# Tor
and
# The Tor Project

Sebastian Hahn, Linus Nordberg
The Tor Project
**https://torproject.org/**

# What is Tor?

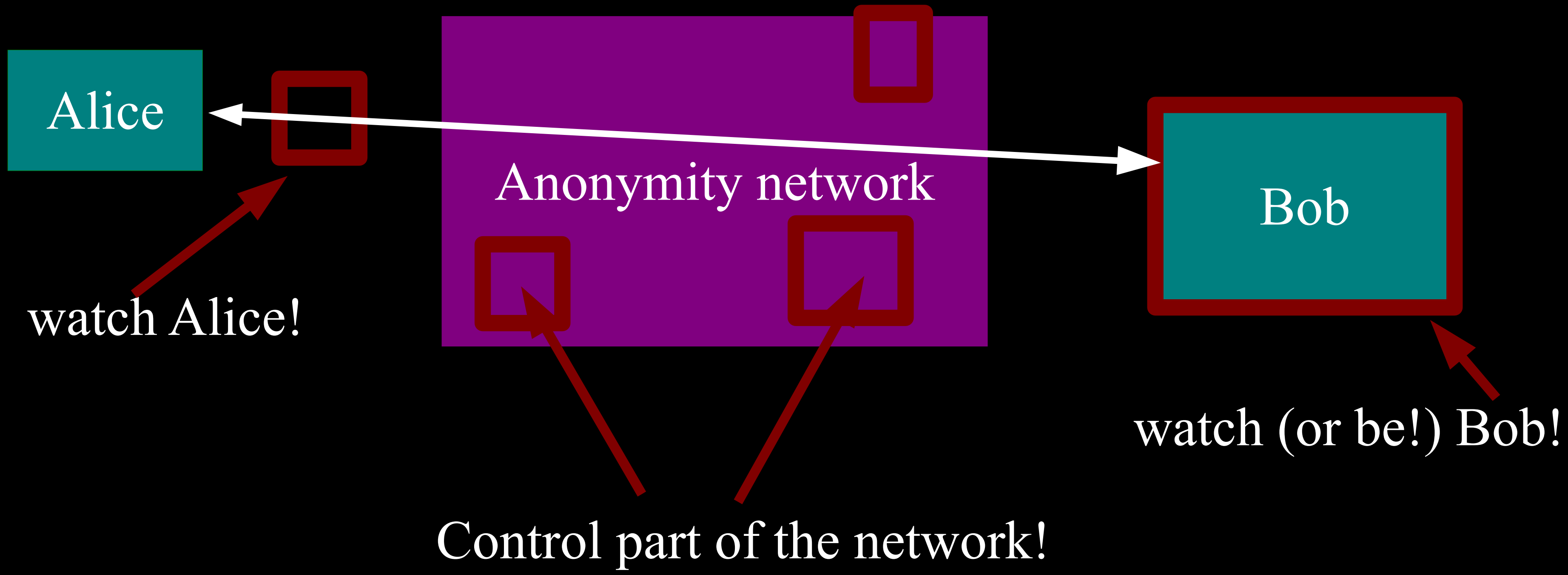
- Online anonymity 1) software 2) network 3) protocol
- Open source, freely available
- Community of researchers, developers, users, and relay operators
- Funding from NLNet, US DoD, EFF, Voice of America, Google, Human Rights Watch, ...

# The Tor Project, Inc.

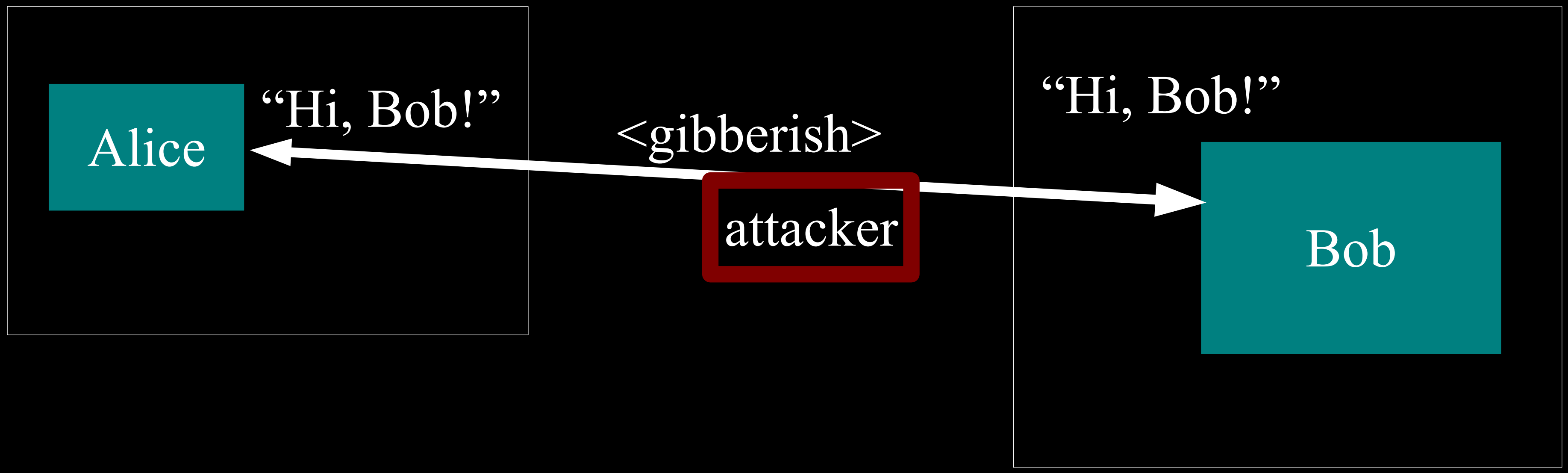
- 501(c)(3) non-profit organization dedicated to the research and development of tools for online anonymity and privacy

Estimated 400,000 daily Tor users

# 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!”

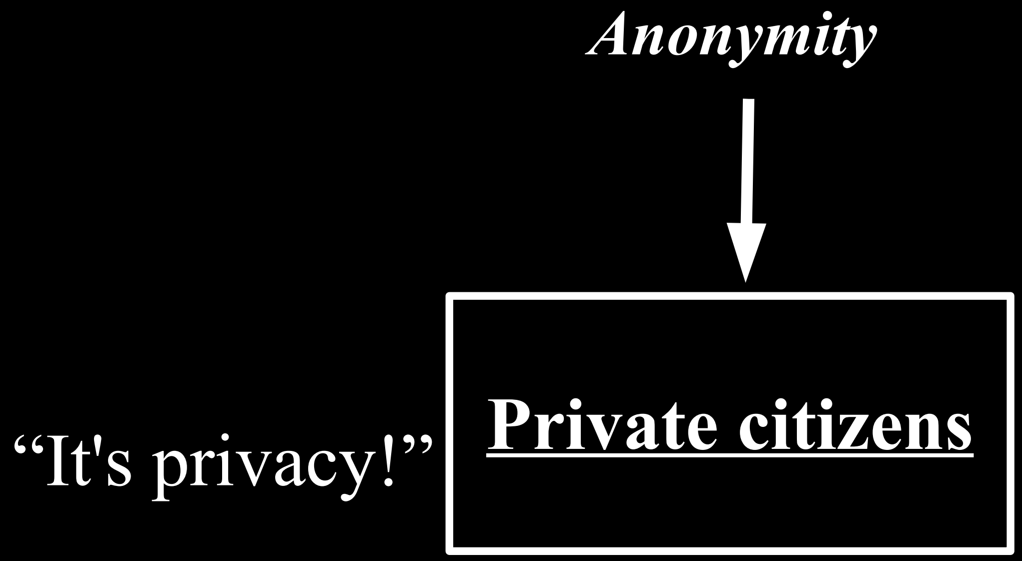
“Promise you won't tell!”

“I didn't write my name on it!”

“Isn't the Internet already anonymous?”

Tor provides anonymity by design, not by policy!

# Anonymity serves different interests for different user groups.

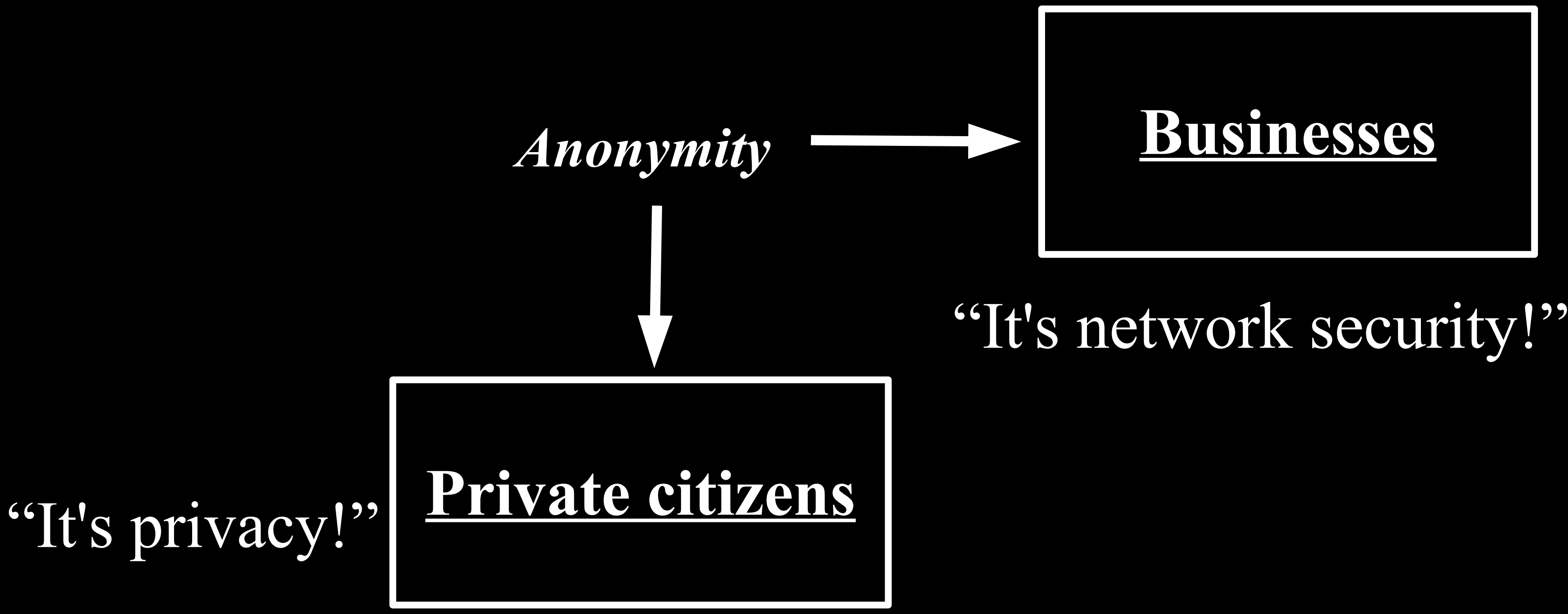


*Anonymity*

**Private citizens**

"It's privacy!"

# Anonymity serves different interests for different user groups.



*Anonymity*

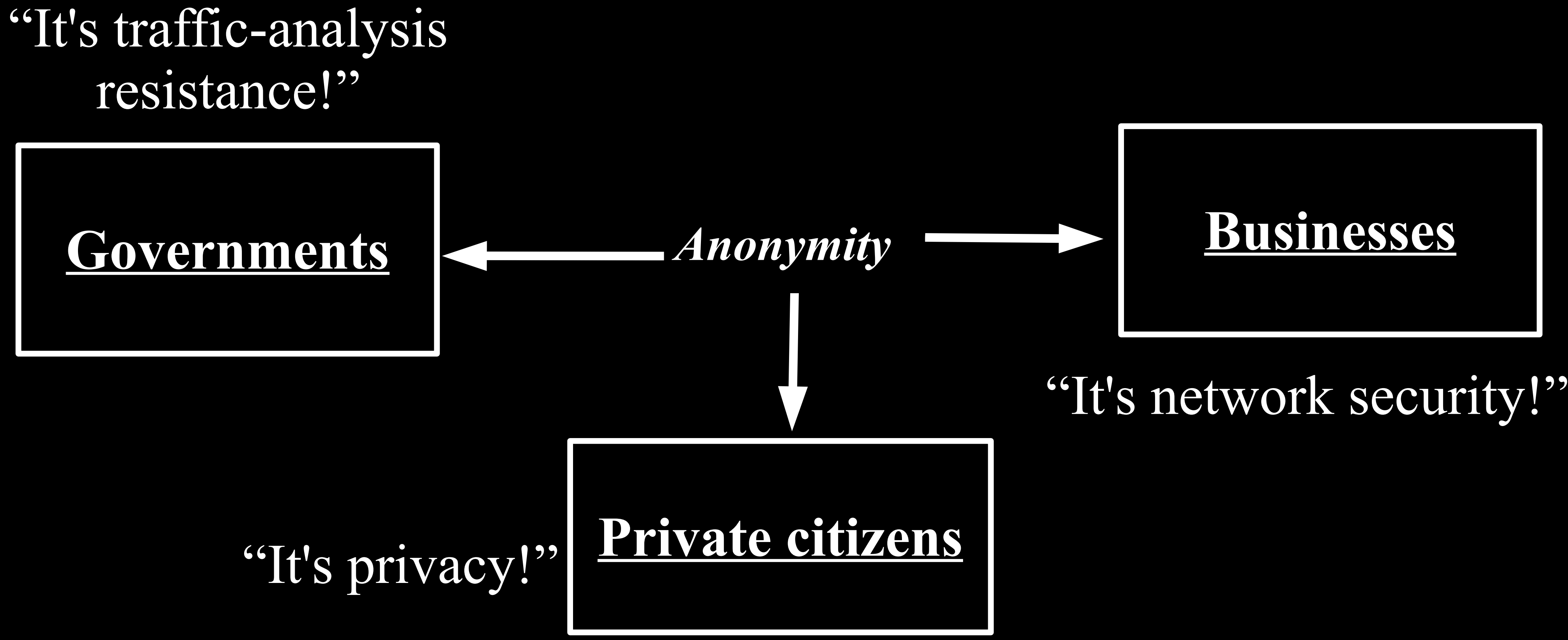
**Businesses**

"It's network security!"

**Private citizens**

"It's privacy!"

# Anonymity serves different interests for different user groups.



“It's traffic-analysis resistance!”

**Governments**

*Anonymity*

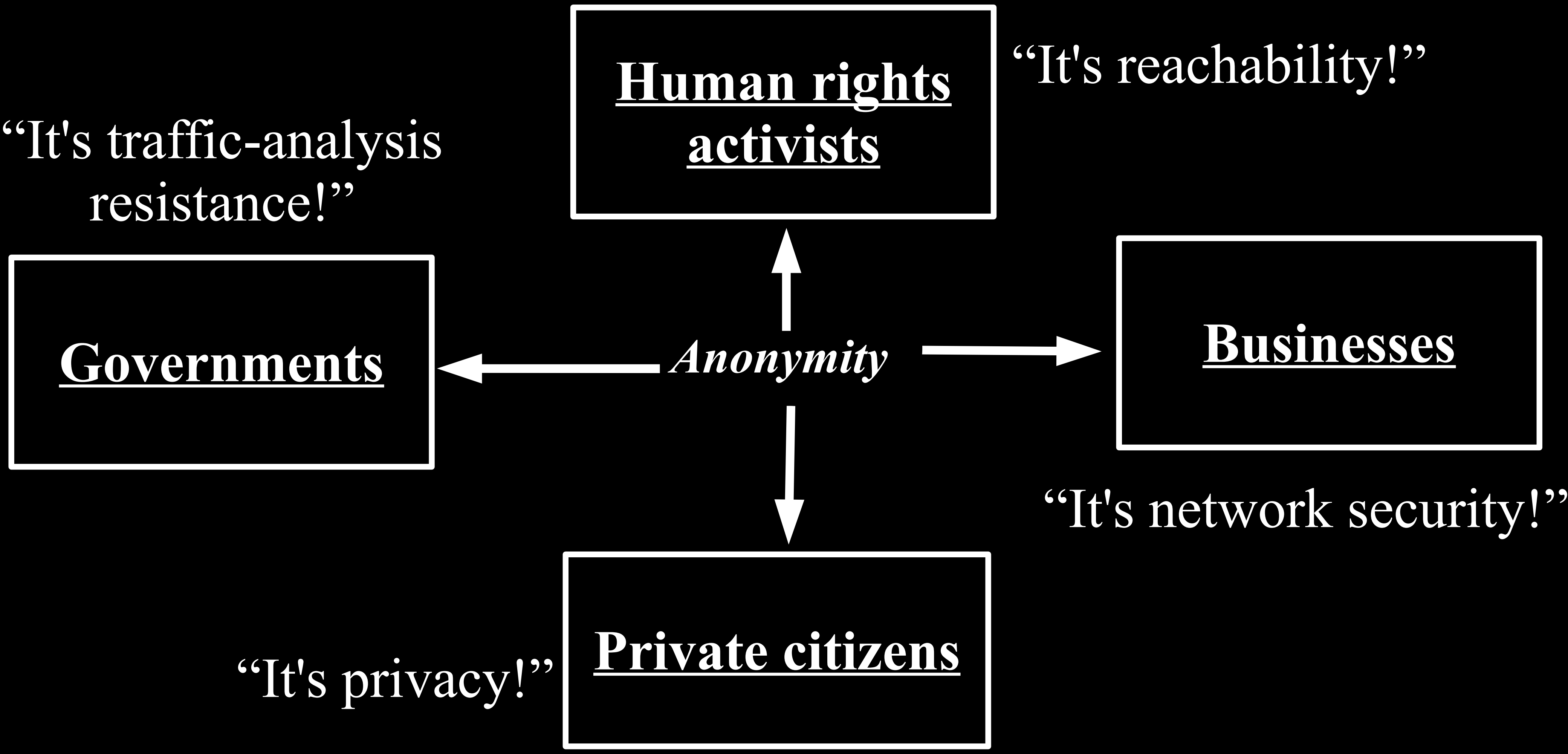
**Businesses**

“It's network security!”

**Private citizens**

“It's privacy!”

# Anonymity serves different interests for different user groups.



*Anonymity*

**Human rights activists**

“It's reachability!”

**Governments**

“It's traffic-analysis resistance!”

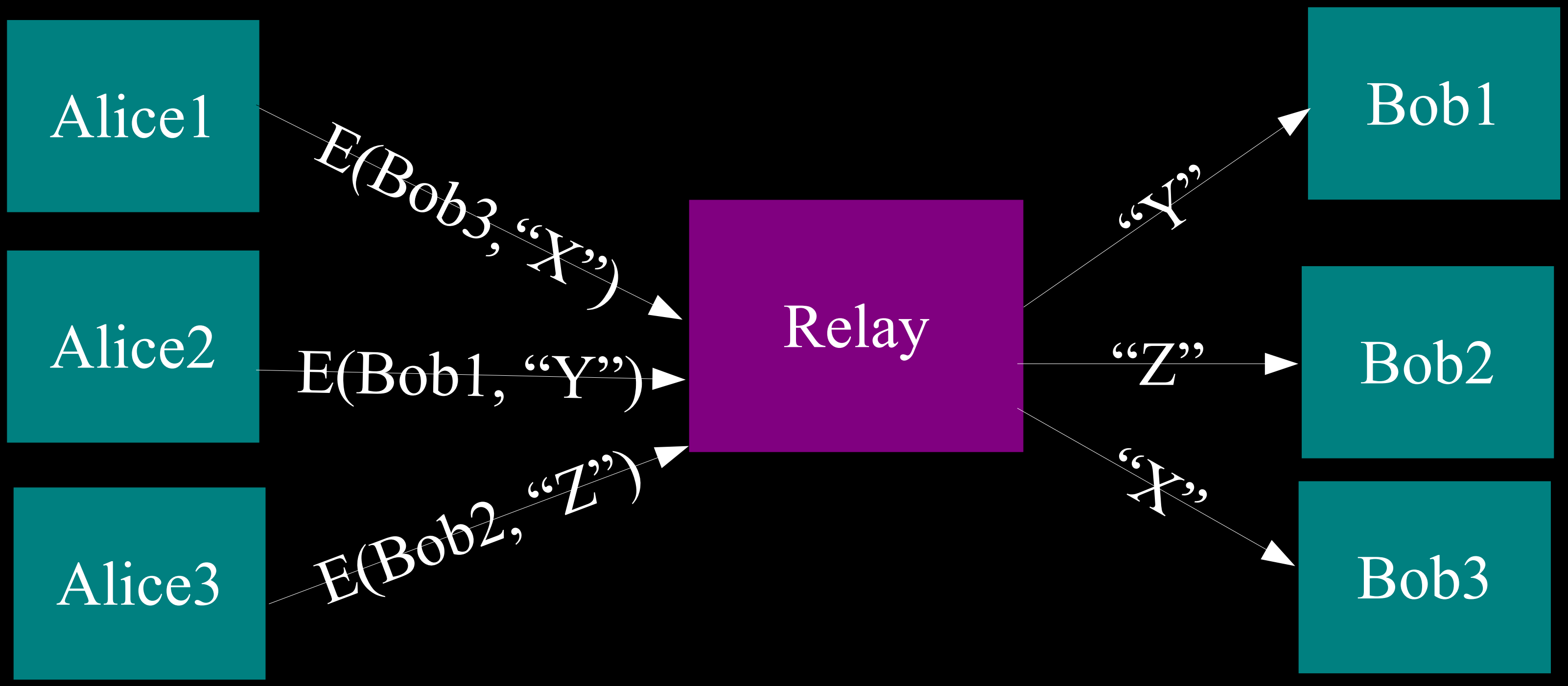
**Businesses**

“It's network security!”

**Private citizens**

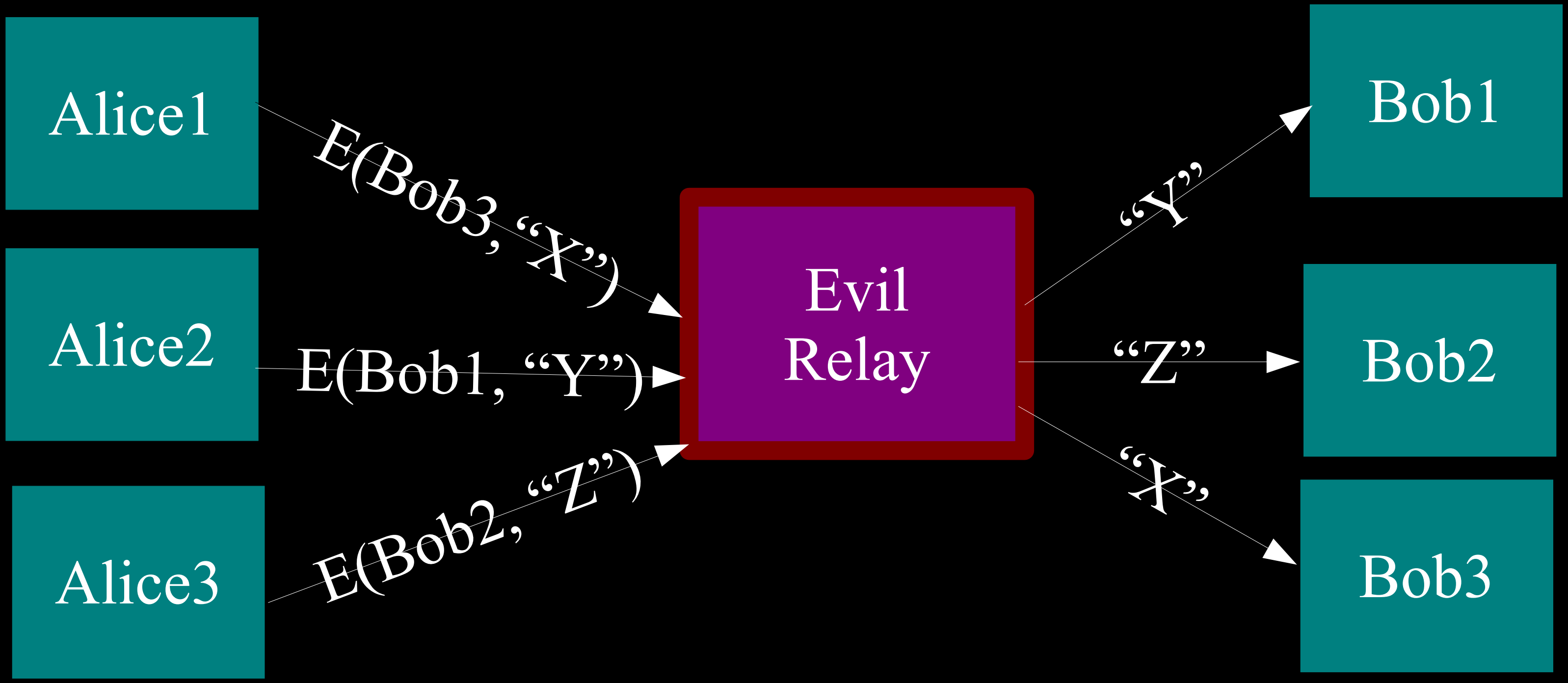
“It's privacy!”

# The simplest designs use a single relay to hide connections.

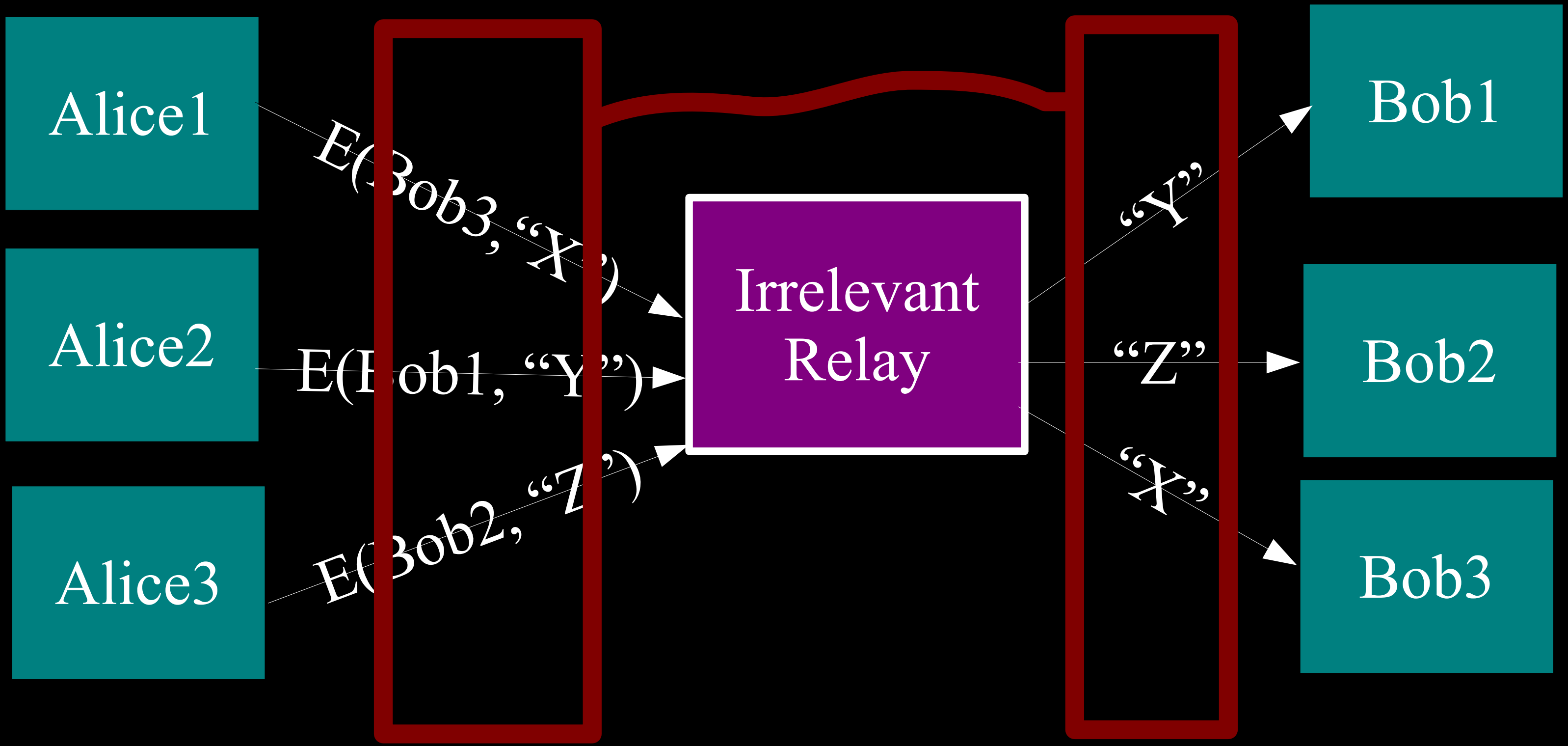


(example: some commercial proxy providers)

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

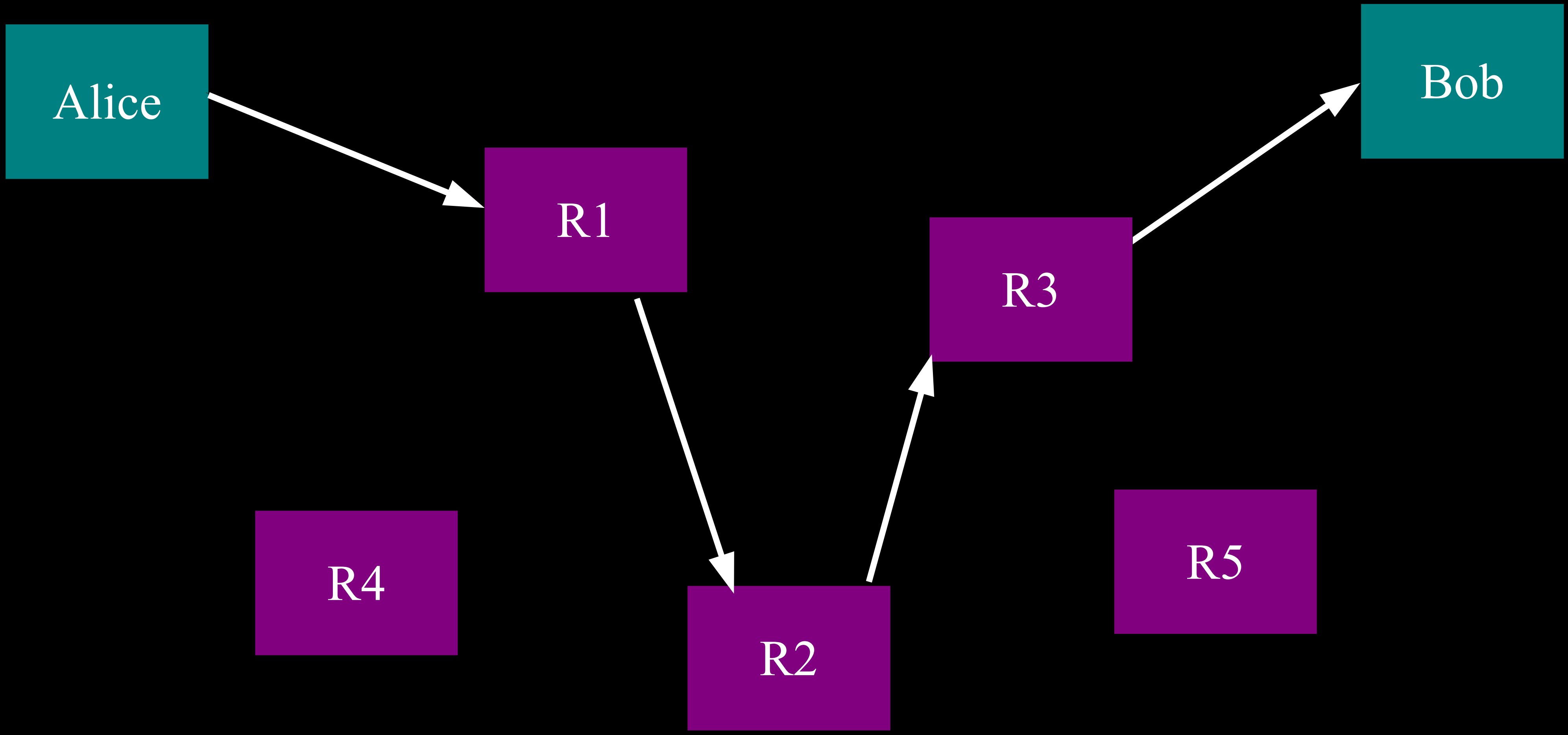


# ... or a single point of bypass.

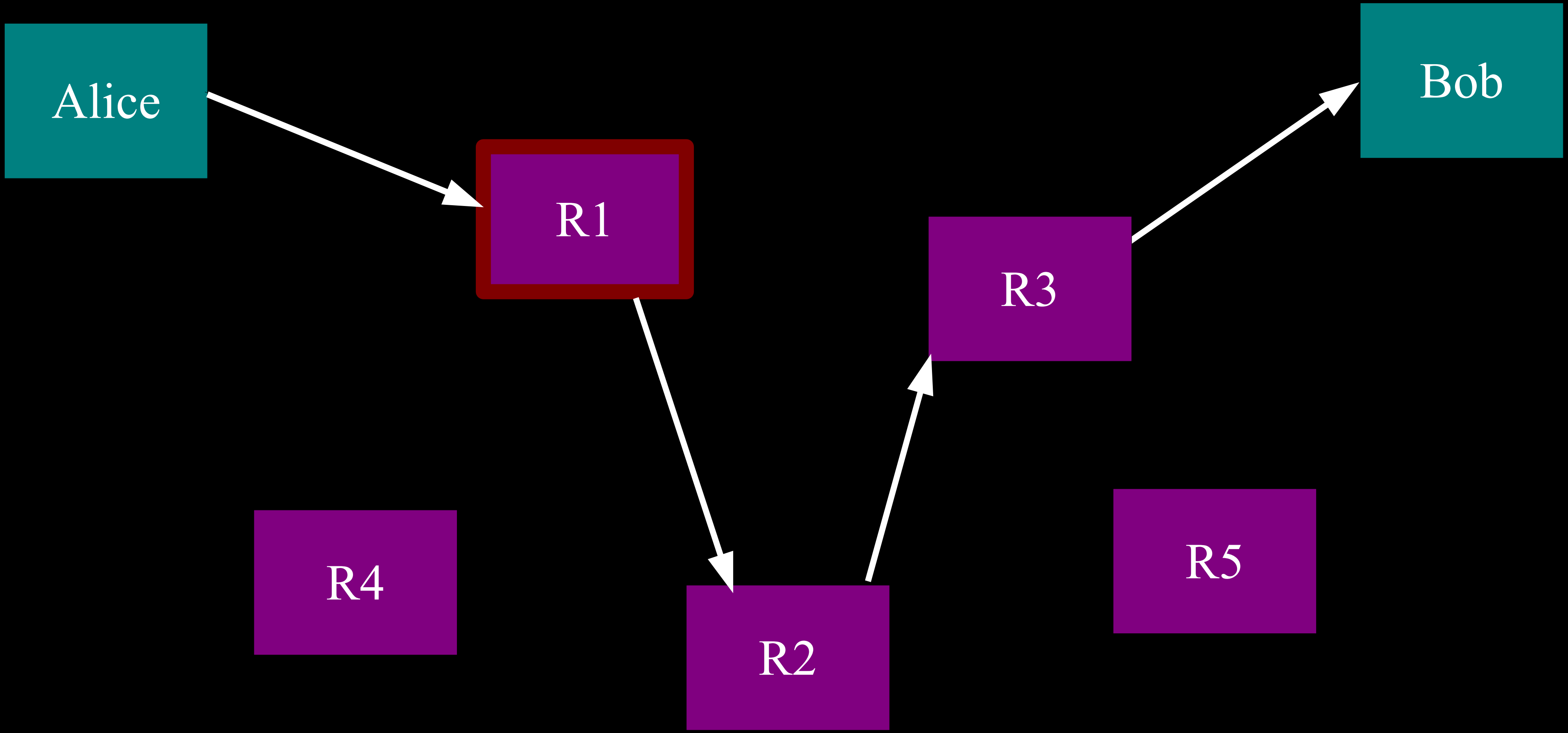


Timing analysis bridges all connections through relay ⇒ An attractive fat target

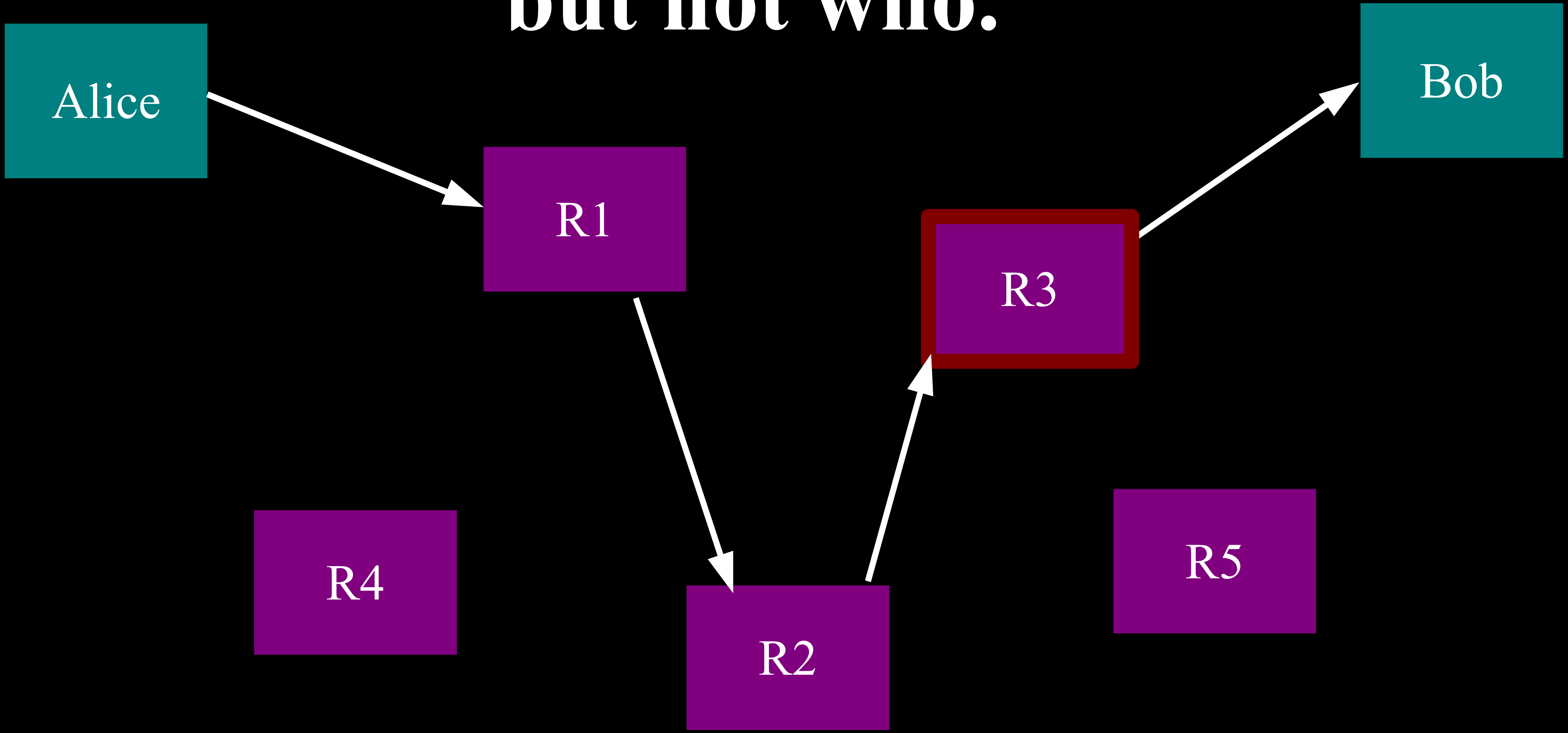
# So, add multiple relays so that no single one can betray Alice.



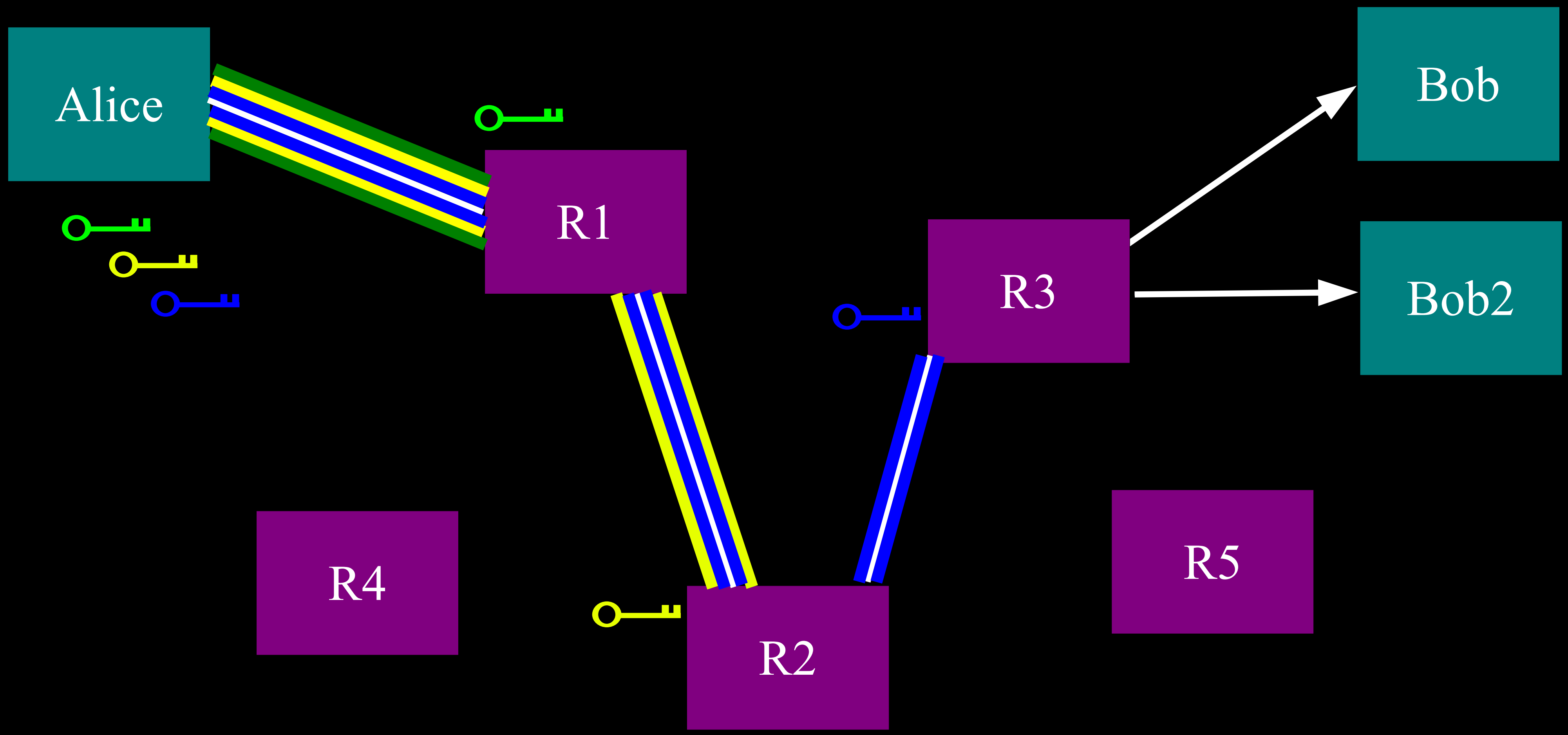
# A corrupt first hop can tell that Alice is talking, but not to whom.



# 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



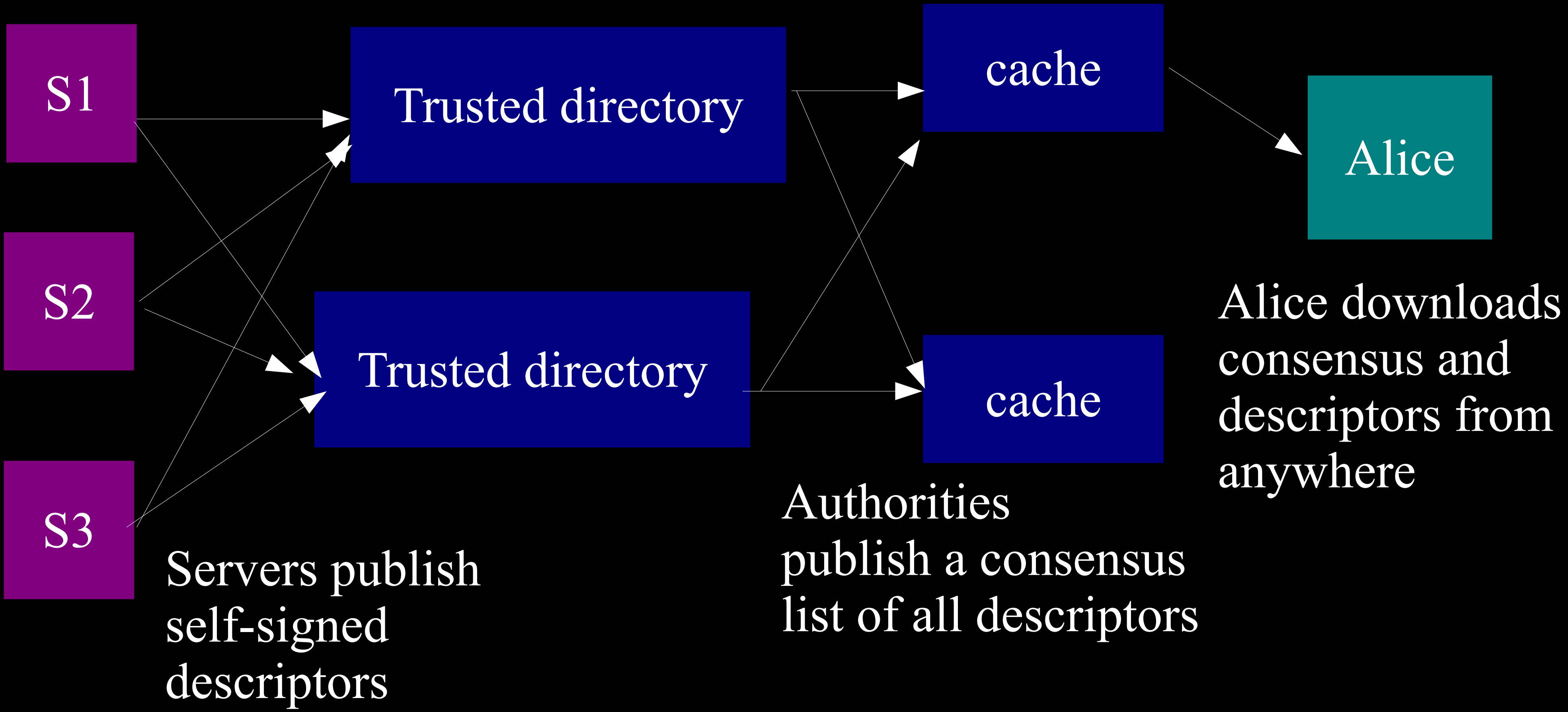
# Relay versus Discovery

There are two pieces to all these “proxying” schemes:

a **relay** component: building circuits, sending traffic over them, getting the crypto right, forwarding traffic to the destination

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

# Sustainability

- Tor has a community of developers and volunteers with an open development model
- Commercial anonymity systems have flopped or constantly need more funding for bandwidth
- Our sustainability is rooted in Tor's open design: clear documentation, modularity, and open source

# Tor gives three anonymity properties

- **#1**: A local network attacker can't learn, or influence, your destination
  - Clearly useful for blocking resistance
- **#2**: No single router can link you to your destination
  - The attacker can't sign up relays to trace users
- **#3**: The destination, or somebody watching it, can't learn your location
  - So they can't reveal you; or treat you differently

# Local network threats

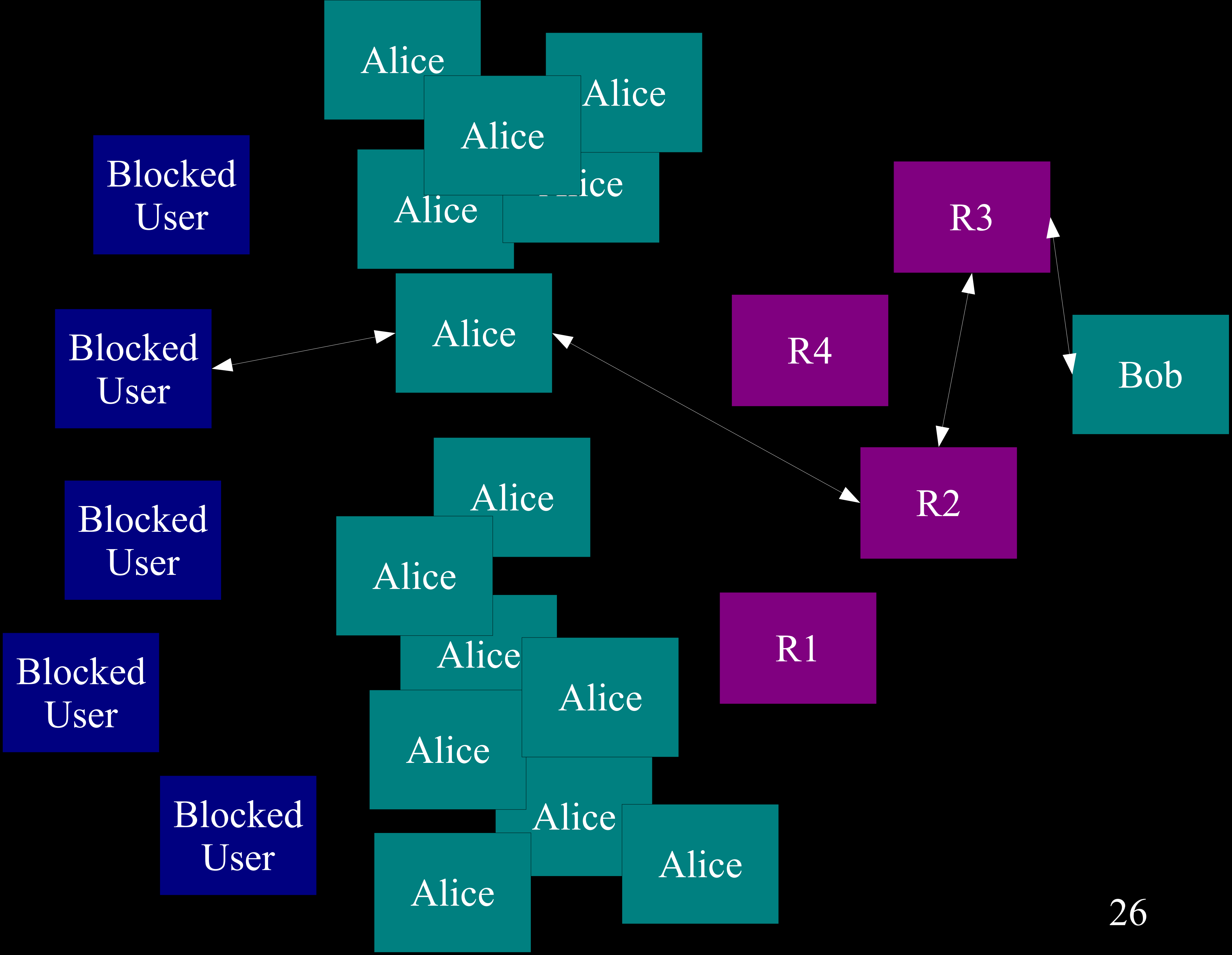
- **#1**: Someone sniffing your W-Lan
  - The guy next to you at Starbucks
  - Your kids?
- **#2**: Your ISP …
  - Logging, active attacks on traffic
  - DNS attacks (censorship, hijacking, ...)
- **#3**: … and their partners
  - Phorm

# ISP-level attacks

- Block by IP address / port at firewall
- Intercept DNS requests and give bogus responses or redirects
- China: Keywords in TCP packets
- Iran: DPI to filter SSL when they want
- Russia: Don't block, just pollute

# Attackers can block users from connecting to the Tor network

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



Alice

Alice

Alice

Blocked
User

Alice

lice

R3

Alice

R4

Blocked
User

Bob

Alice

R2

Blocked
User

Alice

Alice

R1

Alice

Blocked
User

Alice

Alice

Blocked
User

Alice

Alice

# “Bridge” relays

- Hundreds of thousands of Tor users, already self-selected for caring about privacy
- Rather than signing up as a normal relay, you can sign up as a special “bridge” relay that isn't listed in any directory
- No need to be an “exit” (so no abuse worries), and you can rate limit if needed
- Integrated into Vidalia (our GUI) so it's easy to offer a bridge or to use a bridge

# One working bridge is enough

- Connect via that bridge to the bridge authority
- ...and to the main Tor network
- Remember, all of this happens in the background
- “How to circumvent for all transactions (and trust the pages you get)”
  is now reduced to
  “How to learn about a working bridge”

# Trust and reputation

- See Hal Roberts' blog post about how some tools sell user data http://blogs.law.harvard.edu/hroberts/
- Many of these tools see circumvention and privacy as totally unrelated goals, but both are necessary for protection

# Only a piece of the puzzle

- Assume the users aren't attacked by their hardware and software
  - No spyware installed, no cameras watching their screens, etc
- Users need to know about SSL for gmail. Cookies. End-to-end encryption.
- Many people in Iran in June were using plaintext proxies!

# Know where you send your data

- The data you/your applications share will reach its destination – Tor won't anonymize it for you
- Make your communication partners aware of the threats that you are facing
- Unfortunately, it is still easy to screw up

I CAN HAZ FREEDOM?
Tor
TorProject.org