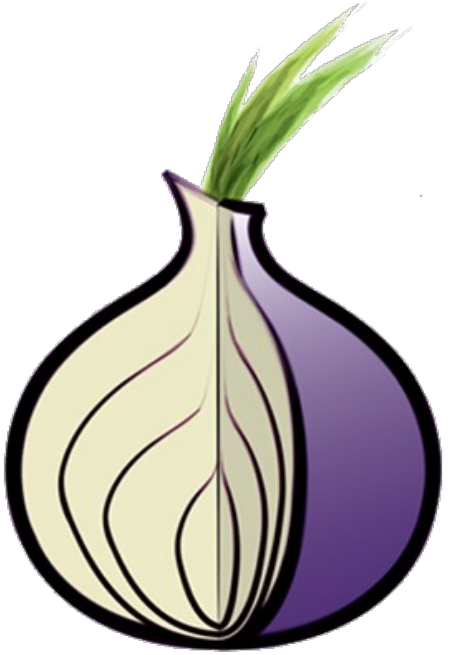
The Tor Project



Anonymity Online

Erinn Clark
erinn@torproject.org
TU-Berlin Techtalks
January 2011

In the future everyone will be anonymous for 15 minutes
– Banksy

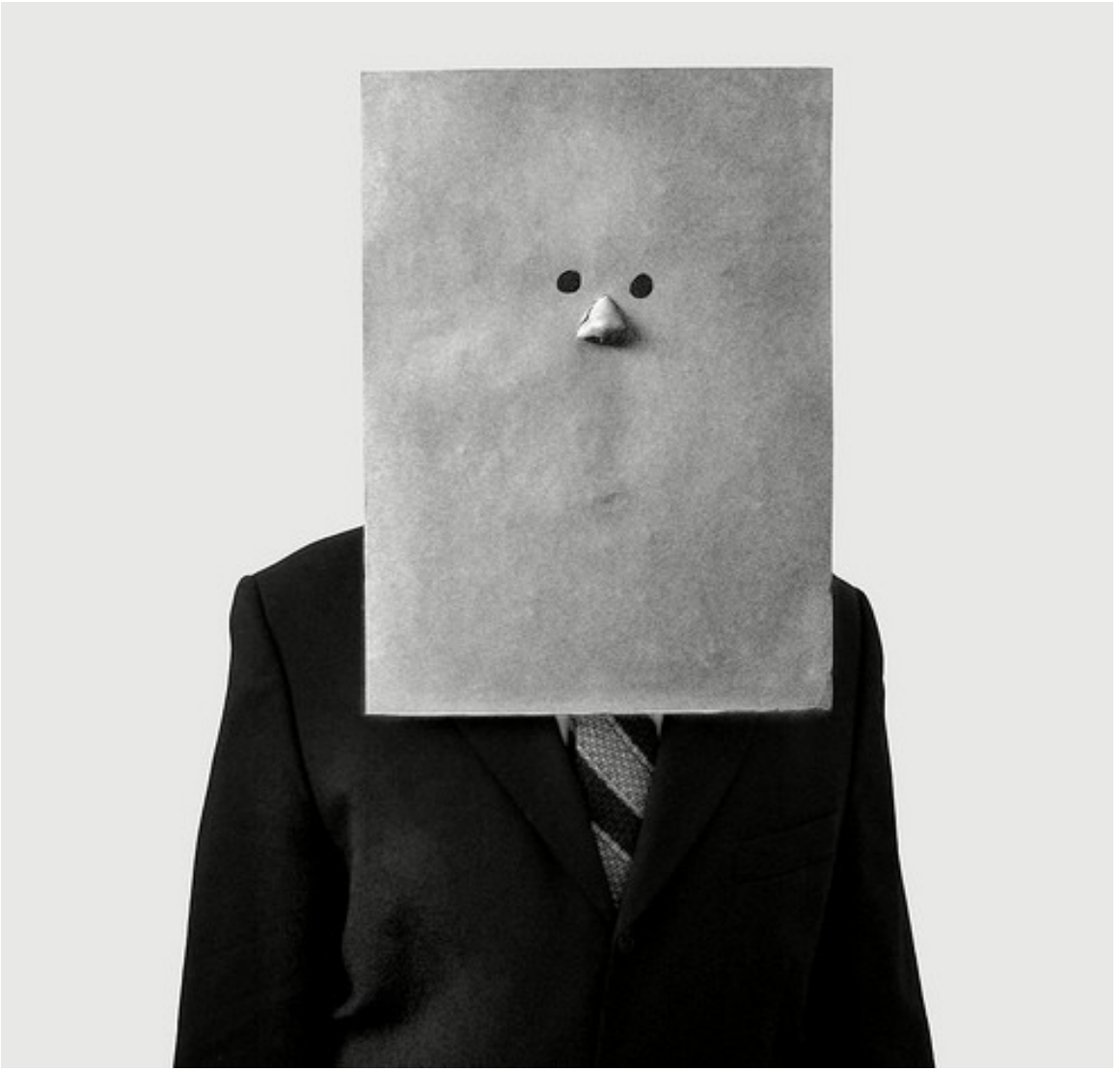
What is Tor?

- Online anonymity: software, network, protocol
- Free software
- Community of researchers, developers, and relay operators
- Funding from US DoD, EFF, Voice of America, Google, NLNet, Human Rights Watch, ...

The Tor Project, Inc.

- 501(c)(3) non-profit dedicated to the research and development of tools for online anonymity and privacy
- Thousands of volunteers running relays
- Dozens of volunteer developers
- Between 7-15 paid developers at any given time

What is anonymity?

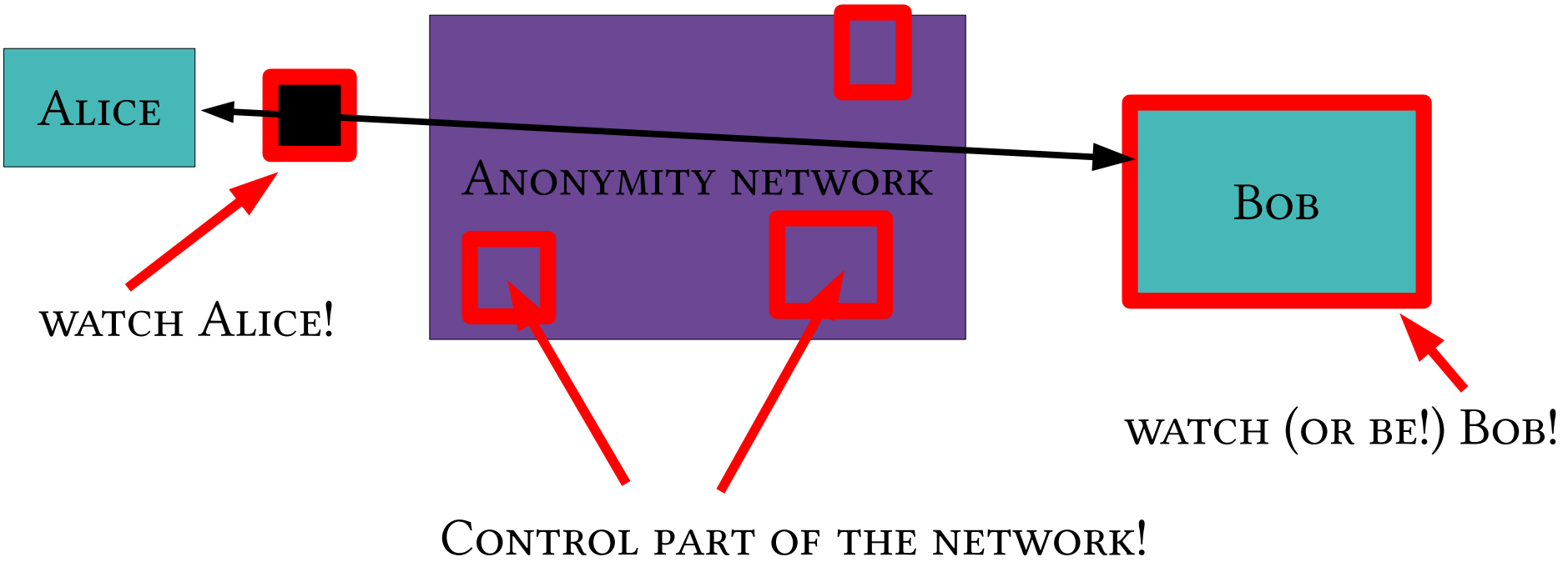


All personal life rested on secrecy, and possibly it was partly on that account that civilized man was so nervously anxious that personal privacy should be respected.

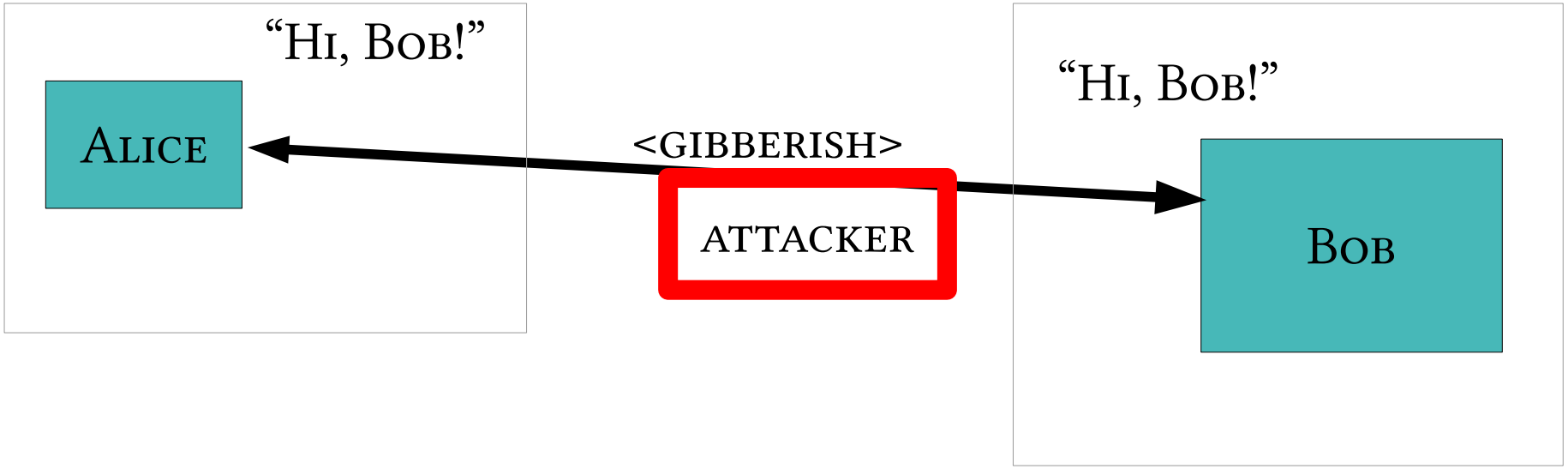
- Anton Chekhov

The Lady with the Little dog

Threat model: what can the attacker do?



Anonymity isn't cryptography: Cryptography just protects contents



Anonymity isn't just wishful thinking...

"You can't prove it was me!"

"Promise you won't look!"

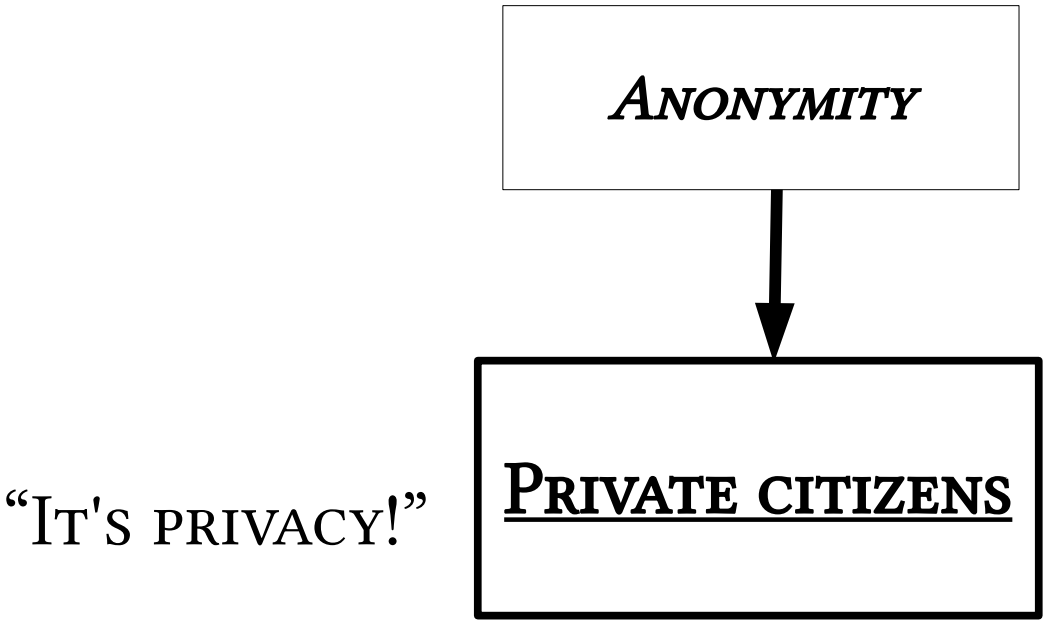
"Promise you won't remember!"

"Promise you won't tell!"

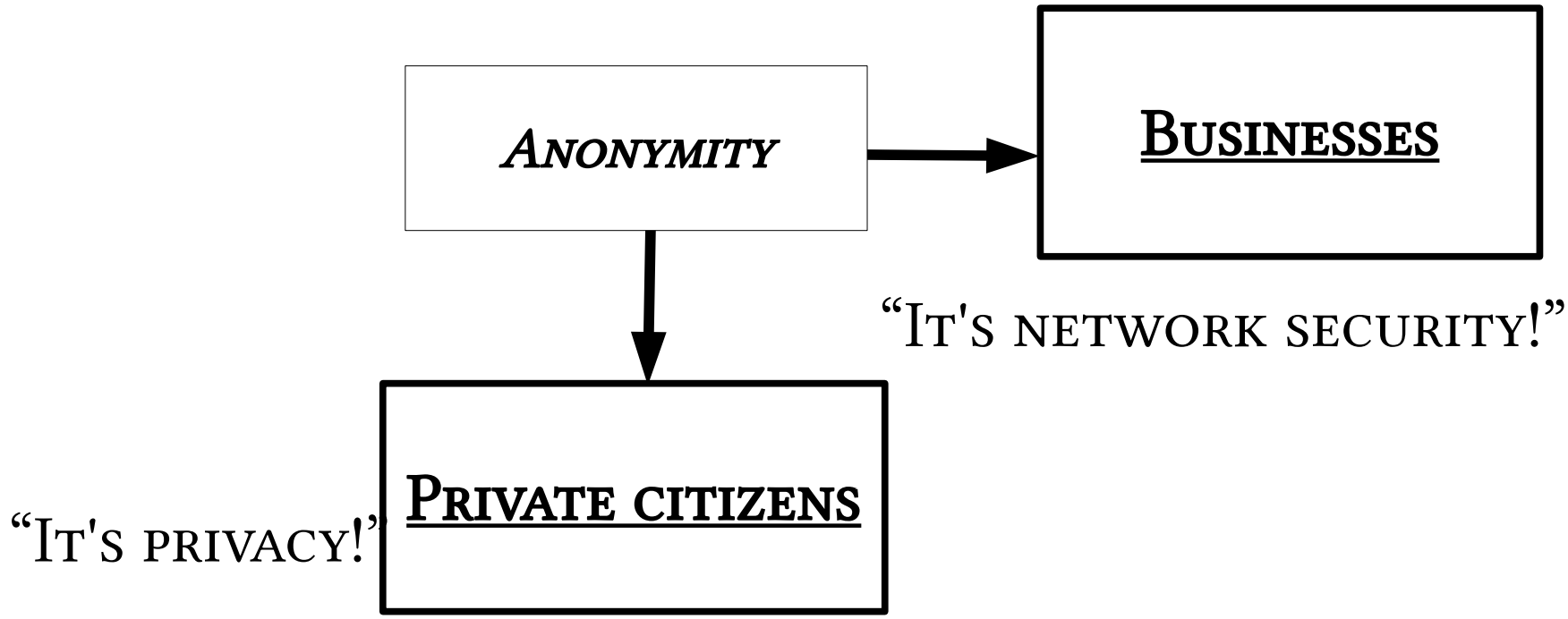
"I didn't write my name on it!"

"Isn't the Internet already anonymous?"

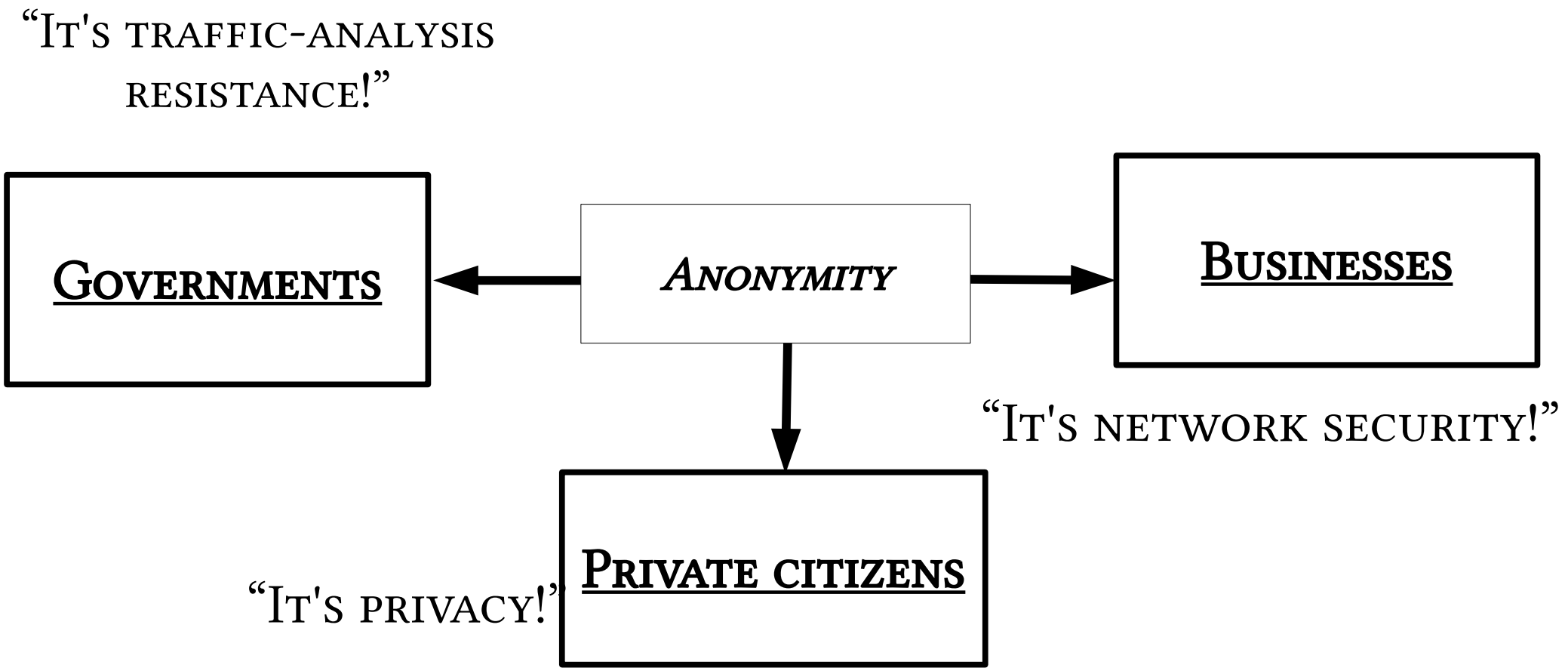
Anonymity serves different interests for different user groups



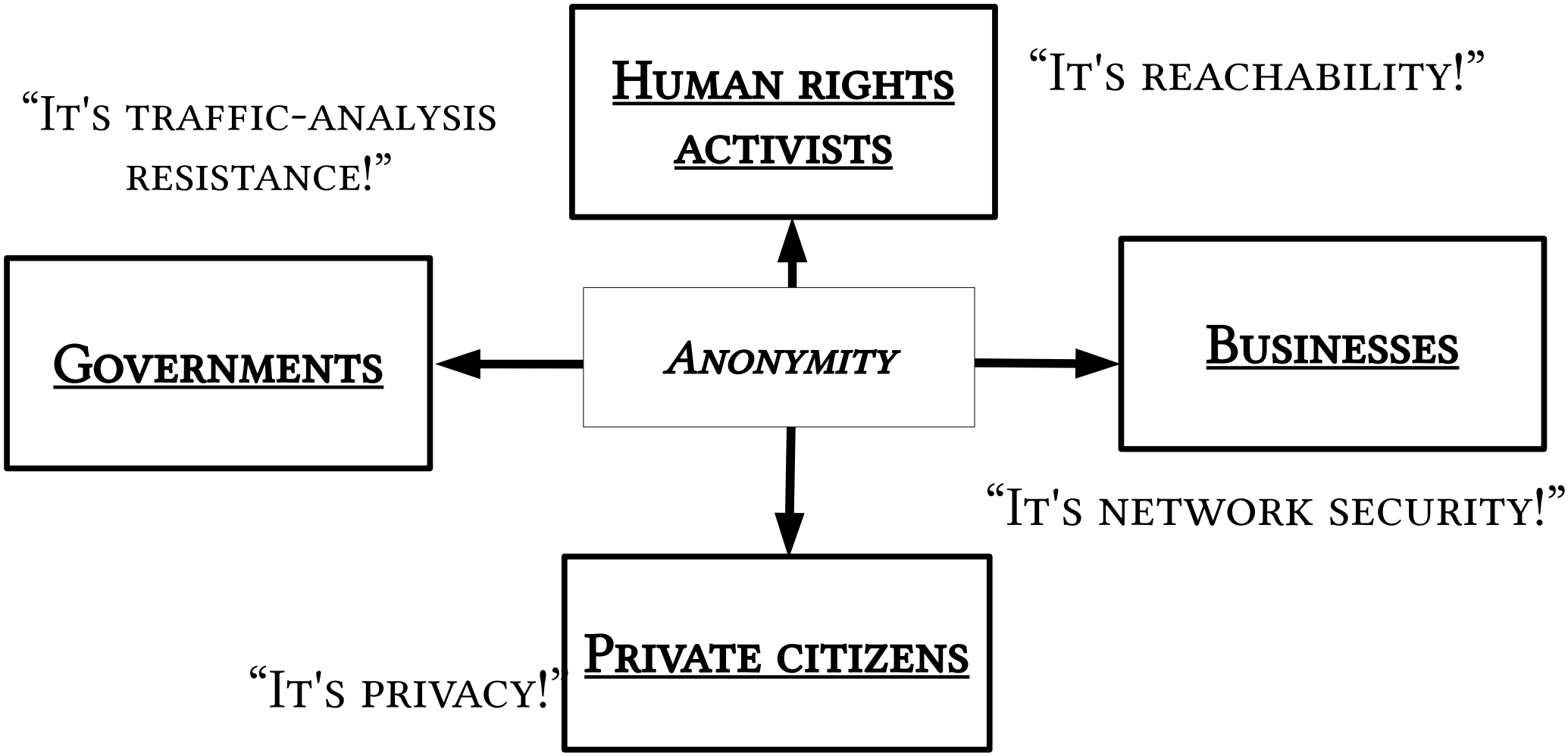
Anonymity serves different interests for different user groups



Anonymity serves different interests for different user groups



Anonymity serves different interests for different user groups



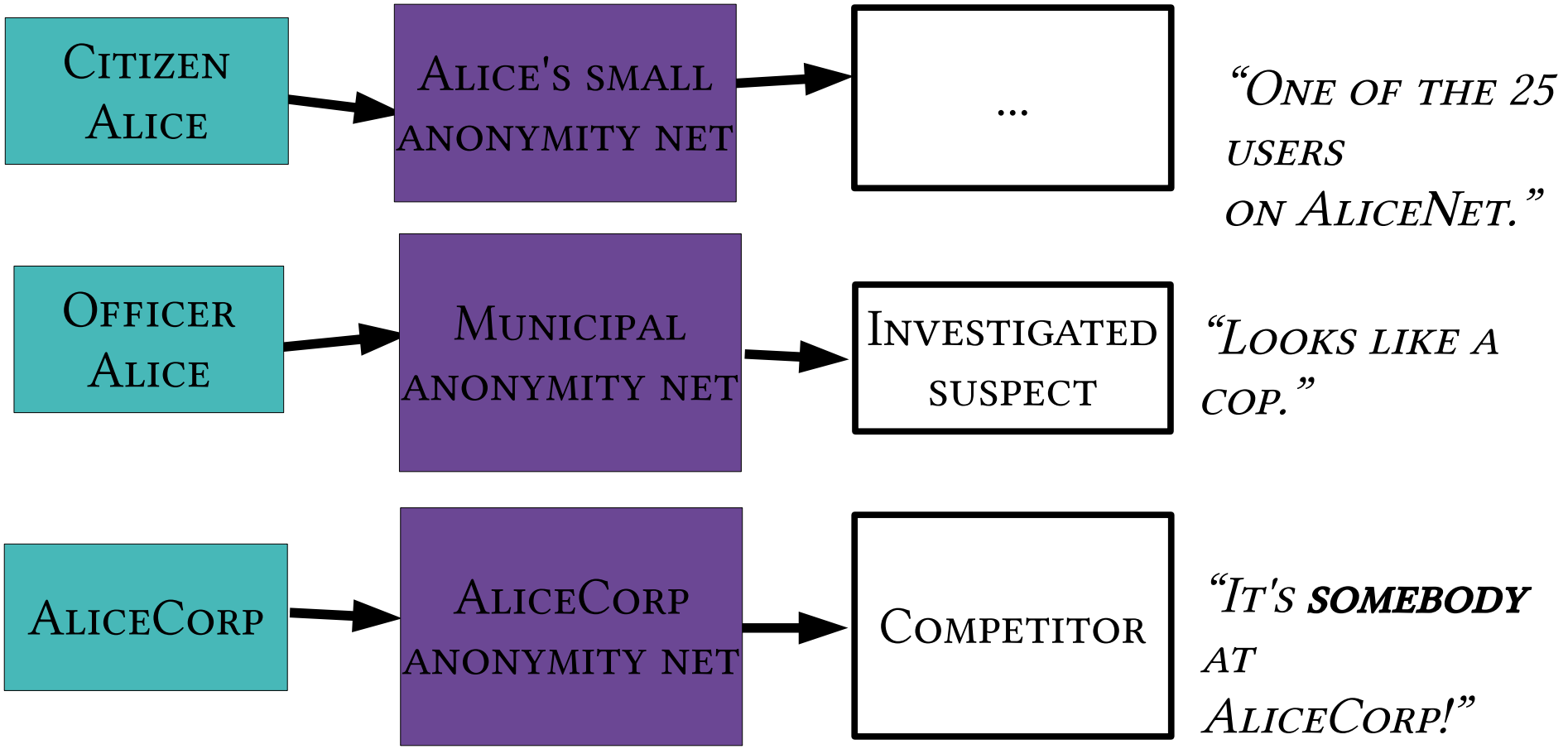
Who uses Tor?

Estimated 500,000

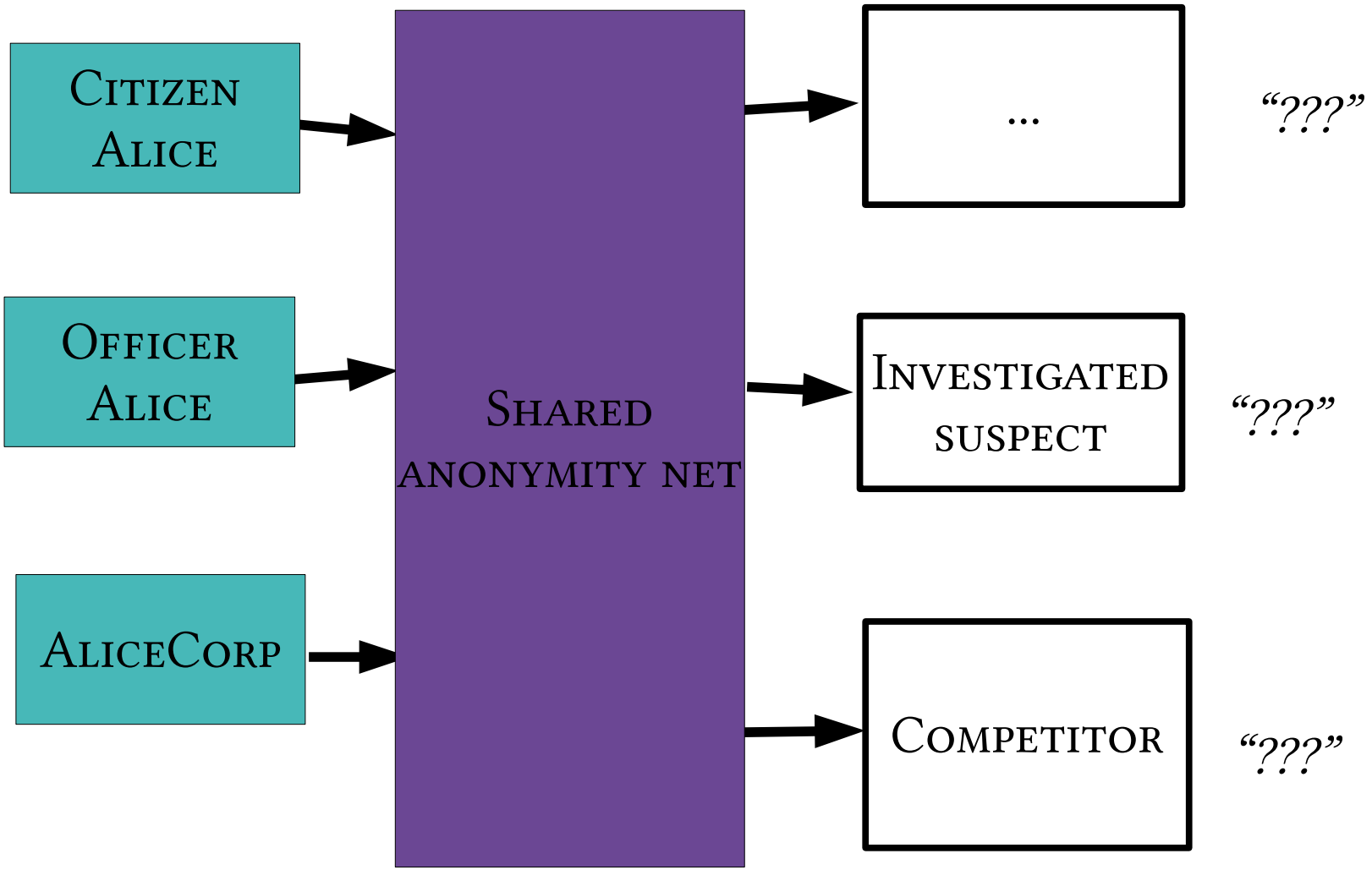
users daily


Average citizens
Businesses
Law enforcement
Governments
Journalists
Whistleblowers

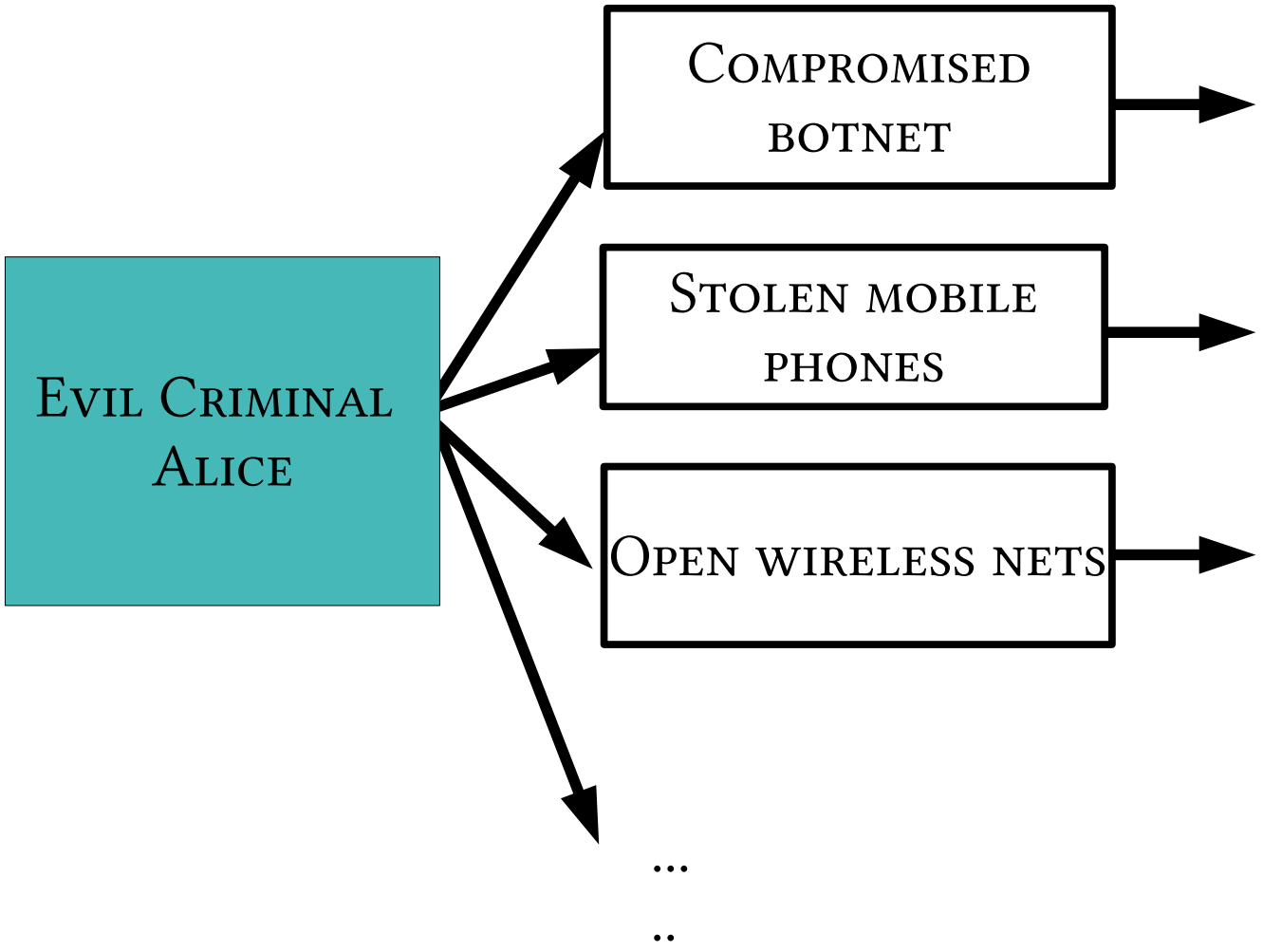
You can't get anonymity on your own: private solutions are ineffective...



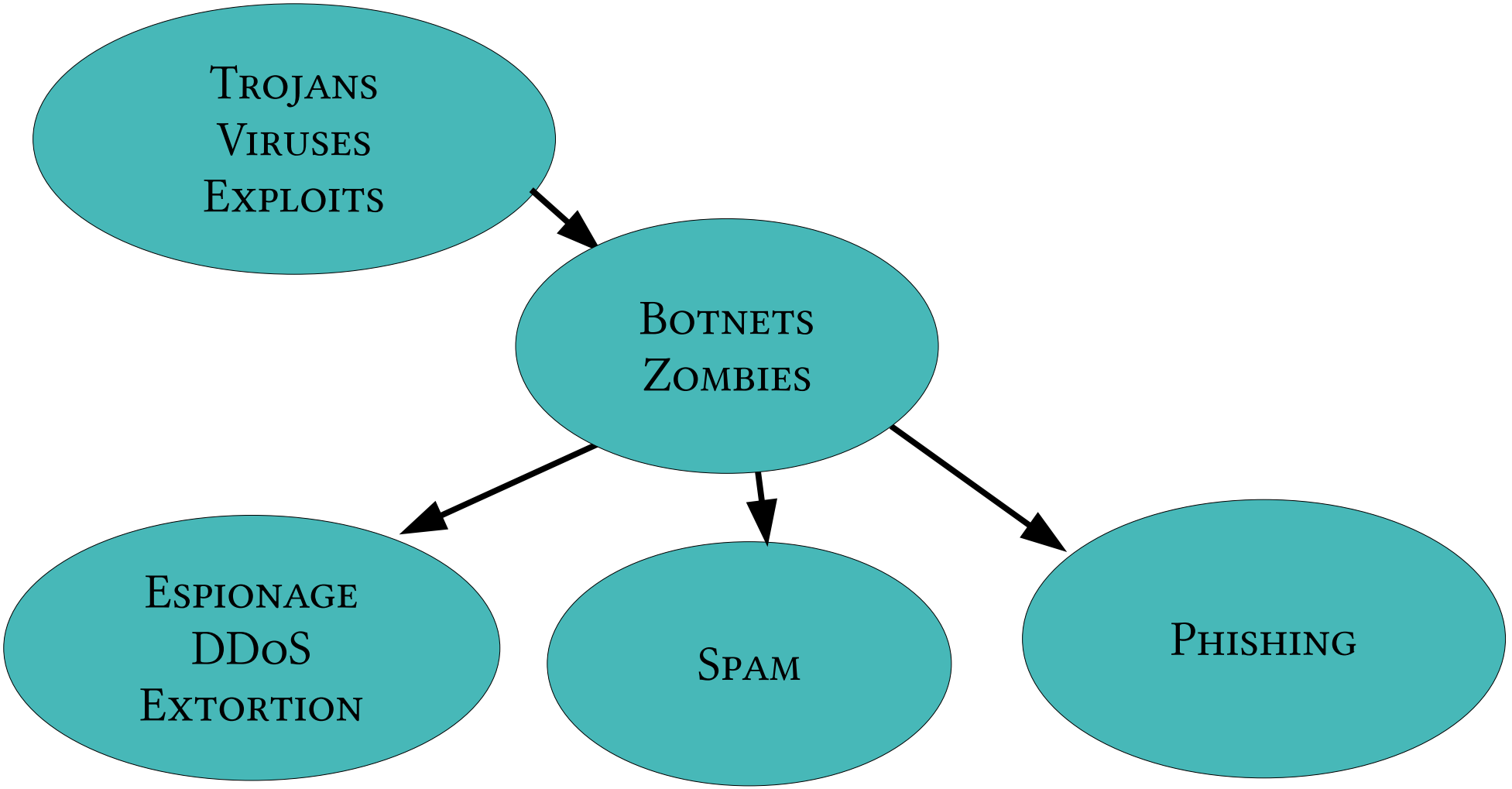
... SO, ANONYMITY LOVES COMPANY!



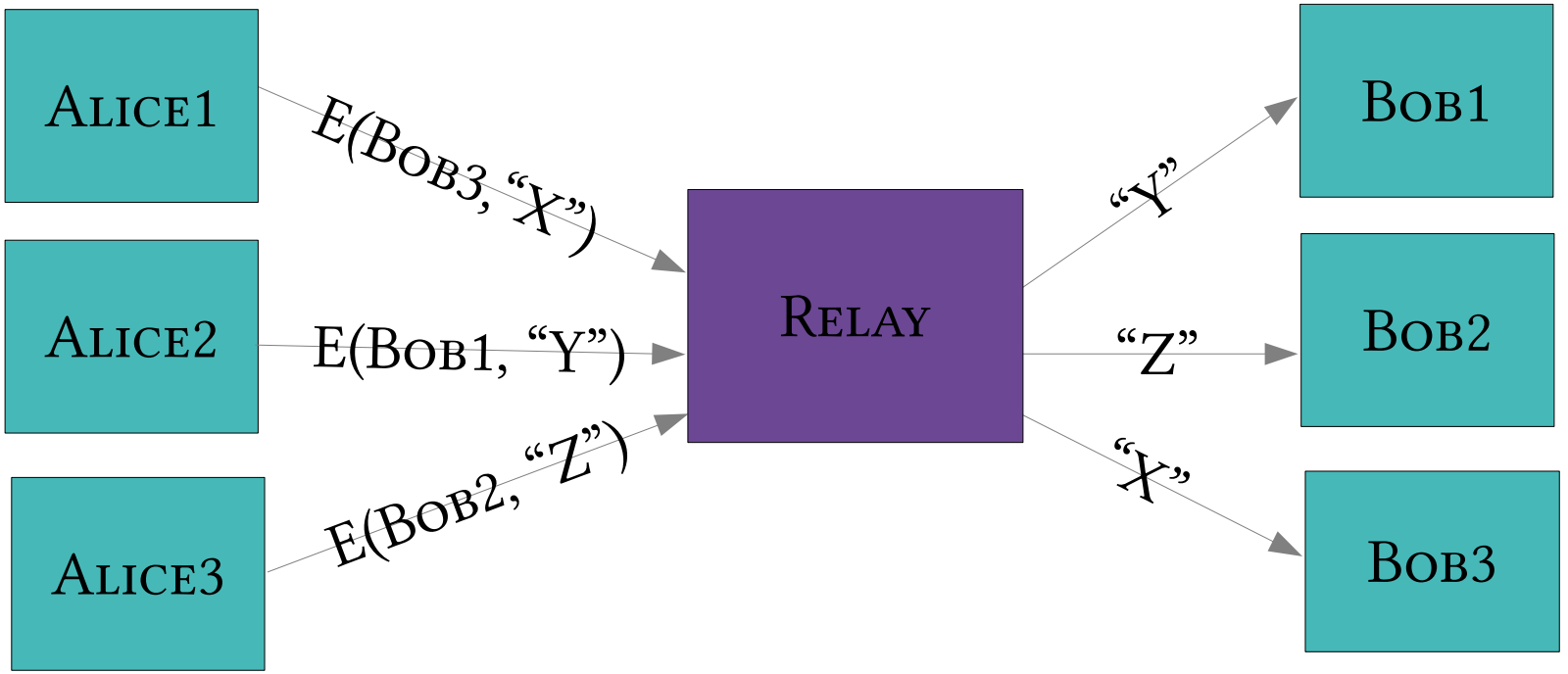
Yes, bad people need anonymity too. But they are *already* doing well.



Current situation: Bad people on the Internet are doing fine

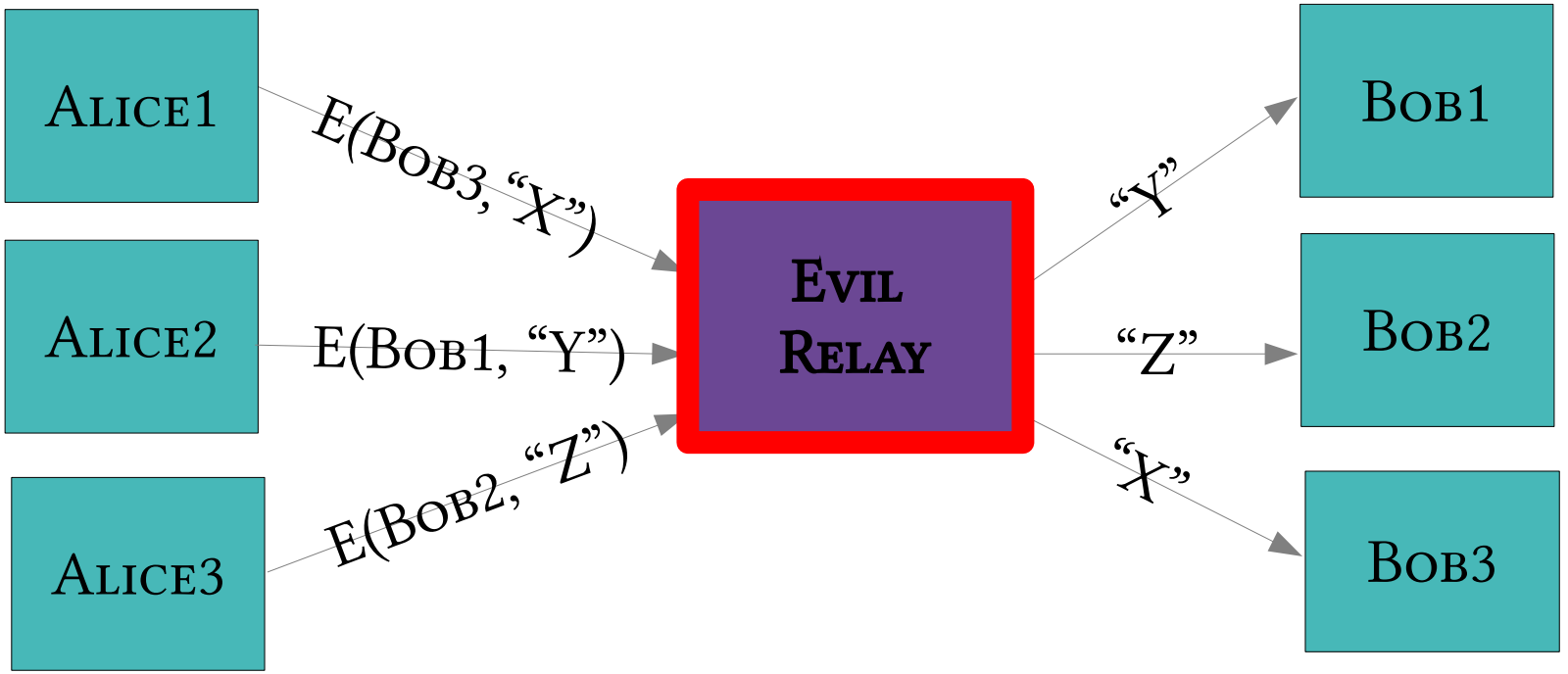


The simplest designs use a single relay to hide connections

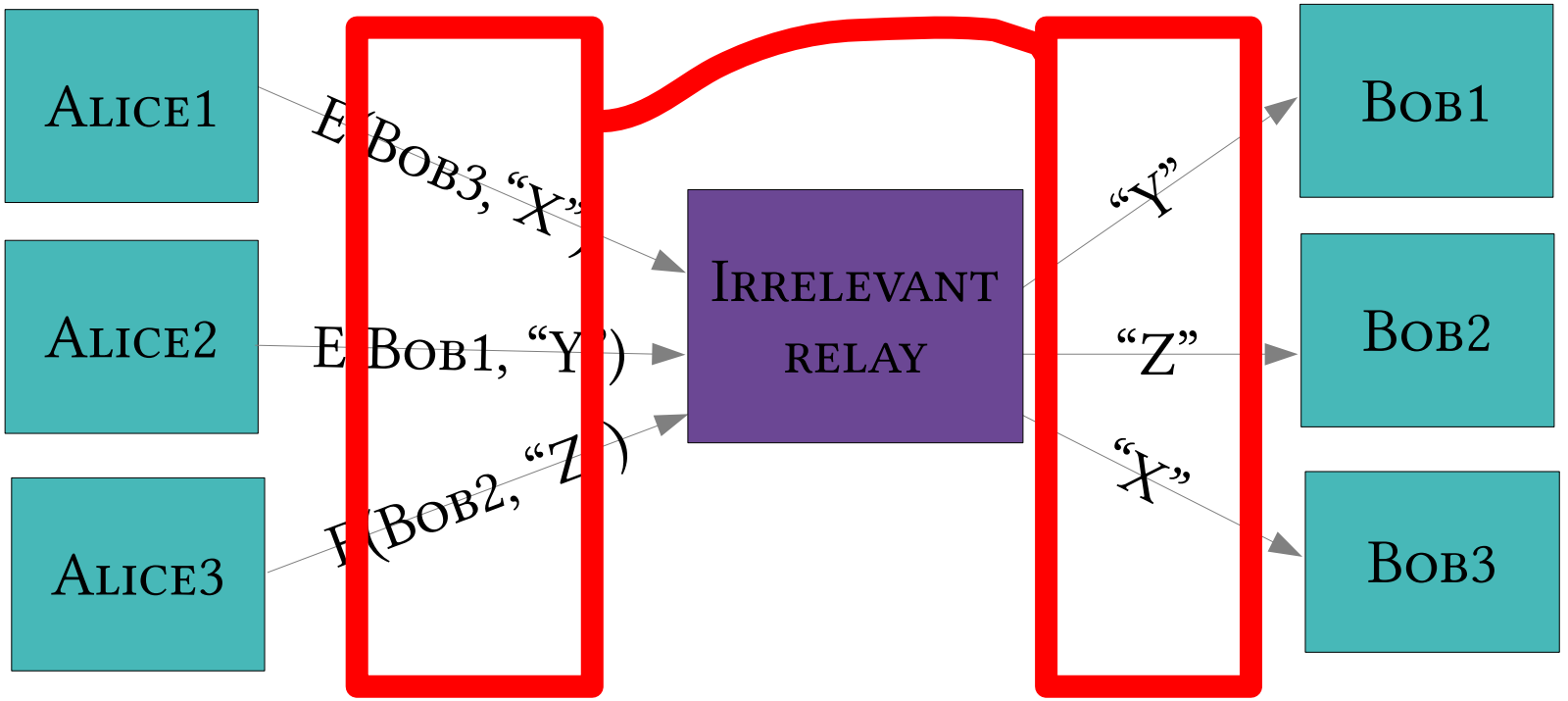


(example: some commercial proxy providers)

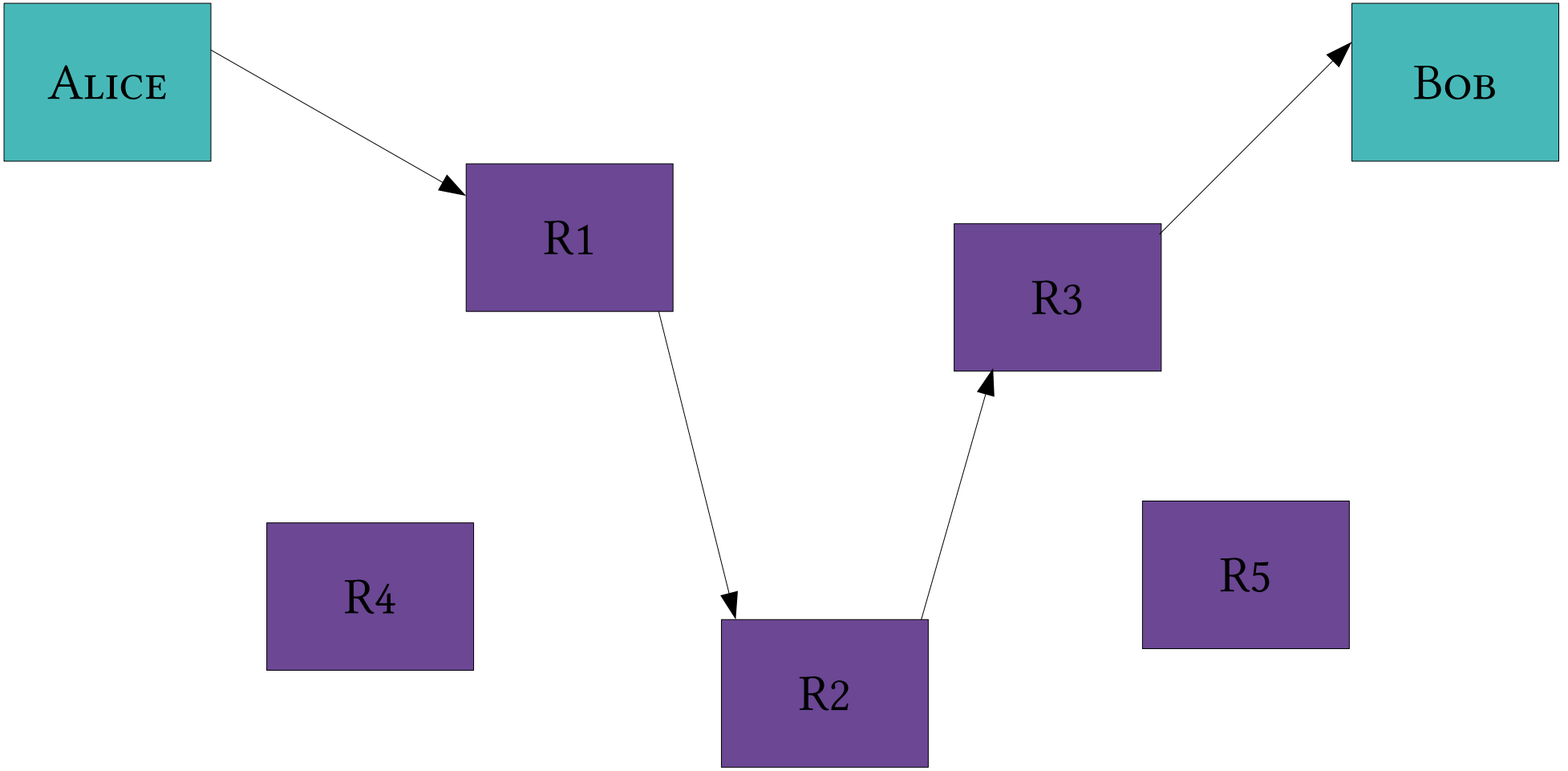
But a single relay (or eavesdropper!) is a single point of failure



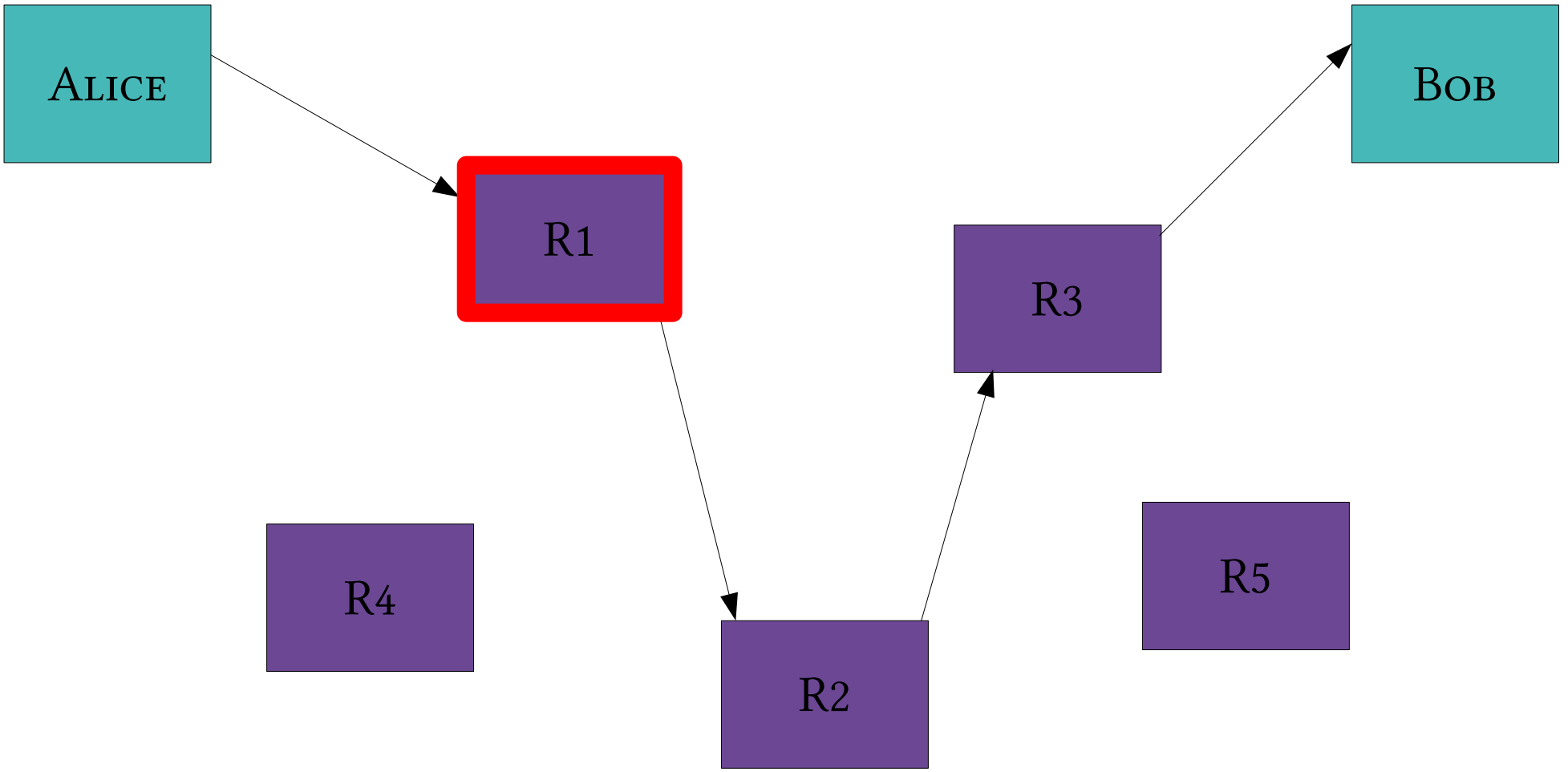
… OR A SINGLE POINT OF BYPASS



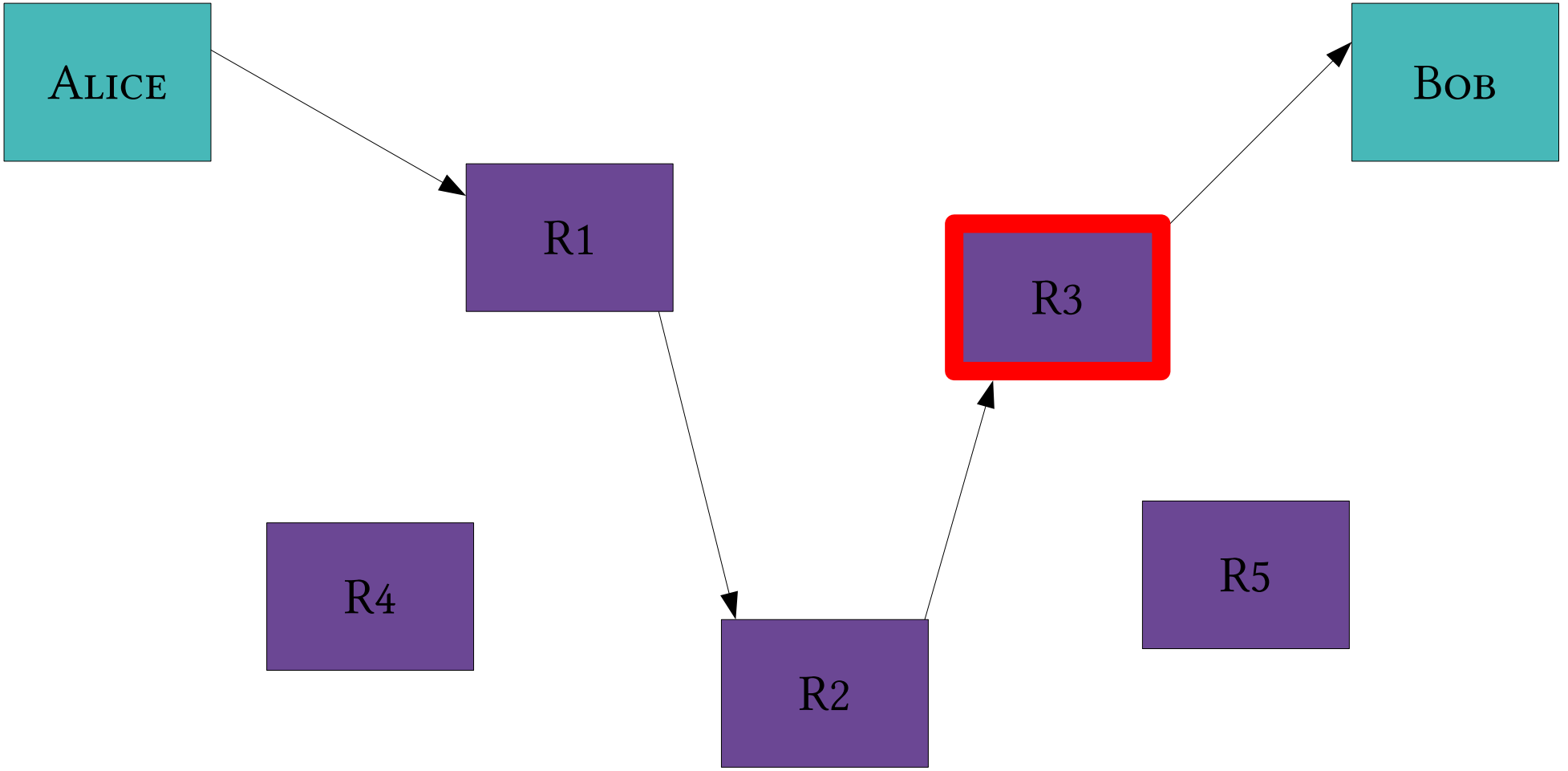
So, add multiple relays so that no single one can betray Alice



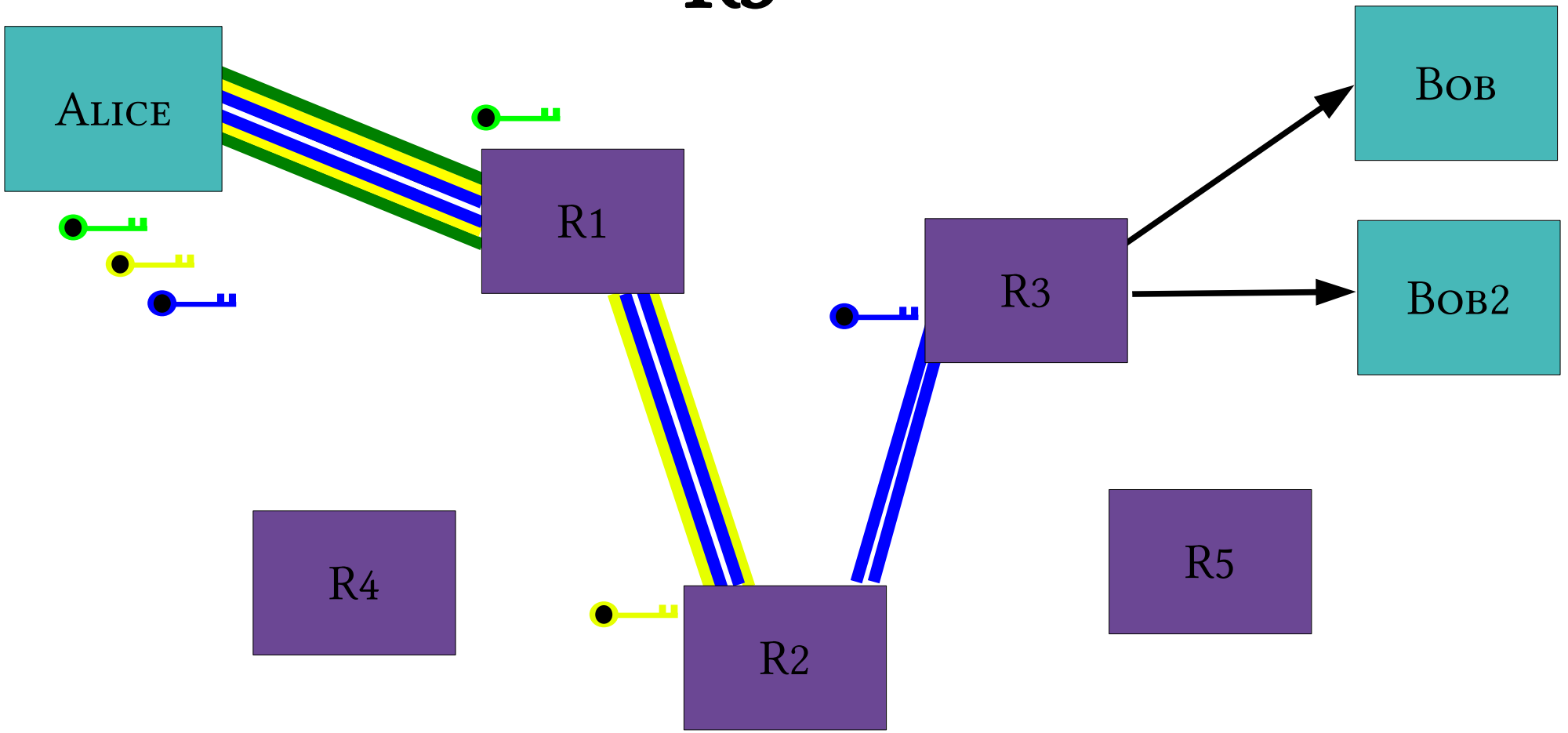
A corrupt first hop can tell that Alice is talking, but not to whom



A corrupt final hop can tell that somebody is talking to Bob, but not who



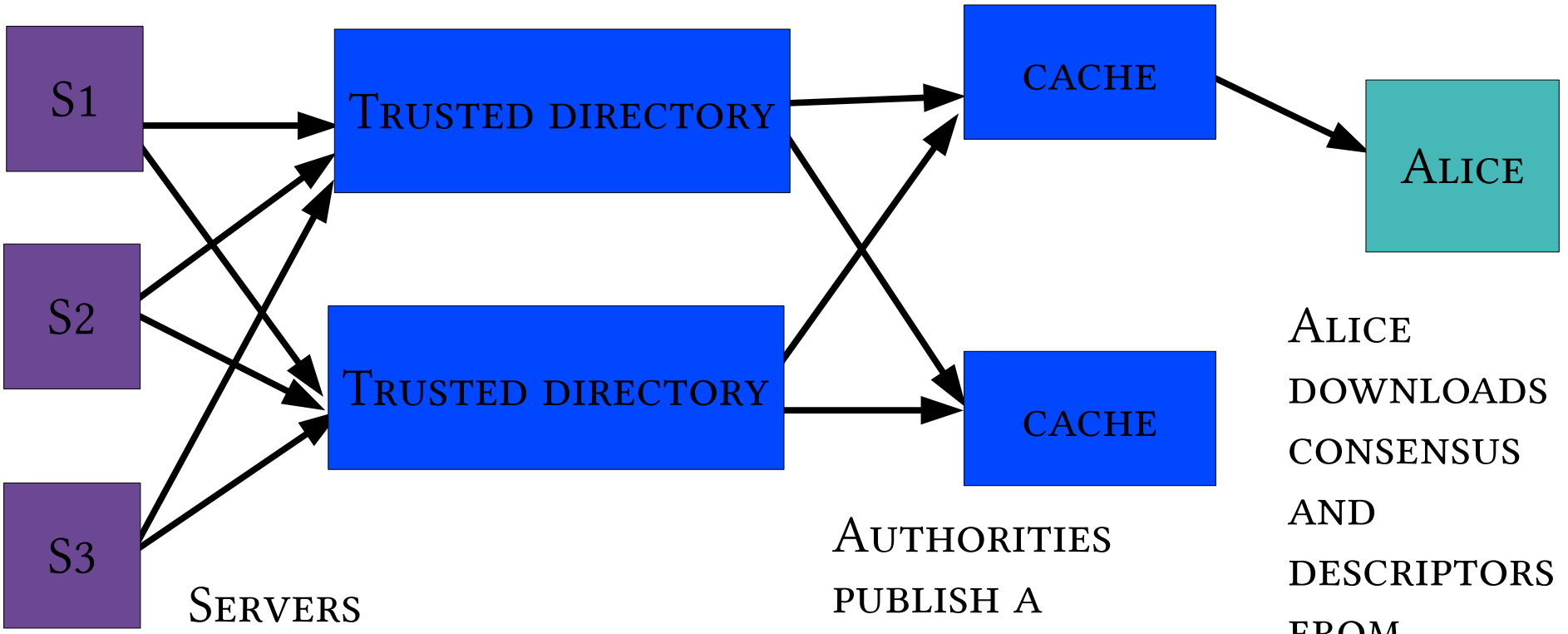
Alice makes a session key with R1 ...And then tunnels to R2...and to R3



Relay versus Discovery

- There are two pieces to all these "proxying" schemes:
- a **relay** component: building circuits, sending traffic over them, getting the crypto right
- a **discovery** component: learning what relays are available

The basic Tor design uses a simple centralized directory protocol



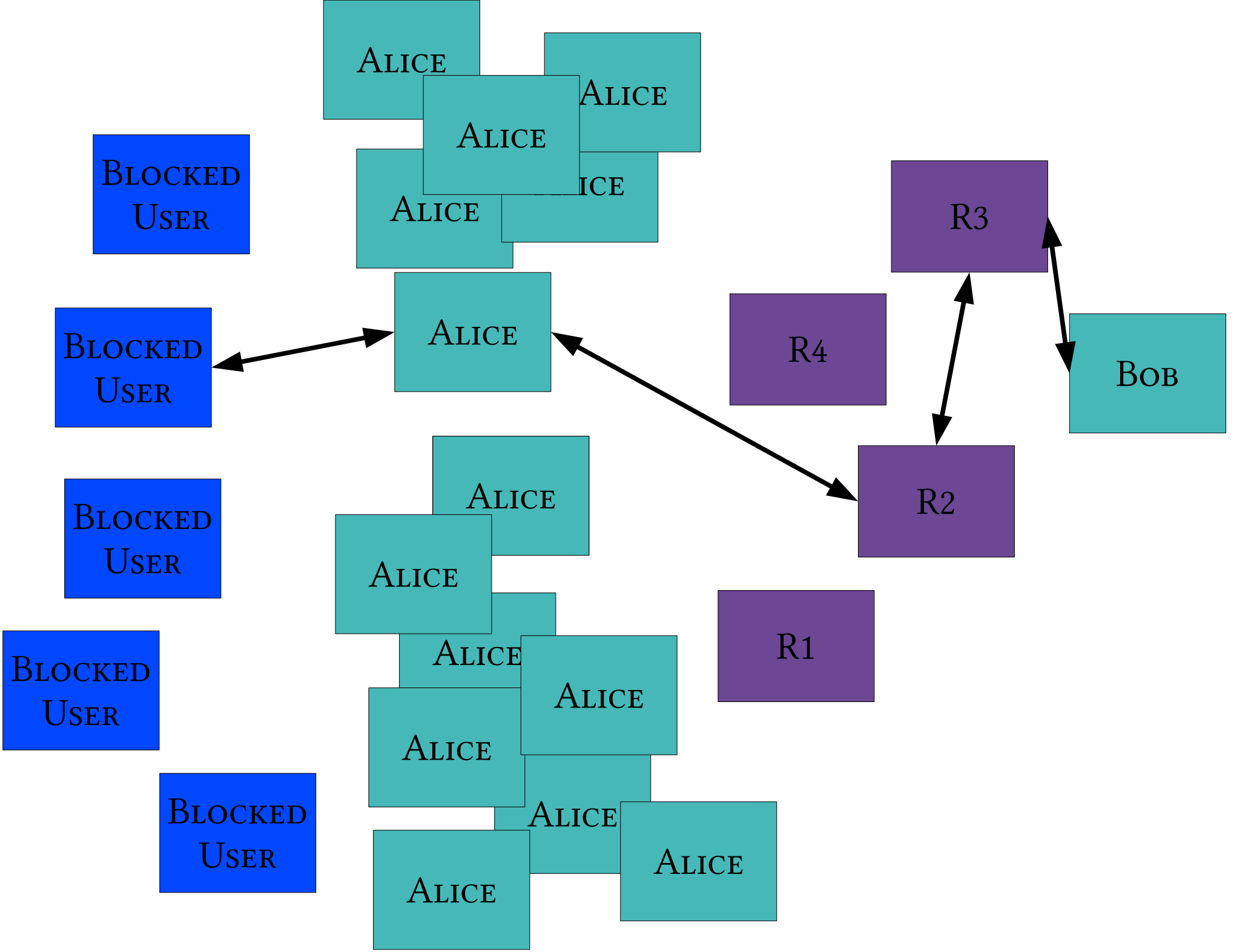
Servers publish self-signed descriptors.

Authorities publish a consensus list of all descriptors

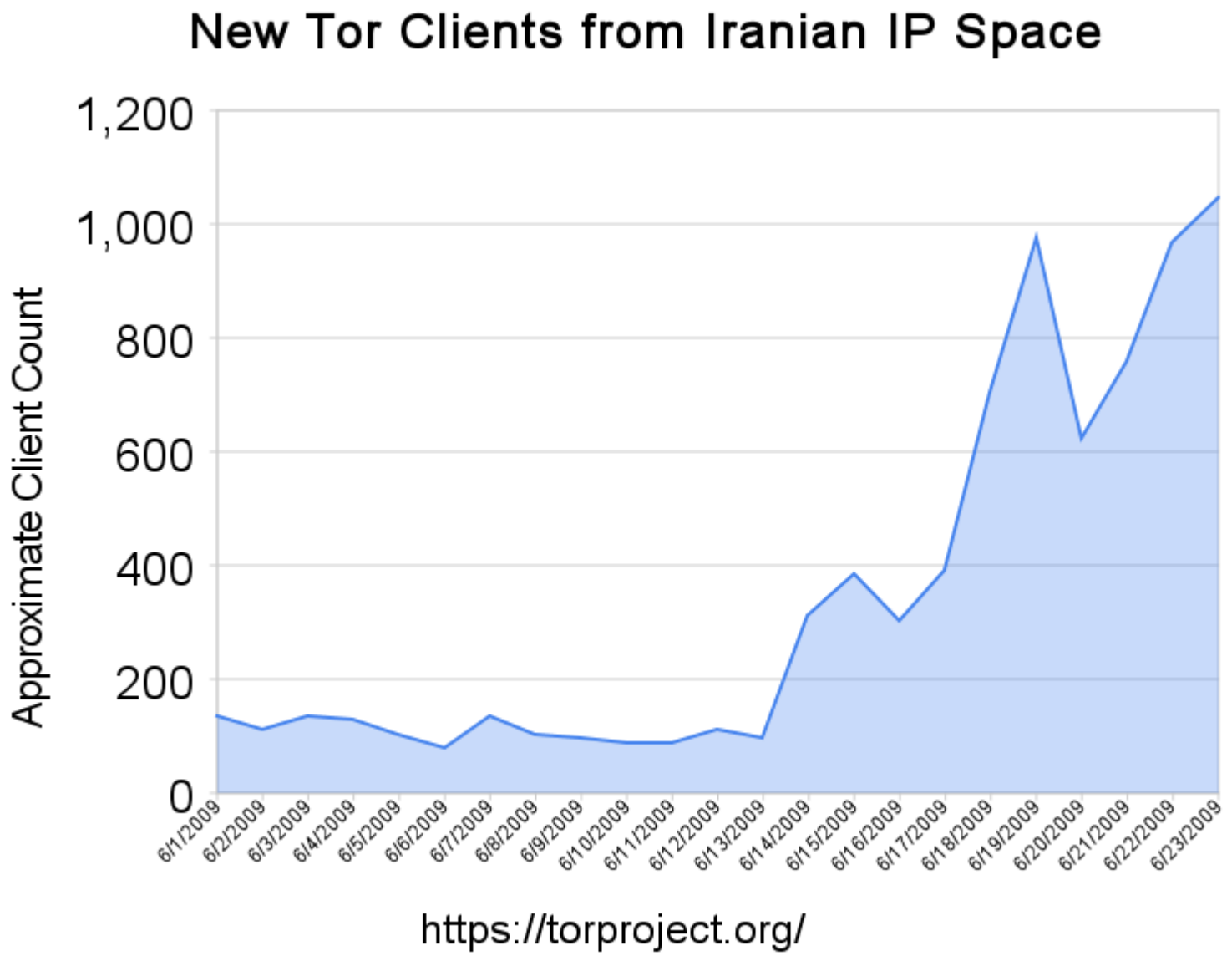
Alice downloads consensus and descriptors from anywhere

Attackers can block users from connecting to the Tor network

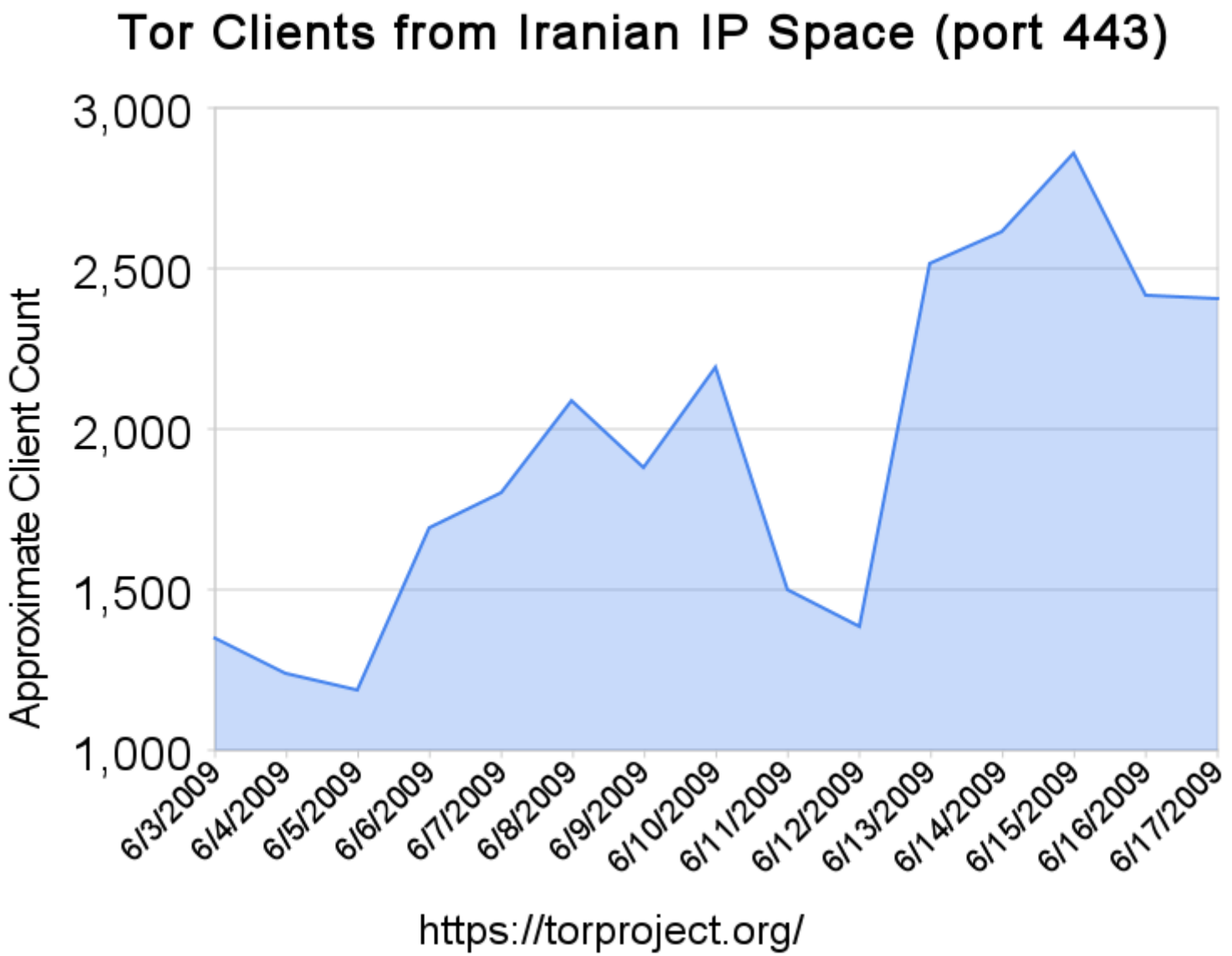
- By blocking the directory authorities
- By blocking all the relay IP addresses in the directory
- By filtering based on Tor's network fingerprint
- By preventing users from finding the Tor software


Alice
Alice
Alice
Alice
Alice
Blocked User
Blocked User
Blocked User
Blocked User
Blocked User
R3
R4
Bob
R2
R1
Alice
Alice
Alice
Alice
Alice
Alice
Alice
Alice

Tor and Circumvention



Tor and Circumvention



Tor and Circumvention

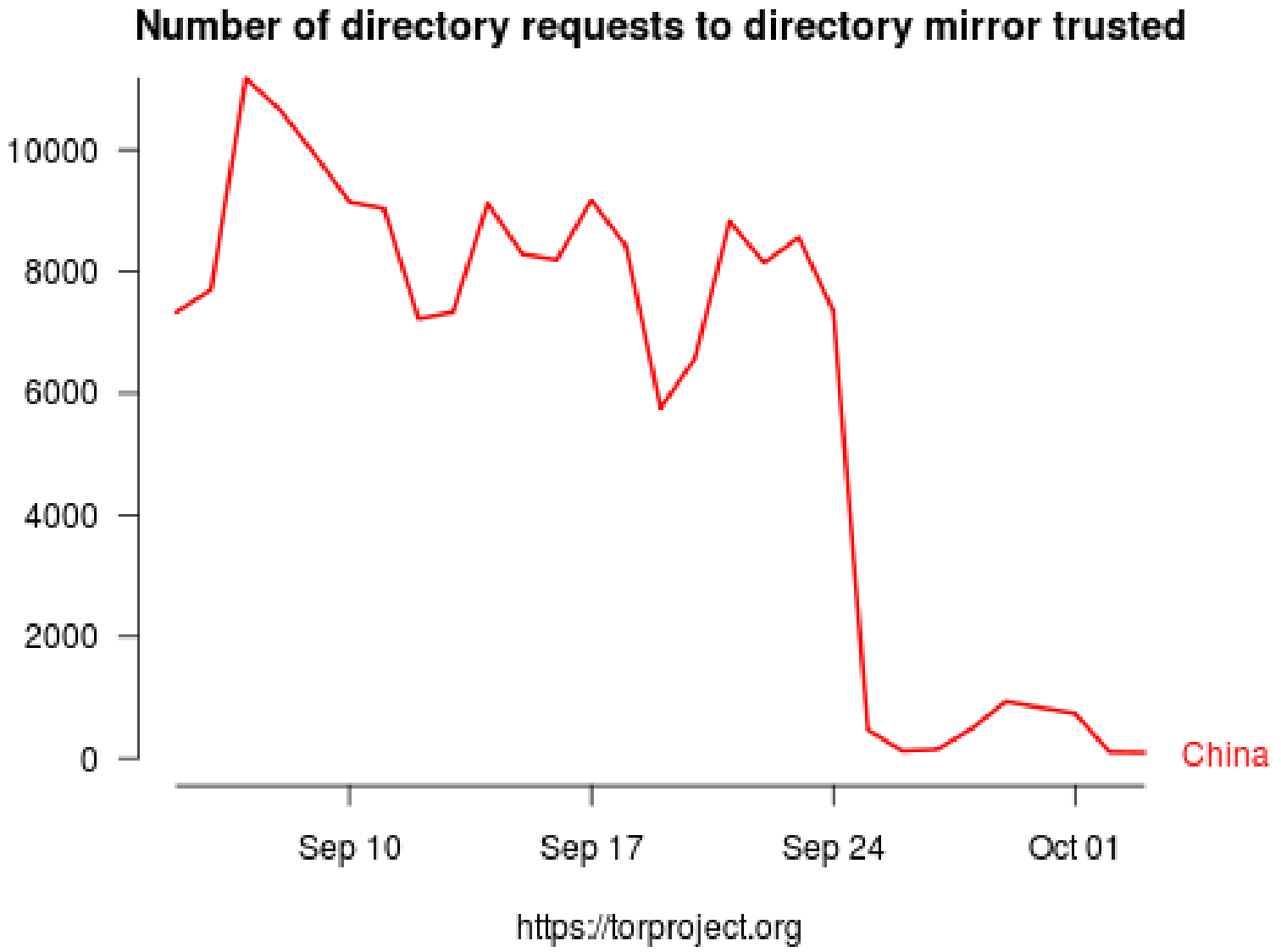
What happened around September 25th, 2009?

Tor and Circumvention

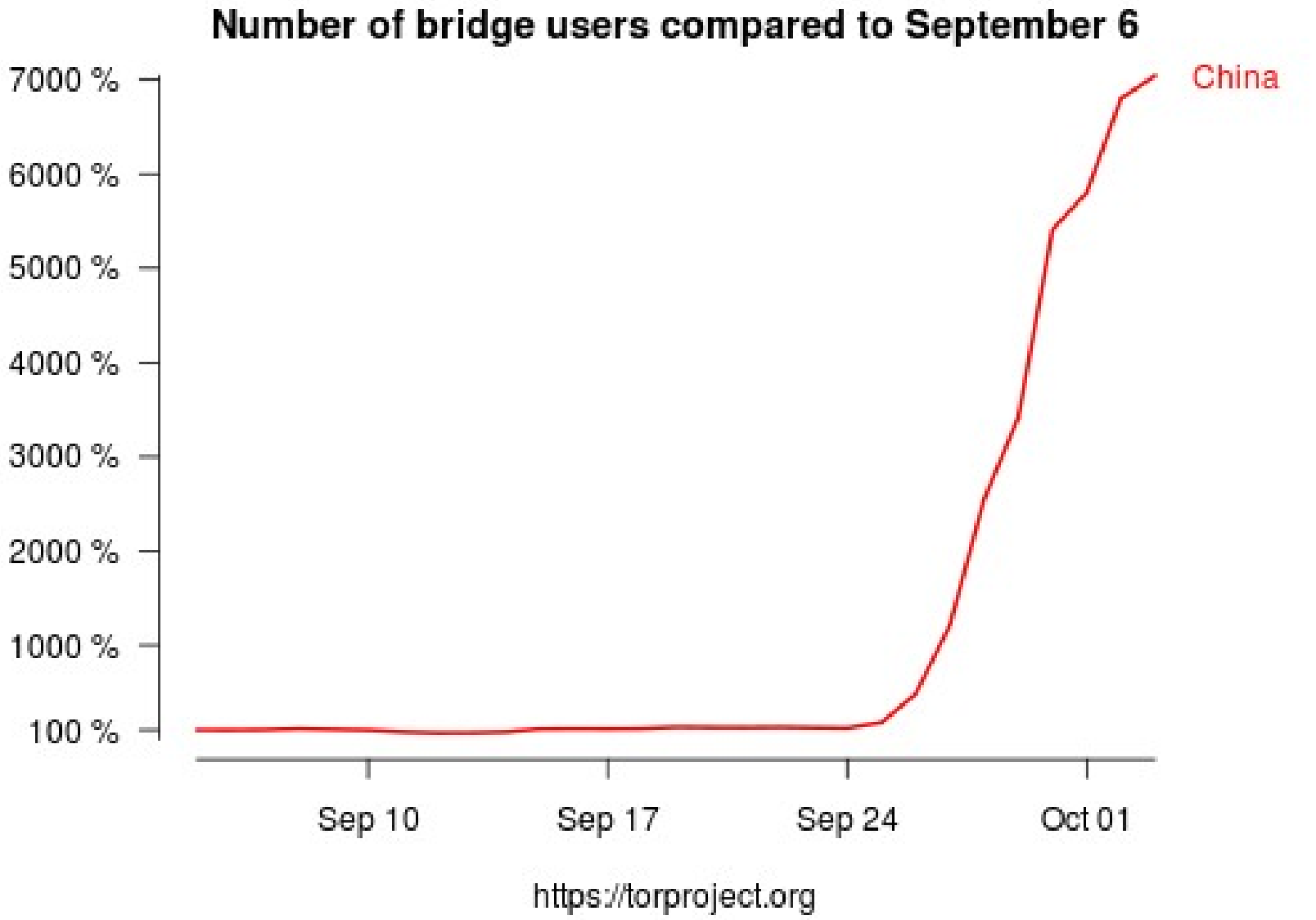
What happened around September 25th, 2009?

China blocked most of the Tor network in anticipation of the CCP 60th anniversary

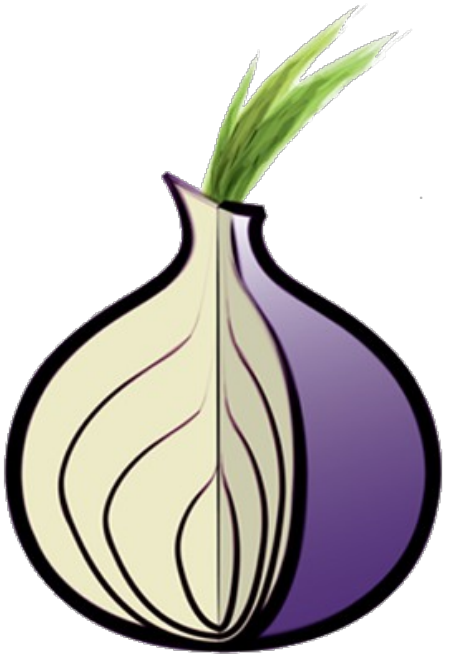
Tor and Circumvention



Tor and Circumvention



Questions?



erinn@torproject.org
https://www.torproject.org