.org

China today

We're seeing a blocking event on average of each quarter of a year. The censors appear to be actively harvesting bridges; any public Tor relay information available appears to go into the filter.

This is probably not such a wise tactic.

What about Lebanon?



Access Denied (content_filter_denied)

Your request was denied because of Parental Protection.Your content categorization: "Computers/Internet;Proxy Avoidance"

For assistance, email us at info@ogero.gov.lb.

OGERO

Ogero is one of the main ISPs in Lebanon. They have filtering that is dangerous for all of internet traffic flowing through their network.

They run heavily overloaded and un-patched Squid machines:
77.42.129.27 - Squid webproxy 2.5.STABLE11
77.42.129.2 - Squid webproxy 2.5.STABLE11

You must reposition from within their network to see these proxies. The proxies are partially hidden from the public internet.

OGERO

Finding the OGERO censorship while filtered is simple.

Inside Beirut we see that it is not afflicted with DNS filtering. These are the correct and expected answers:

```
% host torproject.org
torproject.org has address 86.59.21.36
torproject.org mail is handled by 10 moria.seul.org.
```

OGERO

Gee – only **four hops** to Austria?
Traffic is being routed through an obvious HTTP filter:

```
Tracing the path to torproject.org (86.59.21.36) on
TCP port 80 (www), 30 hops max

 3  77.42.129.27  2538.129 ms * *
 4  * byblos.torproject.org (86.59.21.36) [open]
1469.264 ms  -209.719 ms
```

OGERO

Tracing the path to torproject.org (86.59.21.36) on TCP port 443 (https), 30 hops max

```
 3  77.42.129.27  1313.302 ms  2329.022 ms  1692.057 ms
 4  77.42.129.2  2167.223 ms * *
 5  * * *
 6  * * *
 7  * ae-34-52.ebr2.London1.Level3.net (4.69.139.97)
1440.299 ms *
```

The proxy didn't tamper with the SSL traffic.

OGERO

The filters on the Ogero network are heavily overloaded, easily exploitable, and a danger to anyone using the internet in Lebanon.

The filters are often considered optional. When I inquired, many people were unaware they were being filtered; others were aware thinking it might be good to cut down on their bandwidth costs.

How about TerraNet?

TerraNet is the other major ISP in Lebanon. They pull similar tricks.

From a local cafe with an ip of 212.98.138.15, I found all of my connections to the general internet were shunted through a proxy located at 85.112.95.11 (85.112.95.0/24).

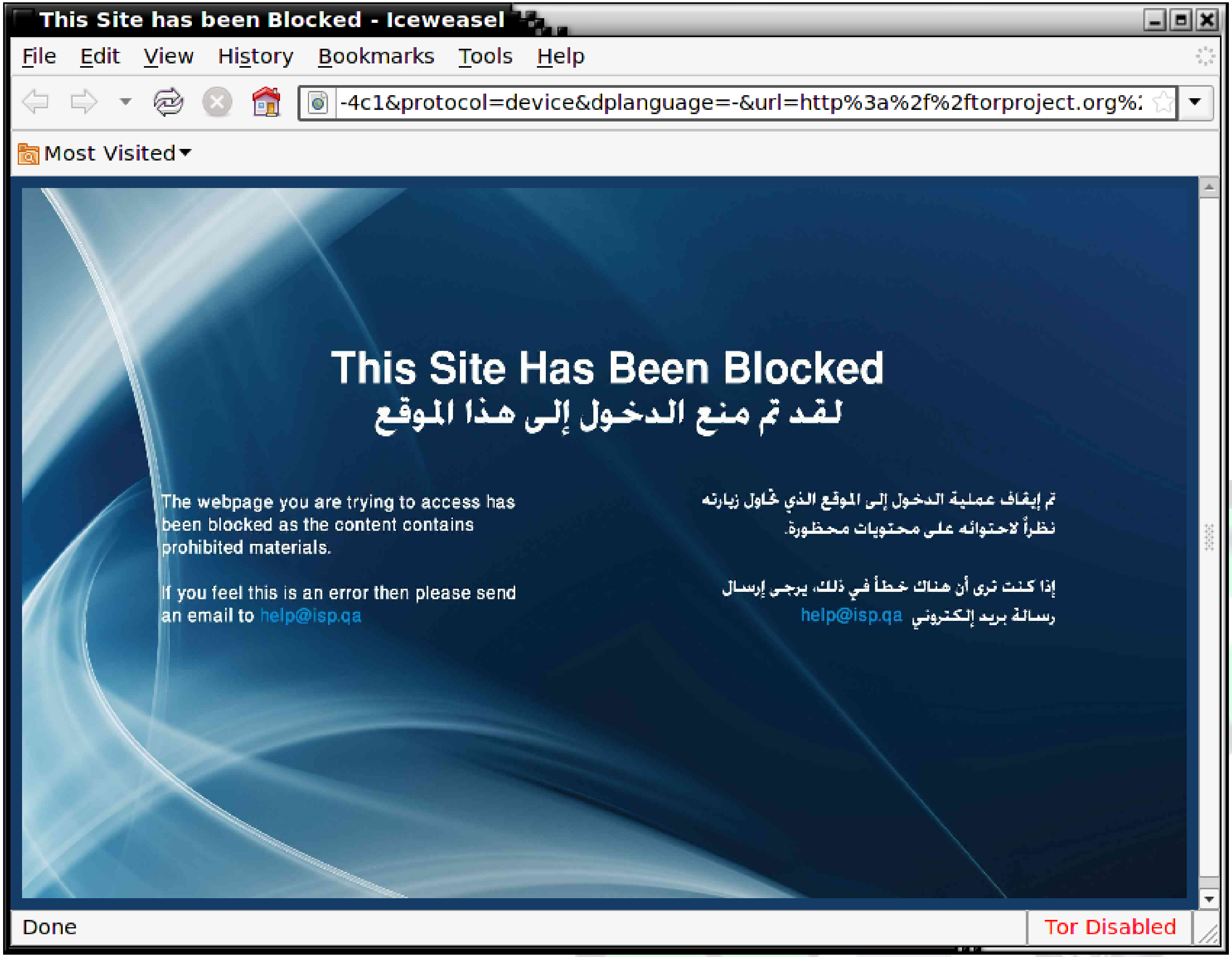
The ISP masked ICMP traceroute but failed to properly mask their TCP mangling.

How about TerraNet?

```
% tcptraceroute check.torproject.org 80
Tracing the path to check.torproject.org (209.237.247.84)
on TCP port 80 (www), 30 hops max
 1  192.168.17.1  1.657 ms  1.555 ms  1.361 ms
 2  check.torproject.org (209.237.247.84) [open]  167.961
ms  119.644 ms  100.813 ms
```

Only **two** hops? My, that's a close cross connect.

Qatar?



-4c1&protocol=device&dplanguage=-&url=http%3a%2f%2ftorproject.org%2

This Site Has Been Blocked
لقد تم منع الدخول إلى هذا الموقع

The webpage you are trying to access has been blocked as the content contains prohibited materials.

If you feel this is an error then please send an email to help@isp.qa

تم إيقاف عملية الدخول إلى الموقع الذي تحاول زيارته
نظراً لاحتوائه على محتويات محظورة.

إذا كنت ترى أن هناك خطأ في ذلك، يرجى إرسال
رسالة بريد إلكتروني help@isp.qa

Qatar?

Qatar's networks are filtered by their local national monopoly telecommunications company Qtel. My hotel's network was no exception.

It appears that they're using the Canadian NetSweeper filter software. Perhaps someone should ring Ottawa to complain?

Take a look at this url:

http://proxy1.isp.qa:8080/webadmin/deny/index.html?
dpid=1&dpruleid=7&cat=105&ttl=0&groupname=filter&policyname=filt
er&username=filter_89_211_128_0_19_&userip=89.211.134.135&conne
ctionip=89.211.134.135&nsphostname=CPU-4c1&protocol=device&dpla
nguage=-&url=http%3a%2f%2ftorproject.org%2f

Qatar!

Qtel needs to patch their networks:

```
proxy1.isp.qa has address 82.148.98.52
censor.qa has address 82.148.100.101
```

Contact NetSweeper!

Don't like that they're selling filter software to block and censor an entire nation?

Contact their executive team:

Perry J. Roach, Chief Executive Officer
Andrew Graydon, Chief Operating Officer
Lou Erdelyi, Chief Technology Officer

http://www.netsweeper.com/

Iran

In my personal time, I've been scanning Iran at various key points in recent history.

They had one of my machines pulled offline from a data center. I put up new machines in better connected data centers.

Iran

Tor use in Iran varies with their general social stability. The government has a “knob” that is used to traffic shape the internet at times of key events.

We try to encourage people to use Tor over other software; there's a great deal of snakeoil proxy software and it appears that the threat for people using proxies is extremely high. Many people have been extremely irresponsible in their efforts to help; those people often mean well but their lack of knowledge about cryptography, security, privacy, data retention, will cost Iranians dearly.
We advise caution.

Iran

Iran

Nokia has reportedly sold equipment to the Iranian government. It helps wiretap, track, and crush dissenting members of Iranian society. Nokia claims that this is *ethical* because they were forced to put legal intercepts into their products by the **West**.

Sounds like **they are in the wrong business**. Sounds like **we're part** of the problem.
Nokia is not alone, we're forcing companies to build interception interfaces.

Take a peek at the Iran Telecommunication Research Center:
80.191.2.0/24

What about Neda?

Curious about the Basij that shot her in the heart?

Ask them about it:
webmail.basij.ir

Wondering about the spooks that protect the Basij?
Welcome to the world of itrc.ac.ir:
laleh.itrc.ac.ir (80.191.2.2), laleh2.itrc.ac.ir (80.191.2.4), amn (80.191.2.15), epol (80.191.2.27), mediaproxy.itrc.ac.ir (80.191.2.101), sipproxy.itrc.ac.ir (80.191.2.103), apa.itrc.ac.ir (80.191.2.150), smsmonitoring.itrc.ac.ir (80.191.2.203), vlib.itrc.ac.ir (80.191.2.207), azmoon.itrc.ac.ir (80.191.2.240)

Iran

Lo-Tech Subversion without Tor?

Sure. Try splitting your requests into strings the censorship equipment isn't expecting.

“GET” is Censored. “G E T” is not censored.

This work(ed,s) in Iran for non-blocked URLs. The Green Anti-Sec group released a local request name splitting proxy for users to bypass some proxies with this bug. This also appears to work in Qatar.

This is unsafe to use but it's too funny to neglect mentioning.

Is this censorship effective?

Technically, almost all of this censorship is simple to bypass.

Socially, it's increasingly common to see regular people subverting filters to find simple information.

Burma

Burma is an example of a country where public pressure has changed the players, but it has not ultimately changed the game.

FortiNet was accused of selling FortiGuard censorship gear to the Burmese Military Junta.

Burma

Fortinet indroduces its products to Burma in May 2004, as Fortinet's Benjamin Teh meets Gen Khin Nyunt (top left)

Burma

It has been reported that FortiGuard may be gone from Burma. Things haven't changed much. New scans of Burma reveal lots of Cisco gear. Burma has two major subnets. They're filled with Cisco routers:

```
% grep -i cisco *.gnmap|wc -l
20
```

They only allow connections ***in*** to around ***200*** machines from the internet. They reportedly MITM all outgoing SSL connections with **BlueCoat** devices these days.

Allow me to clarify

Tor isn't the solution to everything.
The tactics of censorship, blocking, and oppression change over time.

We can **resist** and **improve** the world together.
Pressure your vendors to behave ethically; Call them and ask why **they're helping** to enable human rights abuses with their technology.

A flash mob full of people with cell phones today will probably result in beating, torture, and unending harassment tomorrow.

Be smart, organize safely.

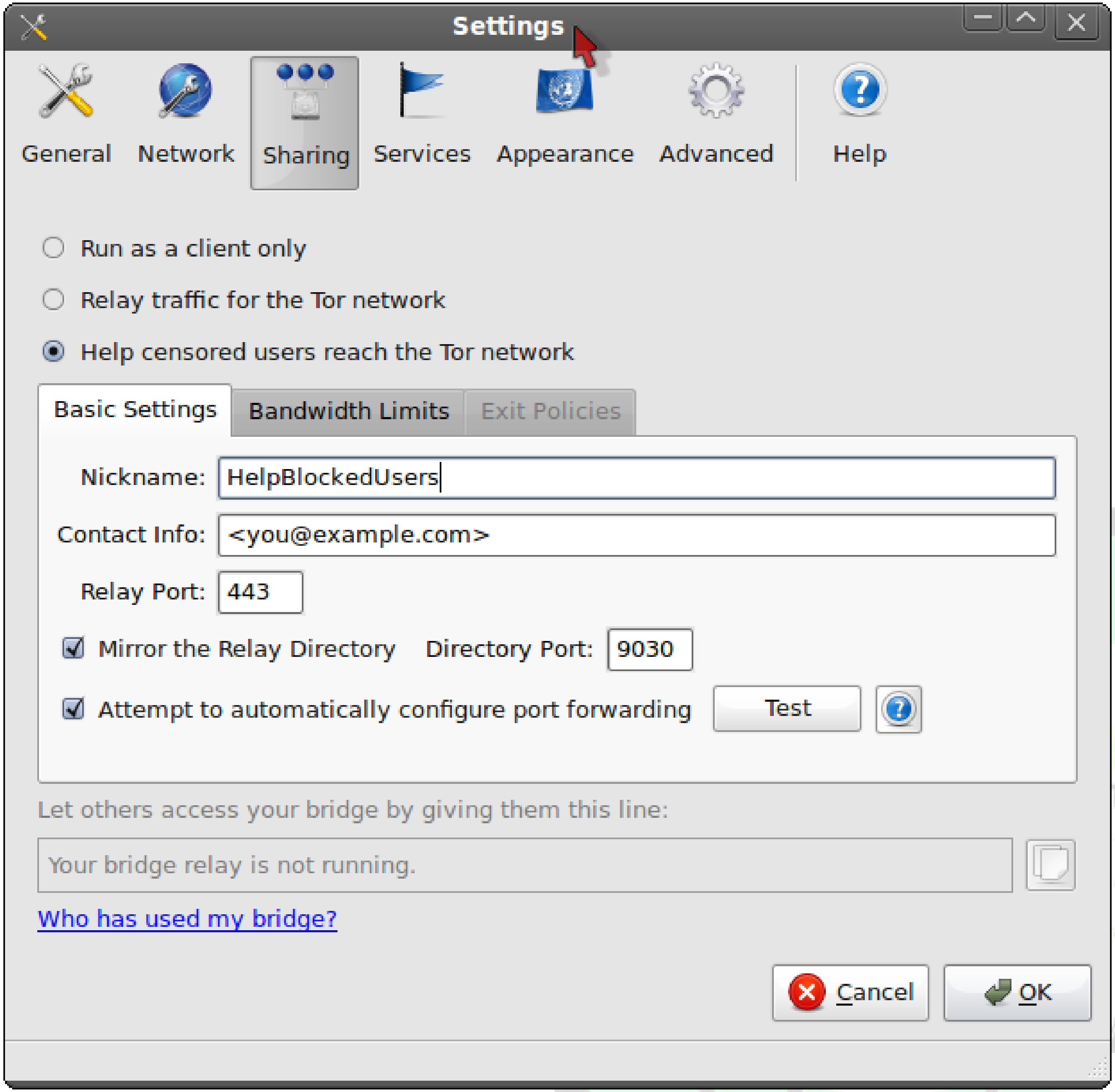
Outrage fatigue? No thanks.

If you'd like to directly help fight censorship, attacks on freedom of expression, attacks on historical events – you don't have to wait:

Run a Tor bridge.

You will directly help a person **who would otherwise be censored**. You do not have to remain silent about your discontent. **You are empowered** to enable others.

Here's how you help



○ Run as a client only

○ Relay traffic for the Tor network

● Help censored users reach the Tor network

Nickname: HelpBlockedUsers

Contact Info: <you@example.com>

Relay Port: 443

☑ Mirror the Relay Directory   Directory Port: 9030

☑ Attempt to automatically configure port forwarding

Let others access your bridge by giving them this line:

Your bridge relay is not running.

Who has used my bridge?

How can we change the game?

We must change society to change the larger picture. Sunlight is the best disinfectant; what have **you** leaked today?

You're the game changer – you can end a war before it starts.

Two great technologies that go great with a desire to change the world:

Tor and Wikileaks!

https://www.torproject.org/
https://secure.wikileaks.org/