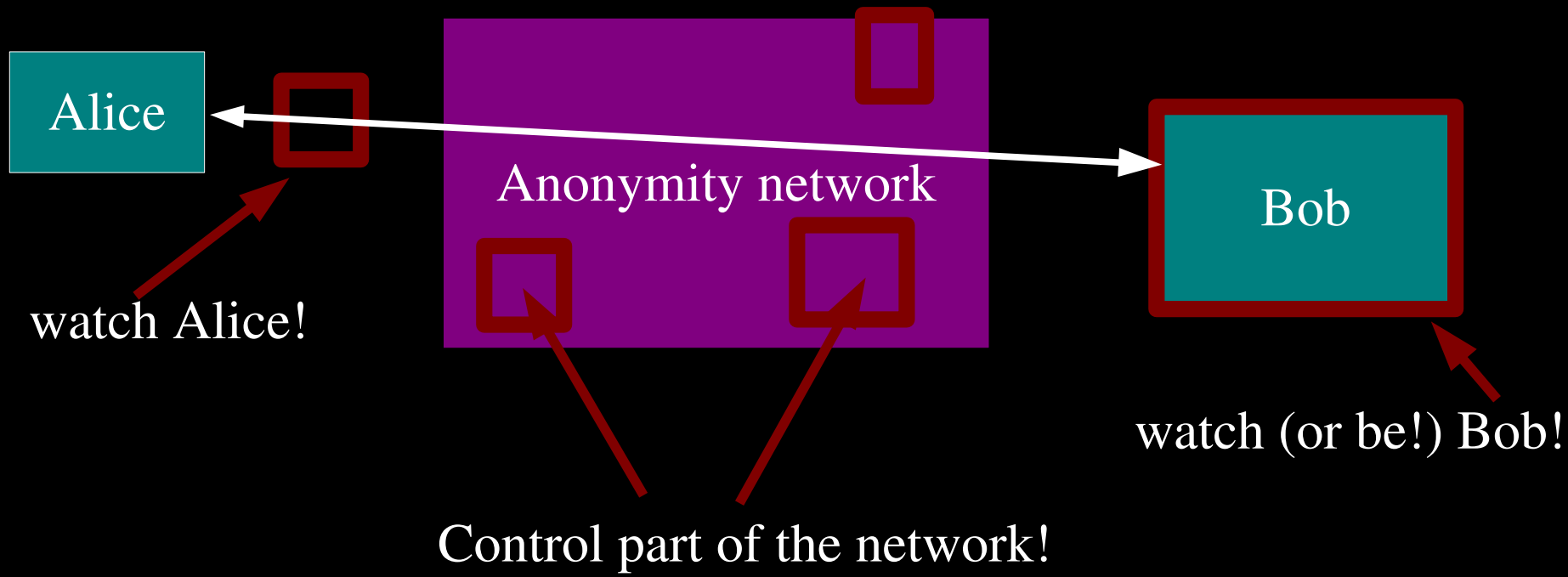
Tor: a quick overview and a call to action

Jacob Appelbaum
The Tor Project
https://www.torproject.org/

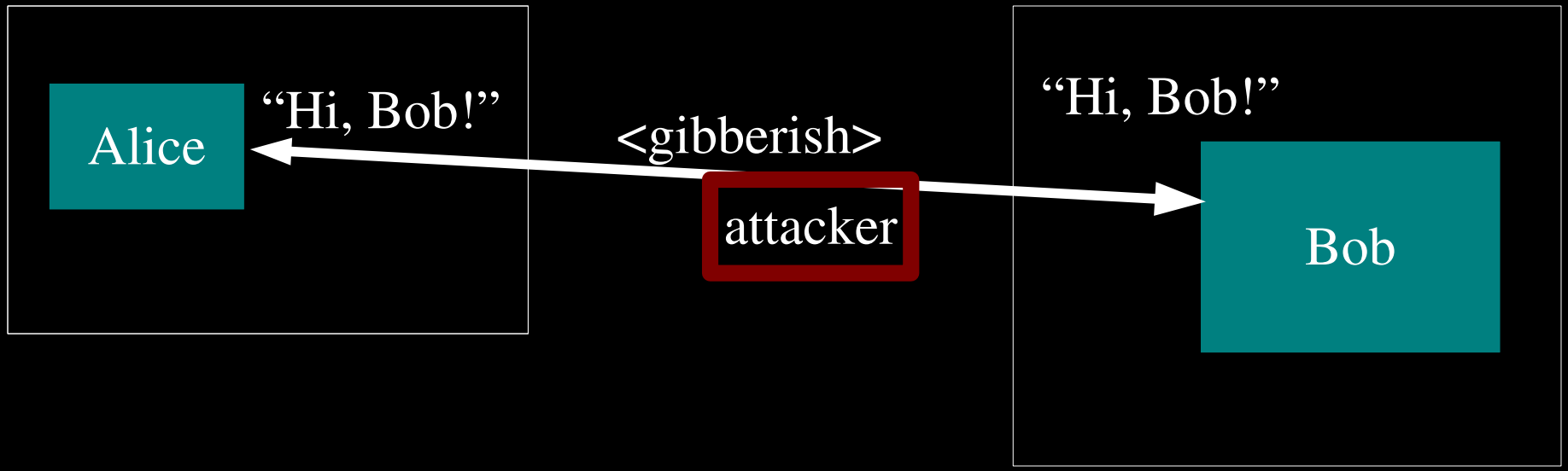
Tor: Big Picture

- 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.
- 1500 active relays, 200000+ active users, >1Gbit/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?

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!”

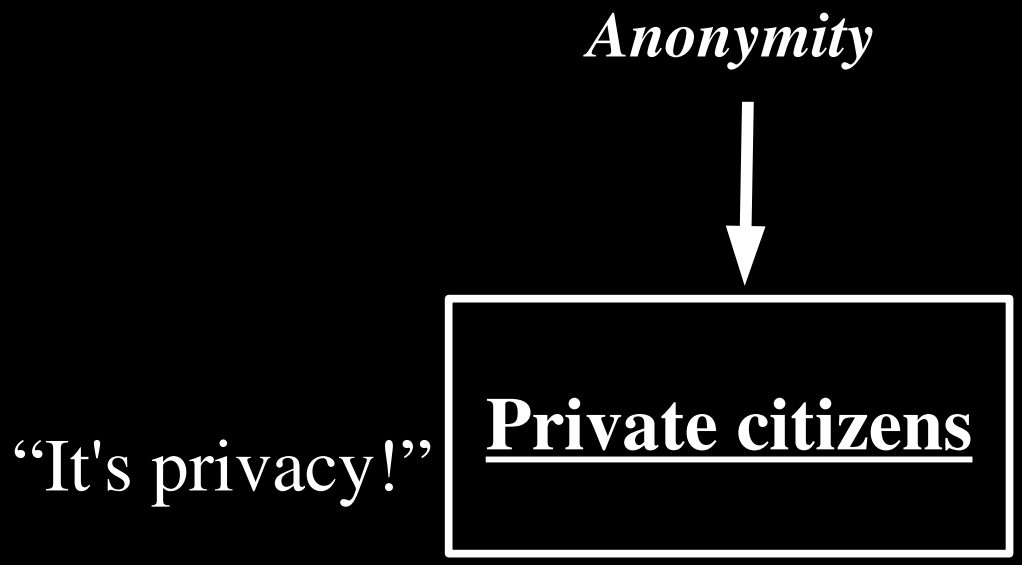
“Promise you won't remember!”

“Promise you won't tell!”

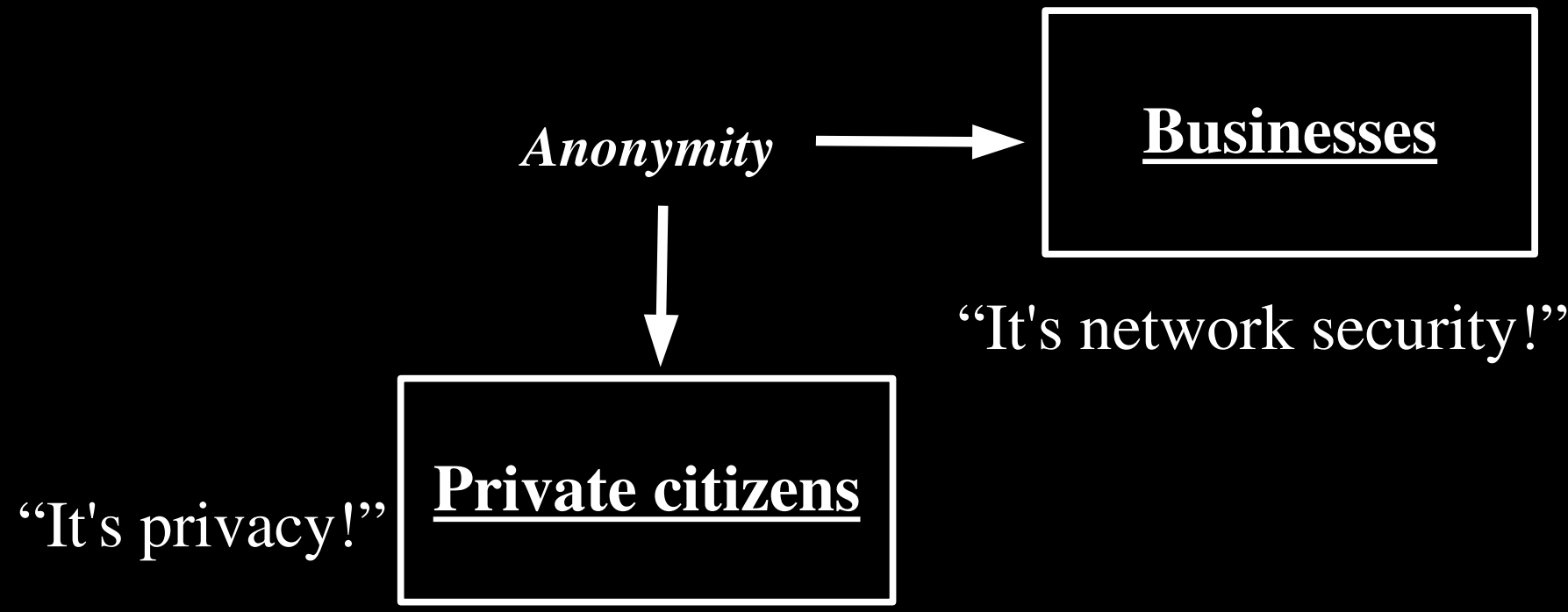
“I didn't write my name on it!”

“Isn't the Internet already anonymous?”

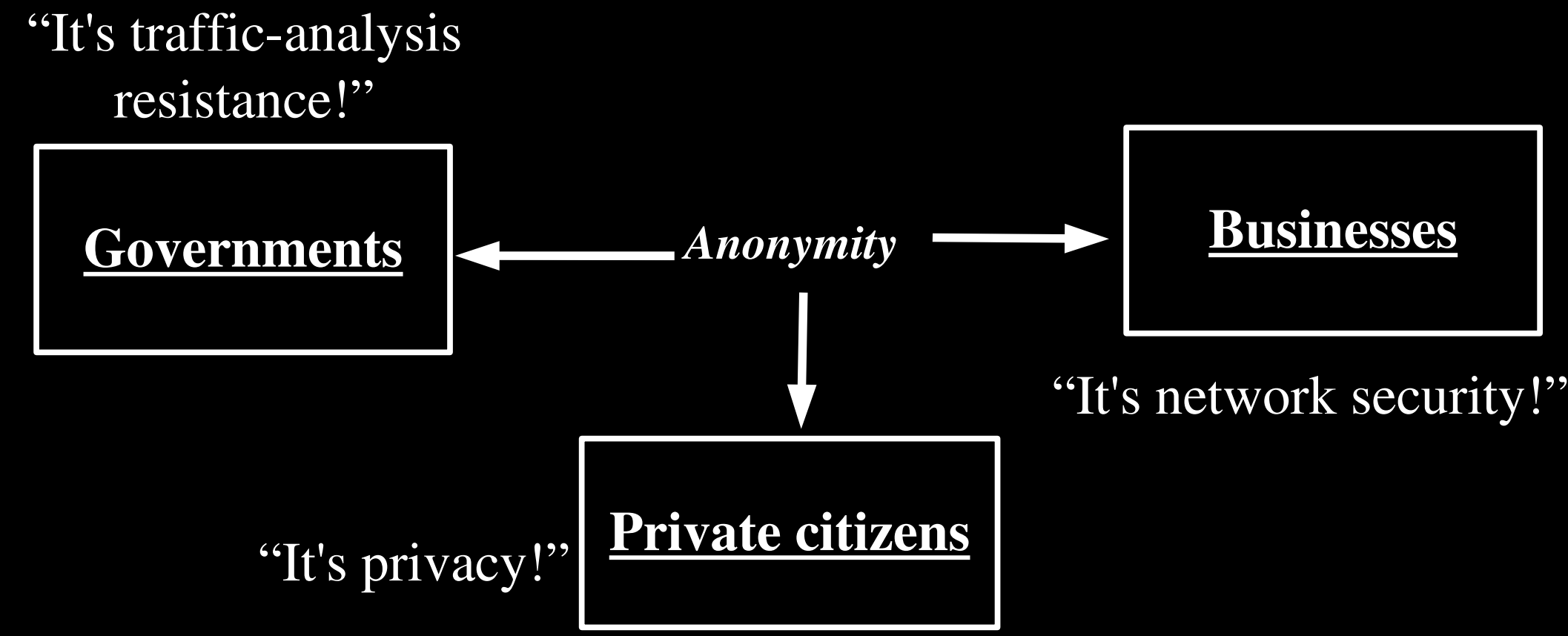
Anonymity serves different interests for different user groups.



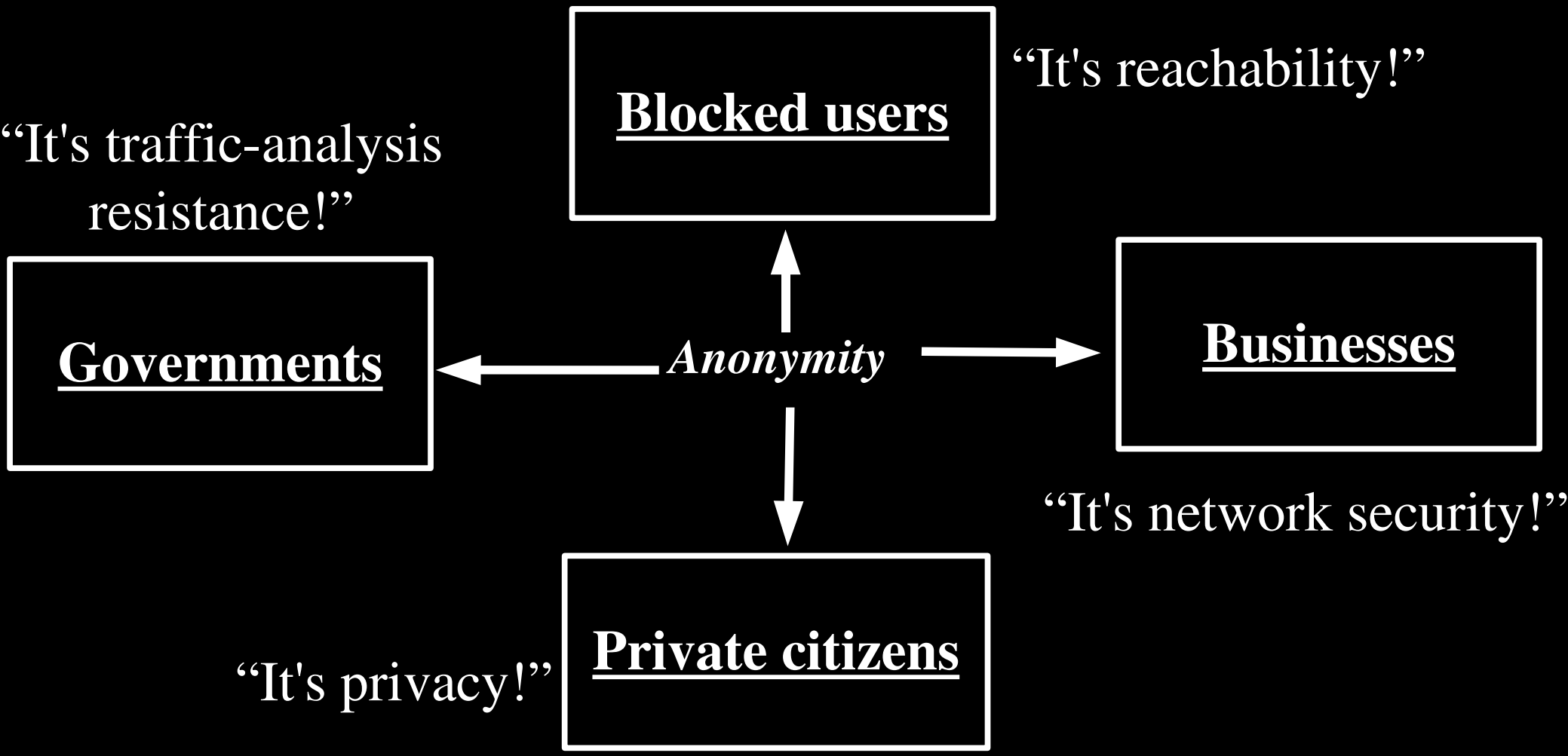
Anonymity serves different interests for different user groups.



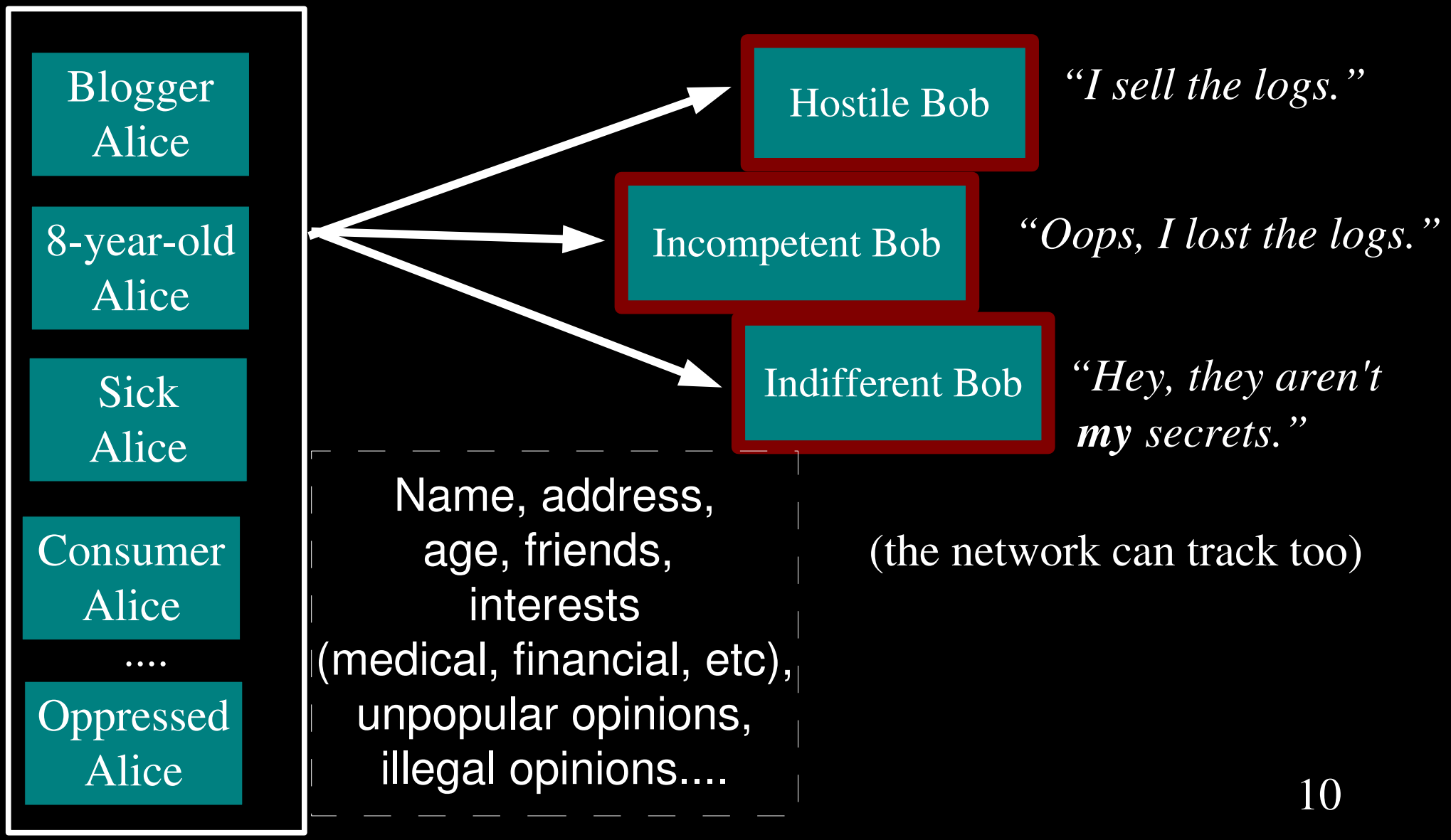
Anonymity serves different interests for different user groups.



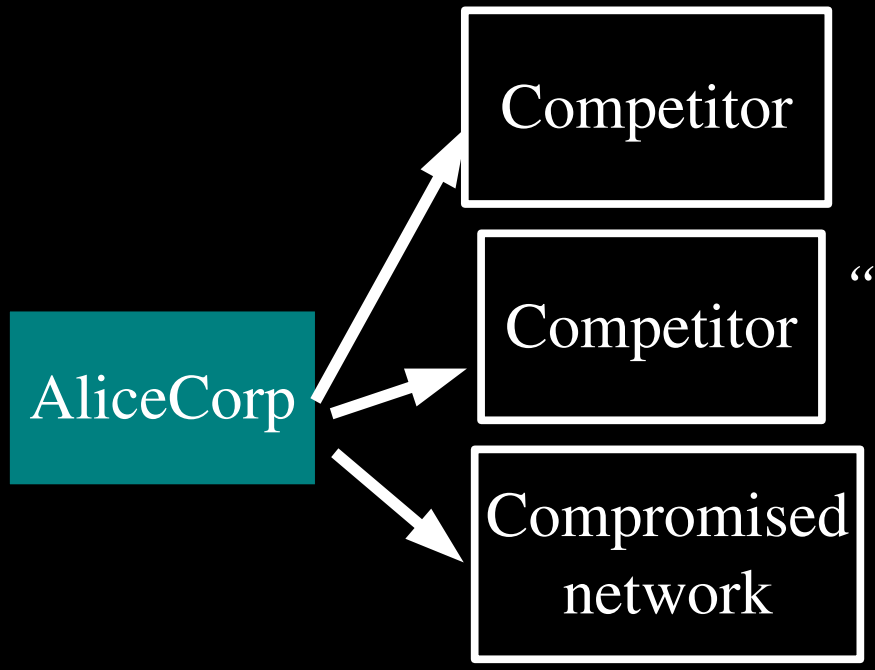
Anonymity serves different interests for different user groups.



Regular citizens don't want to be watched and tracked.



Businesses need to keep trade secrets.



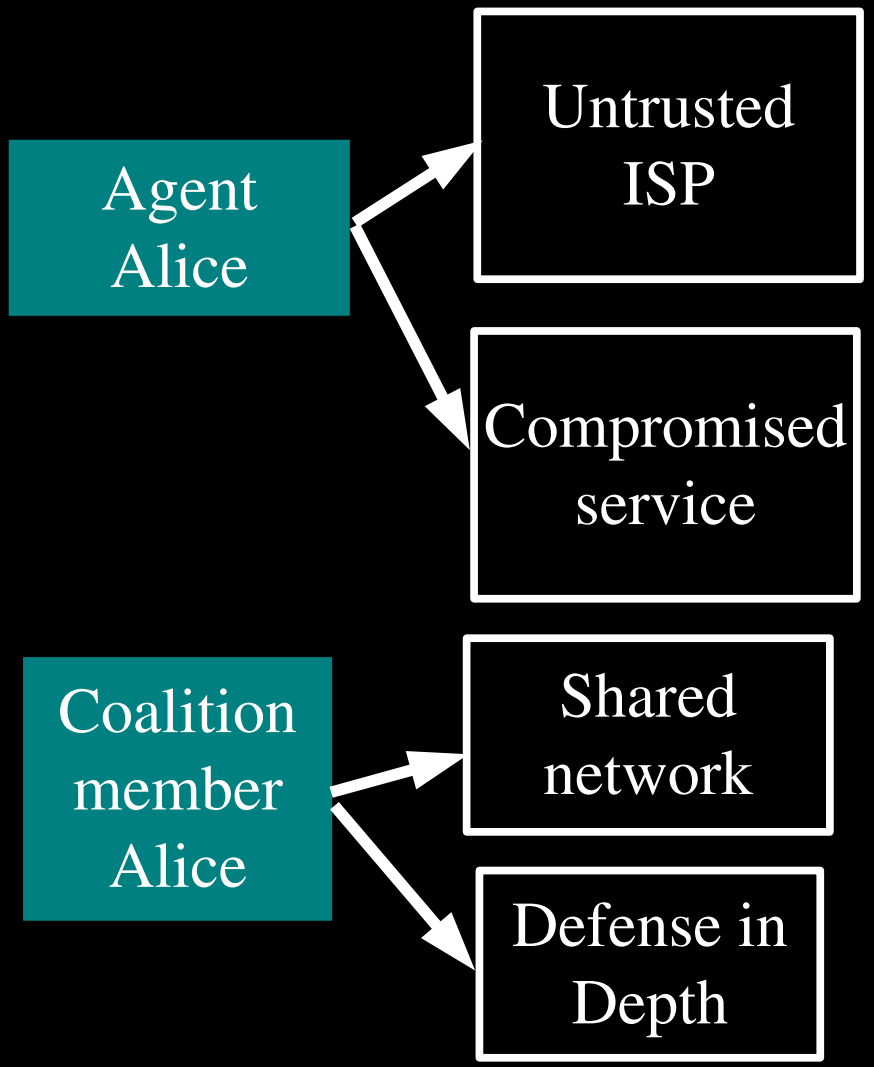
"Oh, your employees are reading our patents/jobs page/product sheets?"

"Hey, it's Alice! Give her the 'Alice' version!"

"Wanna buy a list of Alice's suppliers? What about her customers? What about her engineering department's favorite search terms?"

Law enforcement needs anonymity to get the job done.

Governments need anonymity for their security



"What will you bid for a list of Baghdad IP addresses that get email from .gov?"

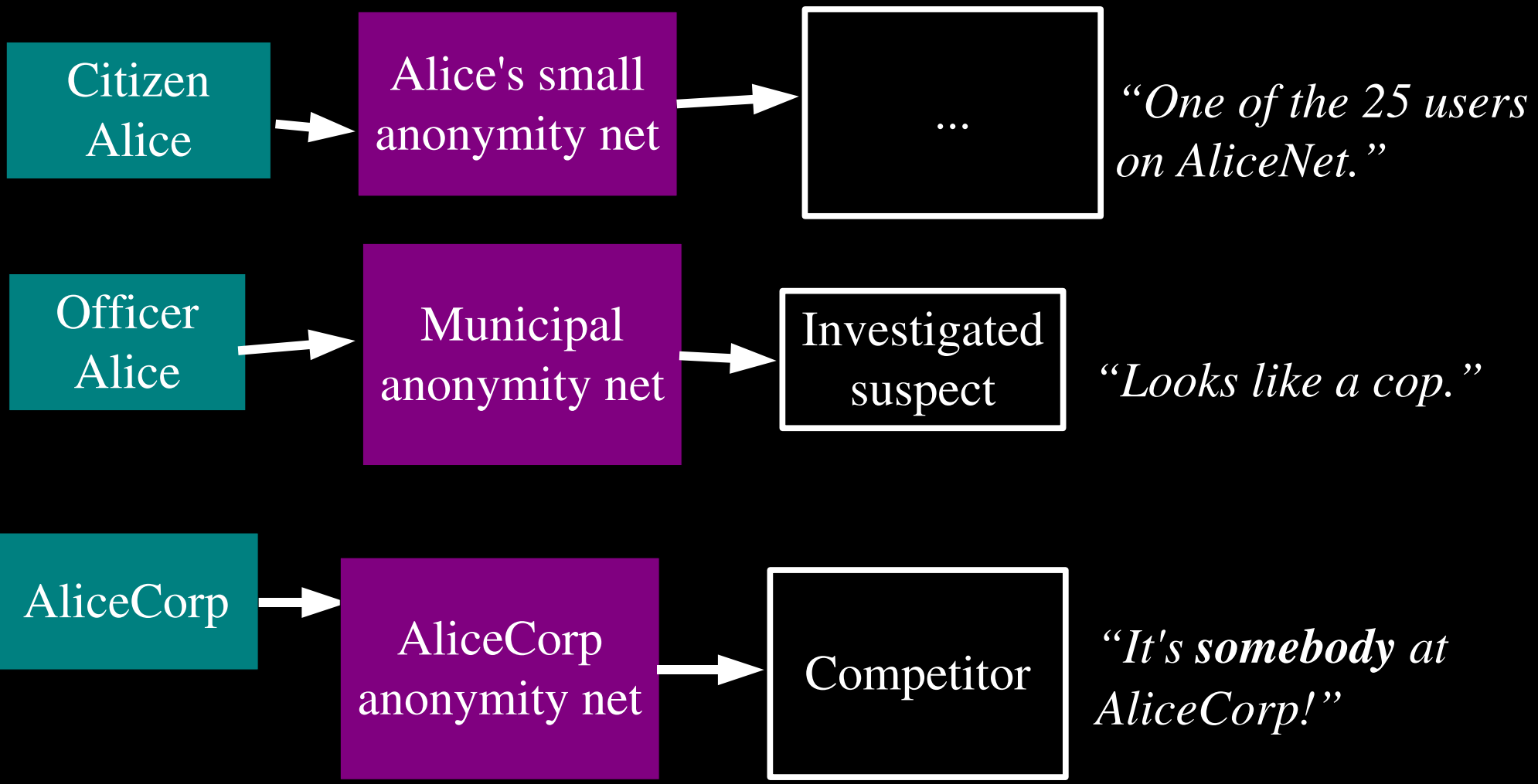
"Somebody in that hotel room just checked his Navy.mil mail!"

"*What* does *FBI Google for?*"

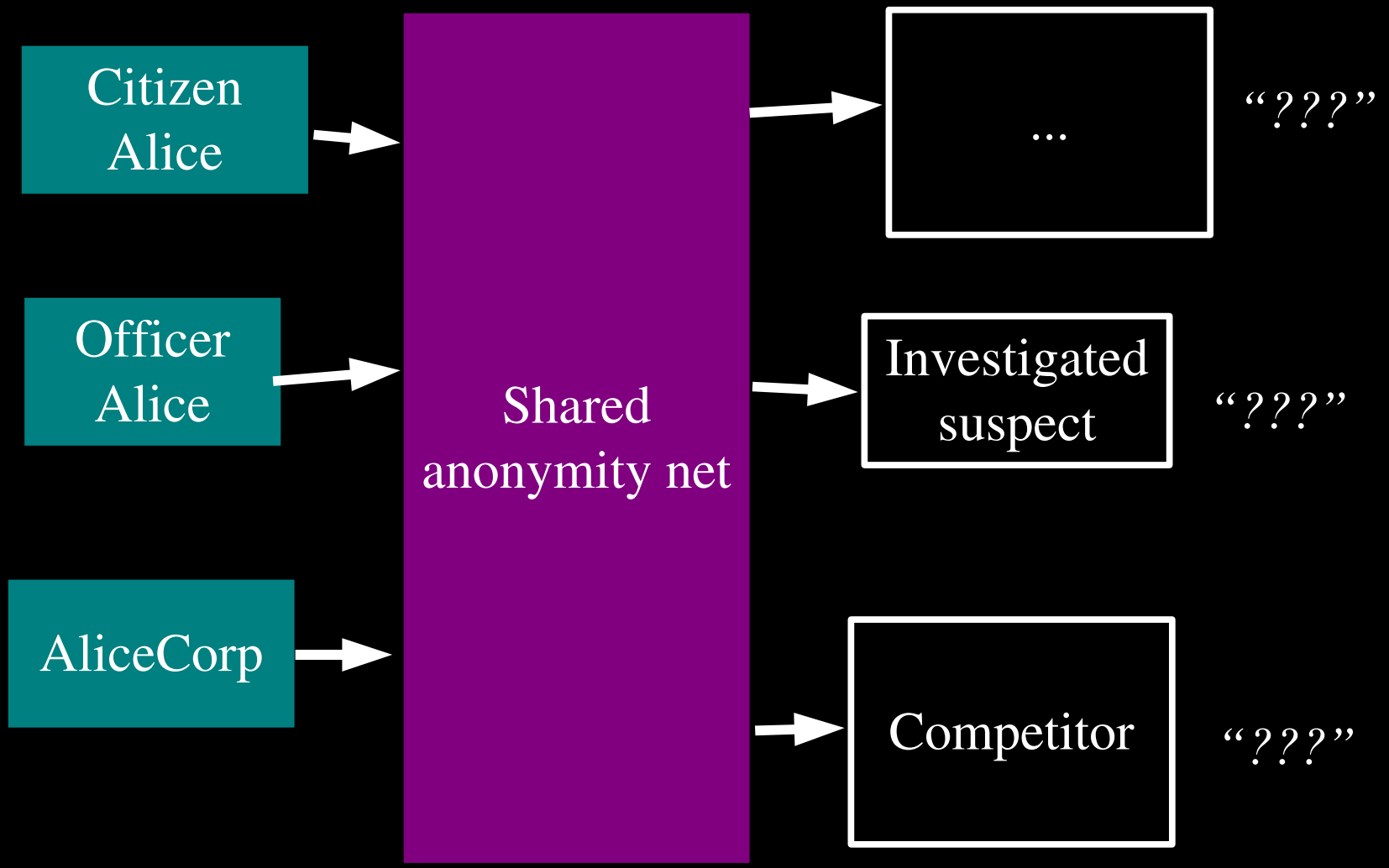
"Do I really want to reveal my internal network topology?"

"What about insiders?"

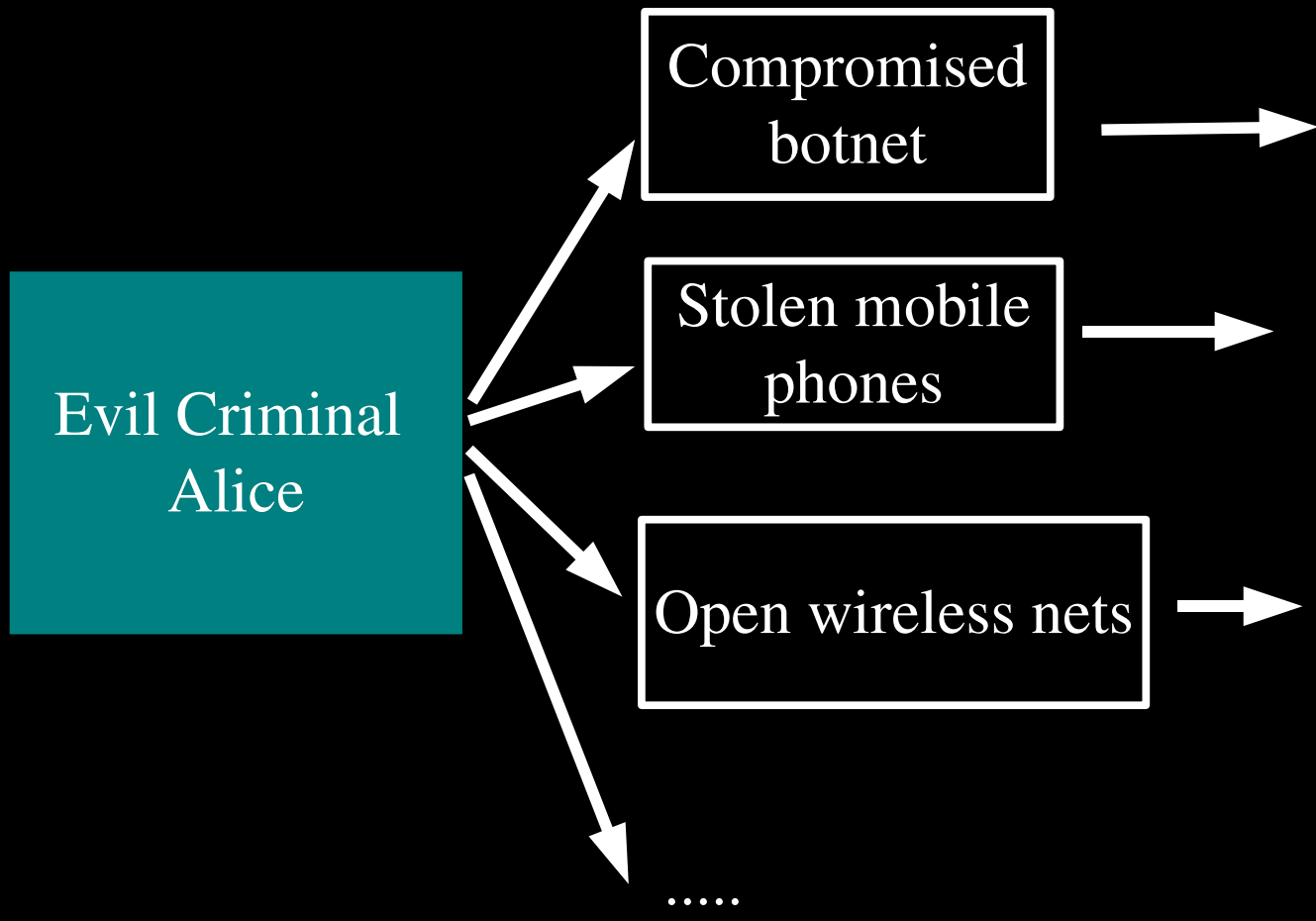
You can't get anonymity on your own: private solutions are ineffective...



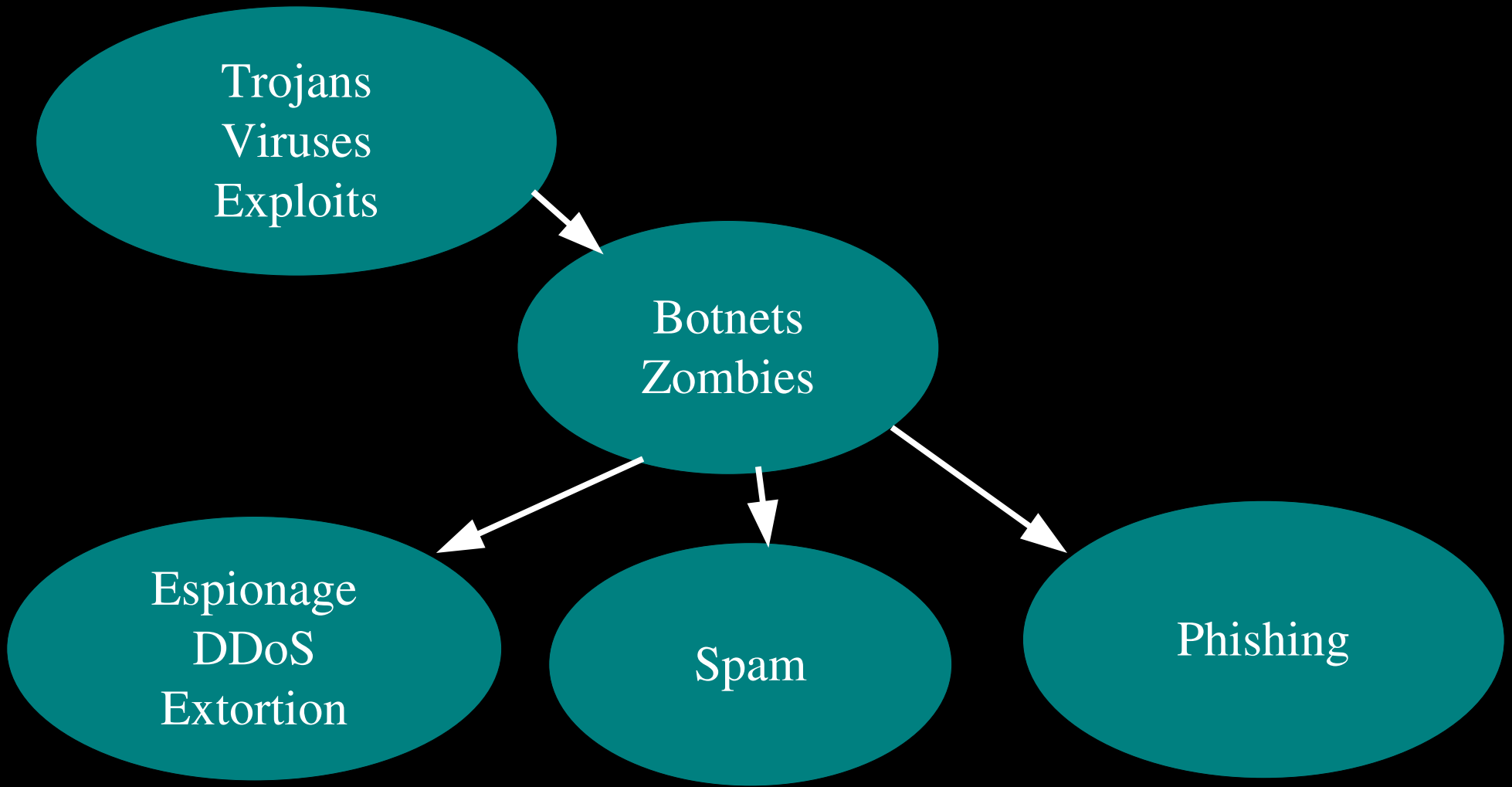
... so, anonymity loves company!



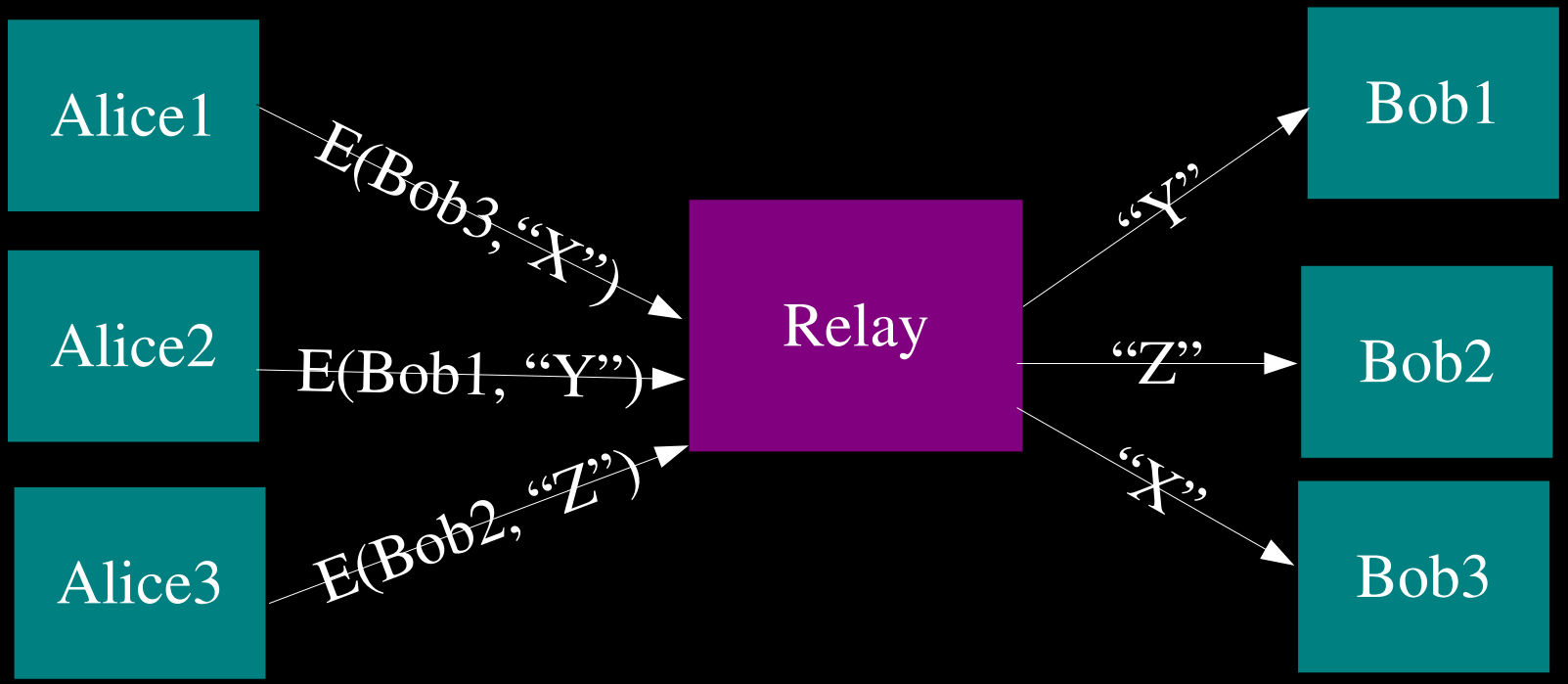
Yes, bad people need anonymity too. But they are *already* doing well.



Current situation: Bad people on the Internet are doing fine

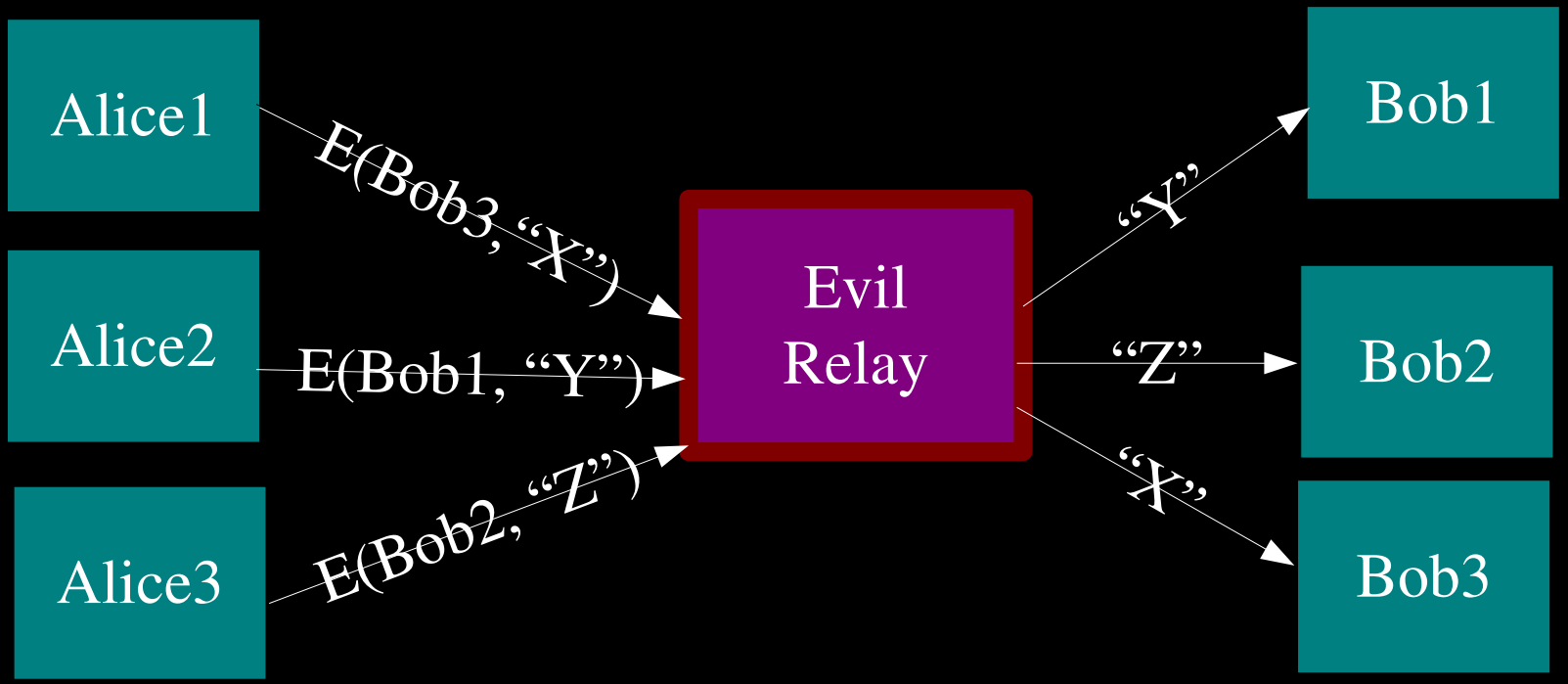


The simplest designs use a single relay to hide connections.

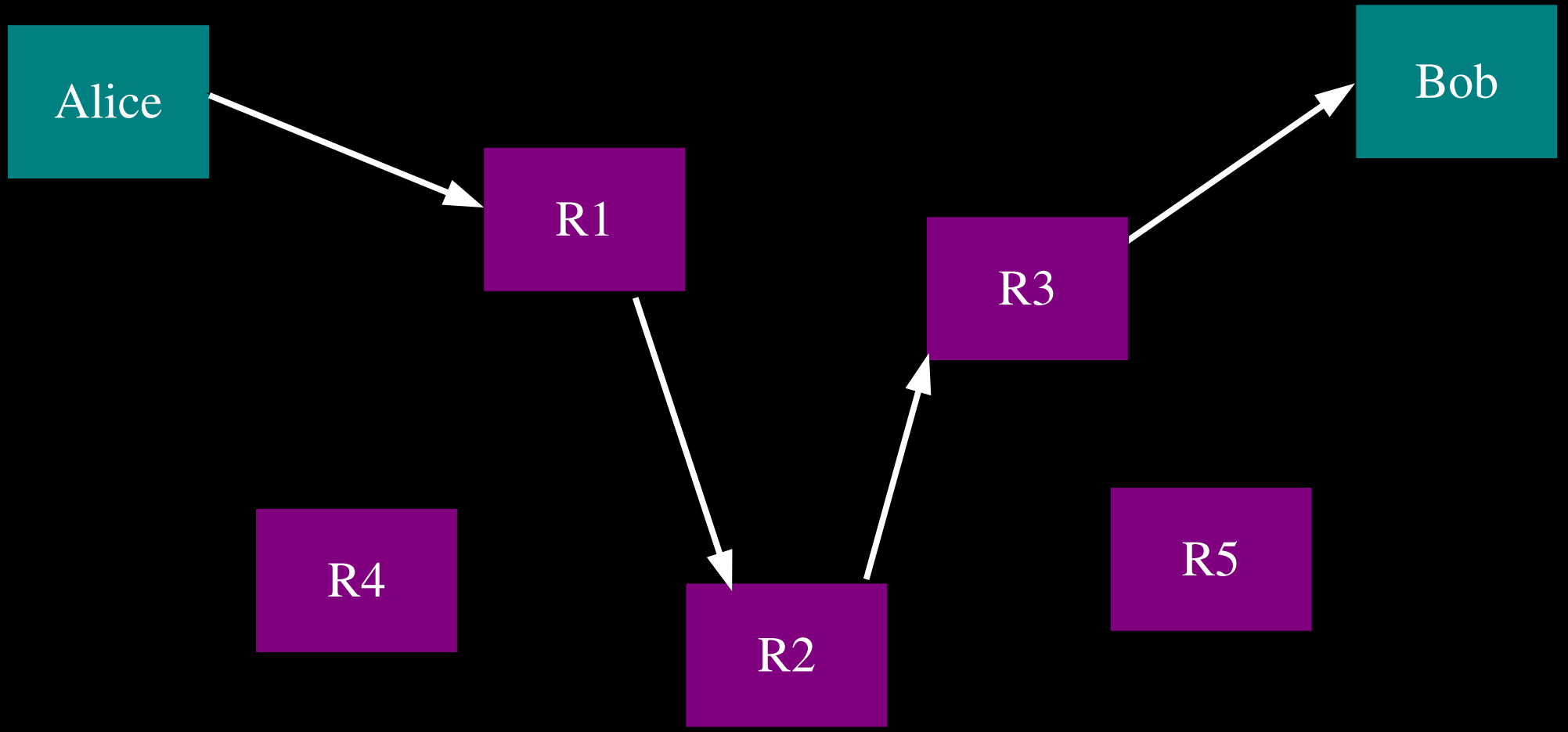


(example: some commercial proxy providers)

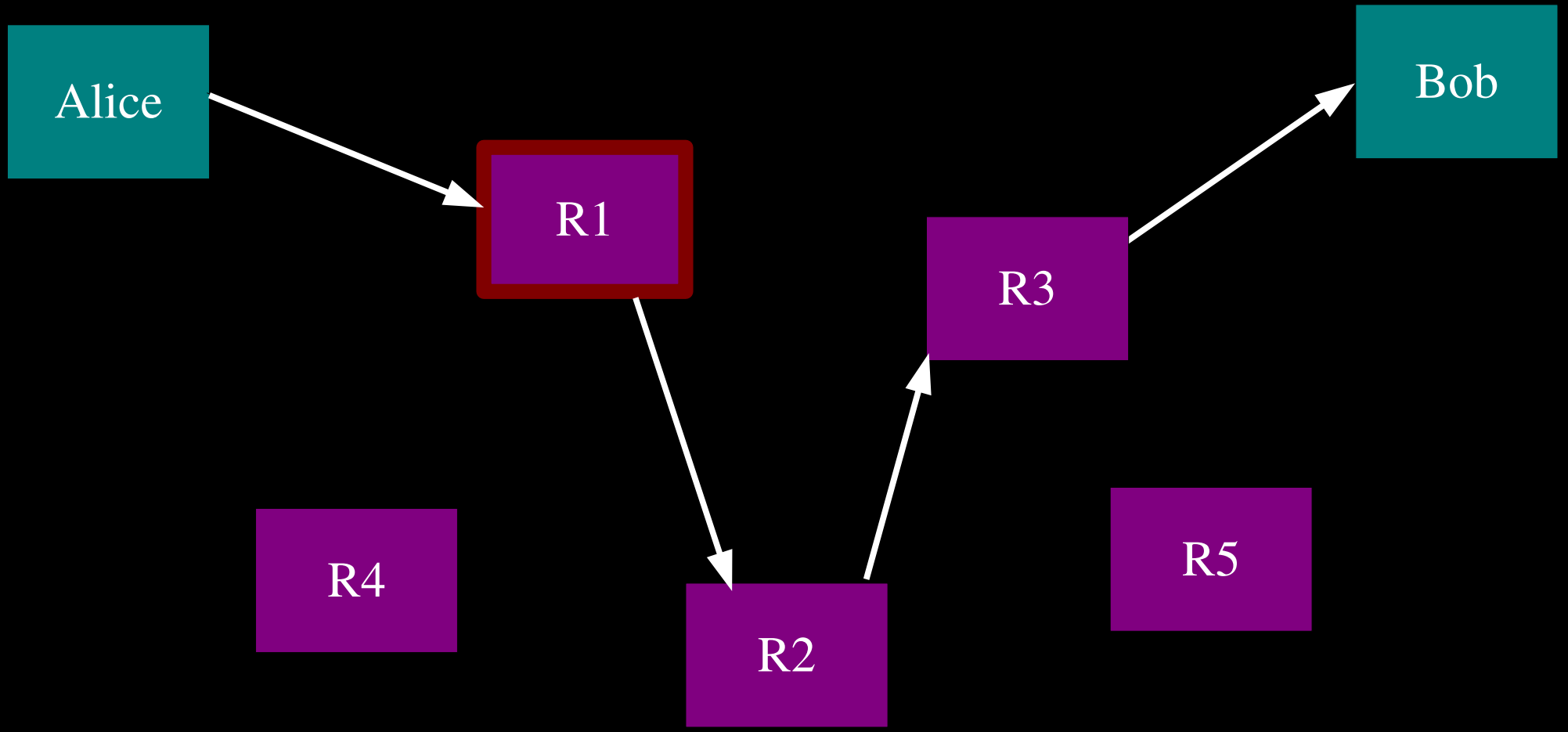
But a single relay (or eavesdropper!) is a single point of failure.



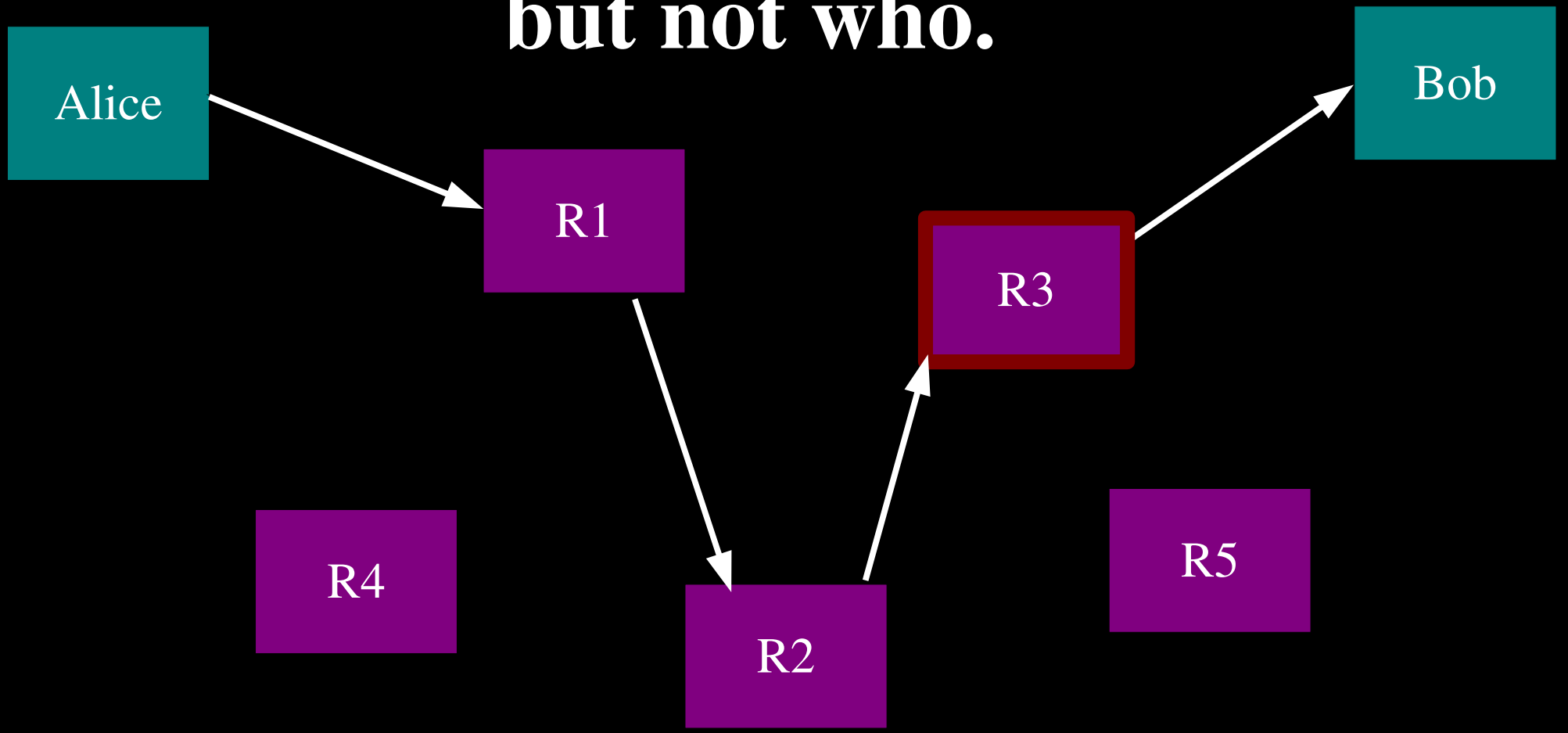
So, add multiple relays so that no single one can betray Alice.



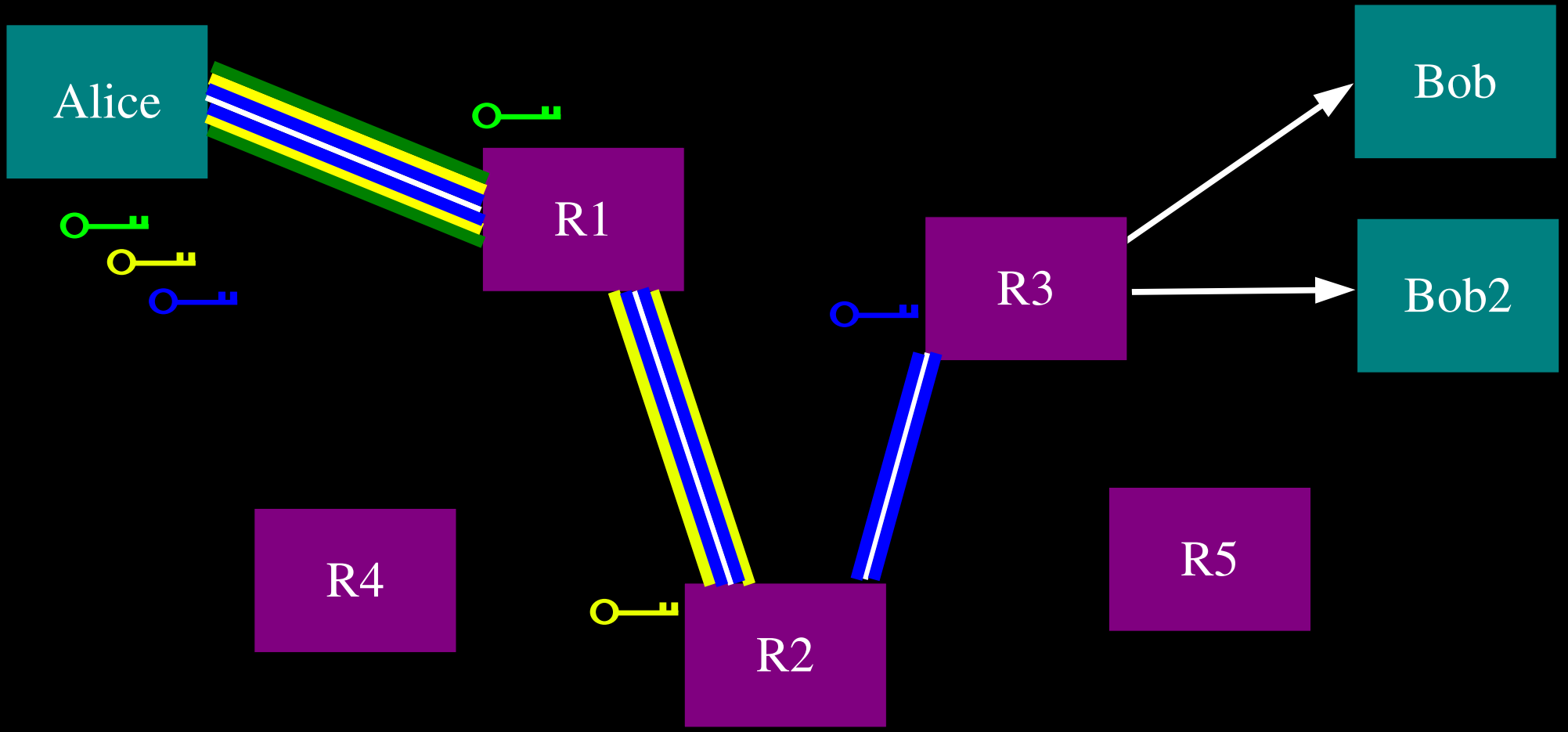
A corrupt first hop can tell that Alice is talking, but not to whom.



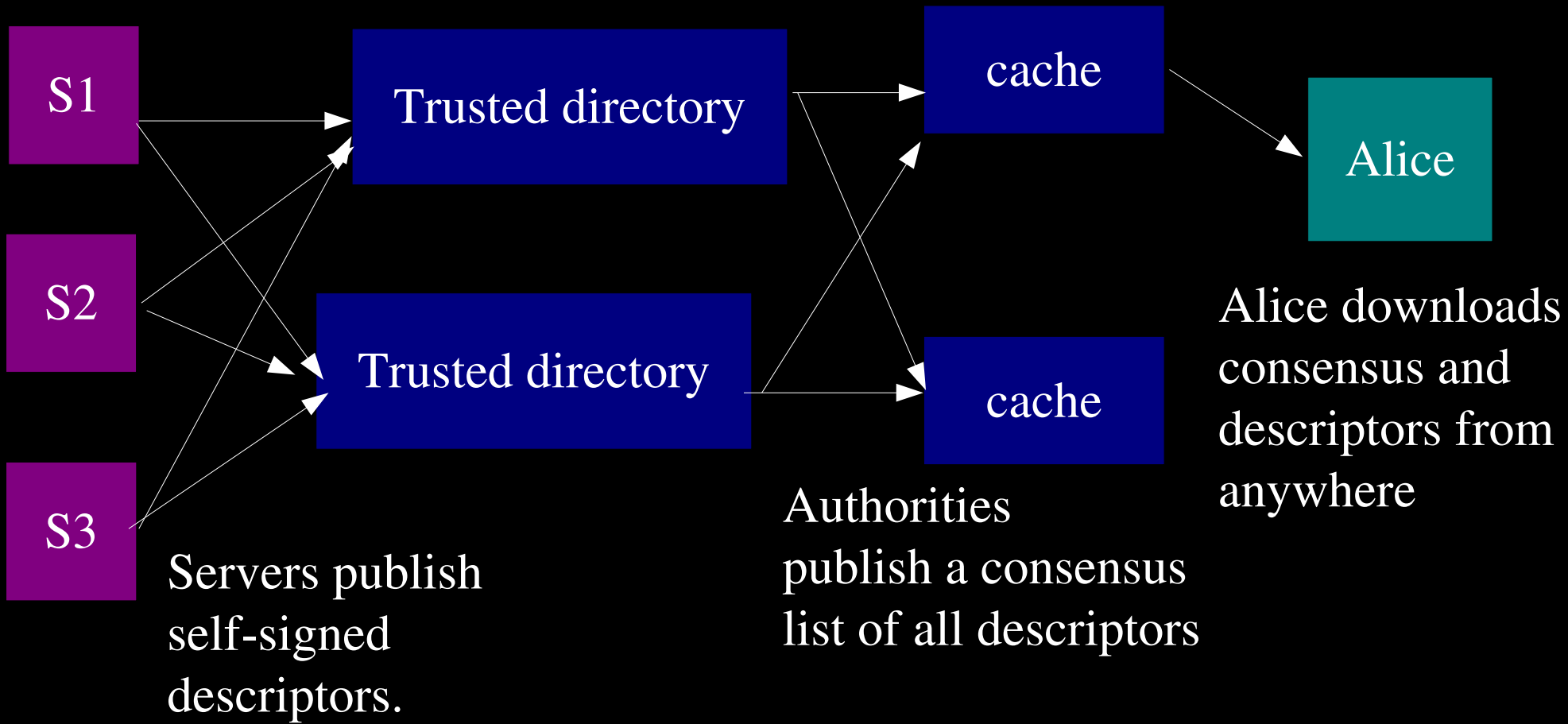
A corrupt final hop can tell that somebody is talking to Bob, but not who.



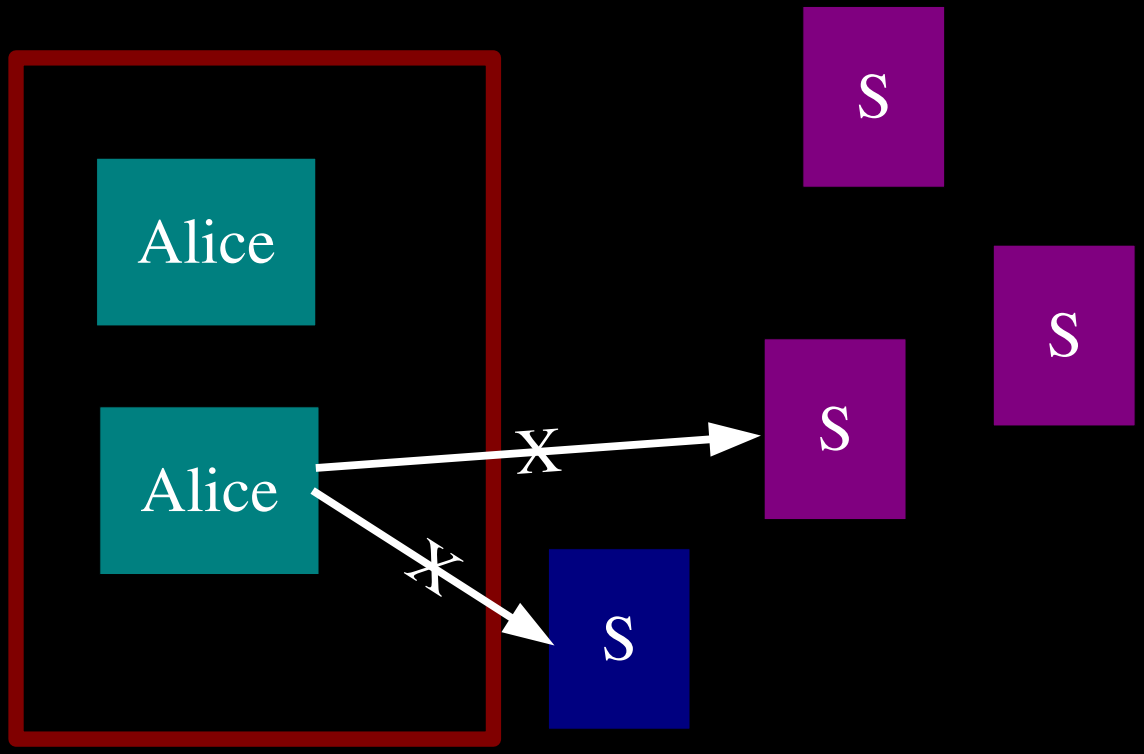
Alice makes a session key with R1 ...And then tunnels to R2...and to R3

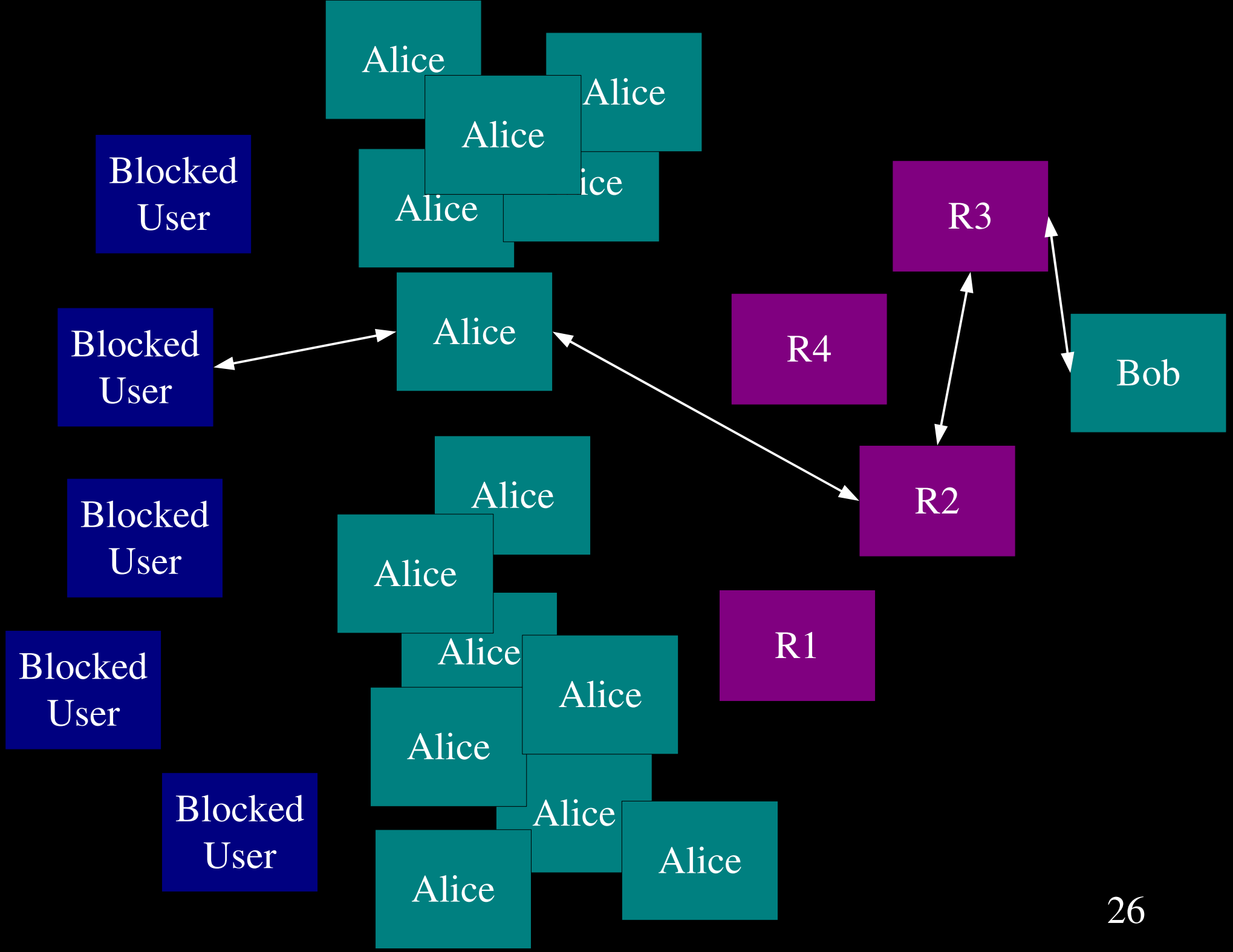


The basic Tor design uses a simple centralized directory protocol.



Governments and other firewalls can just block the whole Tor network.




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

The Tor client:

- One Tor binary for client and server
  - Just configure as you wish
  - By default, clients are just clients
  - Provides a local SOCKS4A interface
  - Can be used transparently

The Tor software ecosystem:

- Firefox/Torbutton
- Vidalia
- Privoxy/Polipo
- Tor Browser Bundle
- Gettor
- Tor DNSEL
- Tor weather

Torbutton

- Don't use Firefox and Tor without it!
- Protection against application layer attacks that hurt your anonymity
- Test for leaks with your setup vs Torbutton and HD's decloak.net
  - Social engineering attacks are nasty and difficult

Vidalia: A controller for Tor

- Used to control basic aspects of Tor as a client and/or server
- Allows for a view of the Tor network and a view of the current servers being used by your Tor
- Makes many common tasks effortless
- Cross platform (QT)

Privoxy or Polipo

- We're currently shipping one or the other, depending on platform
- Firefox and other programs may block on SOCKS connections, we use a caching HTTP proxy to speed things up

But that's... complex!

- Tor Browser Bundle
  - Download, extract to USB key, run
  - Leaves very little behind
  - Currently Windows only
    - Porting to Linux/Mac OS X

But I'm unable to access the Tor website...

- Gettor
  - Send an email to gettor@torproject.org and ask for help
  - We've automated handing this out for users with DKIM signed email
  - Working for blocked users

But I'm unable to access the Tor network...

- Bridges are our current solution
- Tor's Darknet
  - We want to circumvent blocking
  - Exiting is different (Tor DNSEL)
- Get bridges:
  - https://bridges.torproject.org
  - bridges@torproject.org

I run a website and I want to make Tor users jump through extra hoops...

- Tor DNSEL
  - Written by an anonymous author
    - In Haskell
  - Query it about your user, we'll tell you if Tor would allow that kind of traffic from the Tor network
  - This drives https://check.torproject.org

I'd like to become a Tor server:

- One Tor binary for client and server
- Servers require at least a single port for their ORPort
- Servers must be able to reach all other servers – all circuits are multiplexed
- Most things are configurable
  - Relay bandwidth, exit policy, etc

We're looking for a few new nodes

- We want to grow the Tor network
- You're part of the community that can help
- It's easy
- By running a relay, you increase the diversity and thus the security of the network, even if we don't know you

We're looking for a few new nodes

- Germany is home to the largest number of relays in Europe
- Currently Poland has a few Tor servers
  - Why is that?
  - Can you help?

But what about abuse?

- Abuse is real but infrequent
  - It's not a concern for my nodes
- Some abuse is interestingly political
  - If your node is used to upload a human rights violation, does that even upset you? Is that perhaps what drives you to run a node in the first place?

How about the speed of the network?

- Perceived speed is a funny thing
  - It can be latent or very fast
  - The speed of light is a factor
    - Where's your circuit going?
  - (Ab)users are the real issues
    - Many overloaded relays
- We're working on it (Please see our performance road map)

To give you an idea of who's using Tor with three examples:

- Bloggers and Journalists
  - Protection against revealing their location
- UN Aid workers
  - Protection against all kinds of monitoring
- Police
  - They need to hide that they're cops

Who else?

- We don't really know who uses Tor unless they tell us
  - It's an anonymity network!
- We hear from people on all sides of the spectrum
  - Most of them ask us not to quote them
- Some support Tor by running relays

We'll help you setup a relay

- The Tor Project doesn't run relays
- We're more than happy to help you run a relay
- The network grows with passionate people, sharing is caring
- It can be as easy as checking a box
  - It can be as hard as editing a text file :-)

We're looking for a few good hackers...

- Do you program in C or in Python?
- Do you care about freedom of expression?
- Do you want to help impact the lives of hundreds of thousands of users?
- If so...
  - Join us in developing Tor!

Questions?

- Ask them now or contact us
- IRC
  - irc.oftc.net in #tor and #tor-dev
- Feel free to email us:
  - tor-assistants@torproject.org
- Feel free to email me:
  - jacob@appelbaum.net