Online Anonymity

Andrew Lewman
The Tor Project

Outline

- Why anonymity?
- Crash course on Tor
- Future

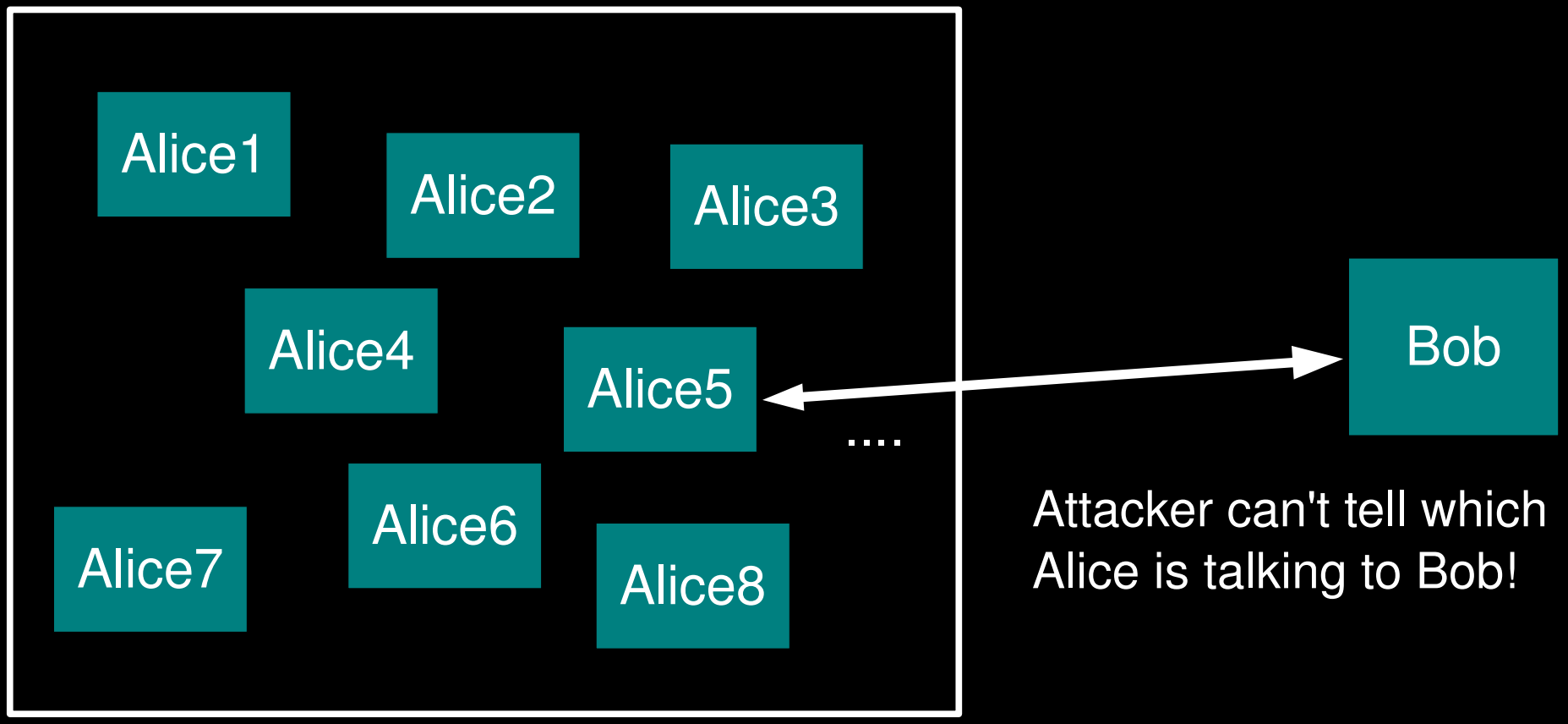
Informally: anonymity means you can't tell who did what

“Who wrote this blog post?”

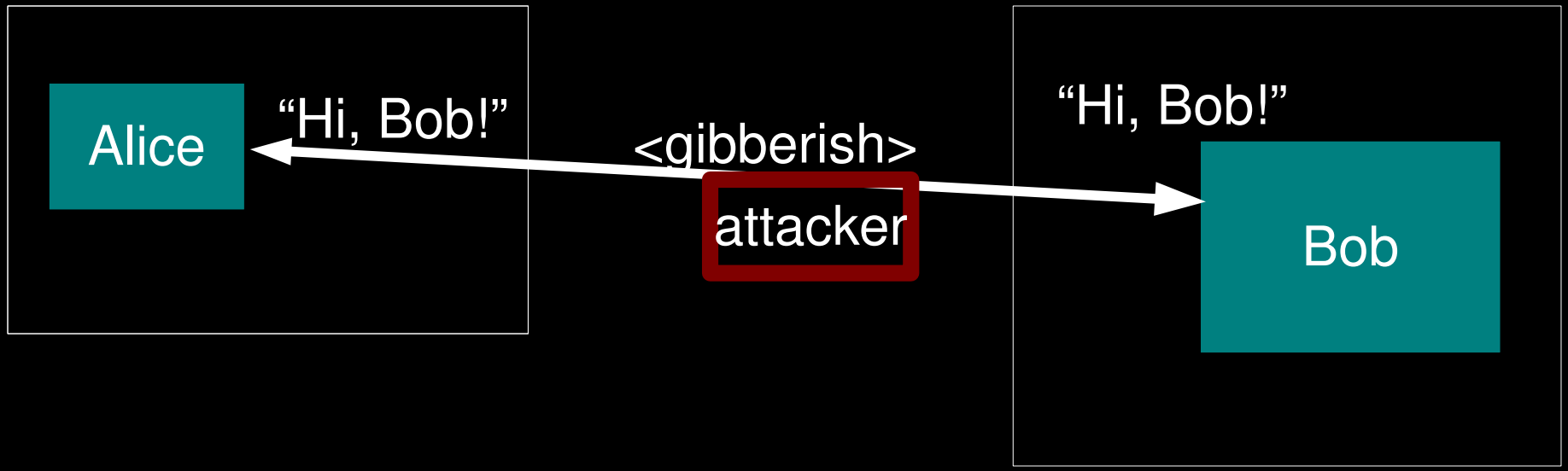
“Who's been viewing my webpages?”

“Who's been emailing patent attorneys?”

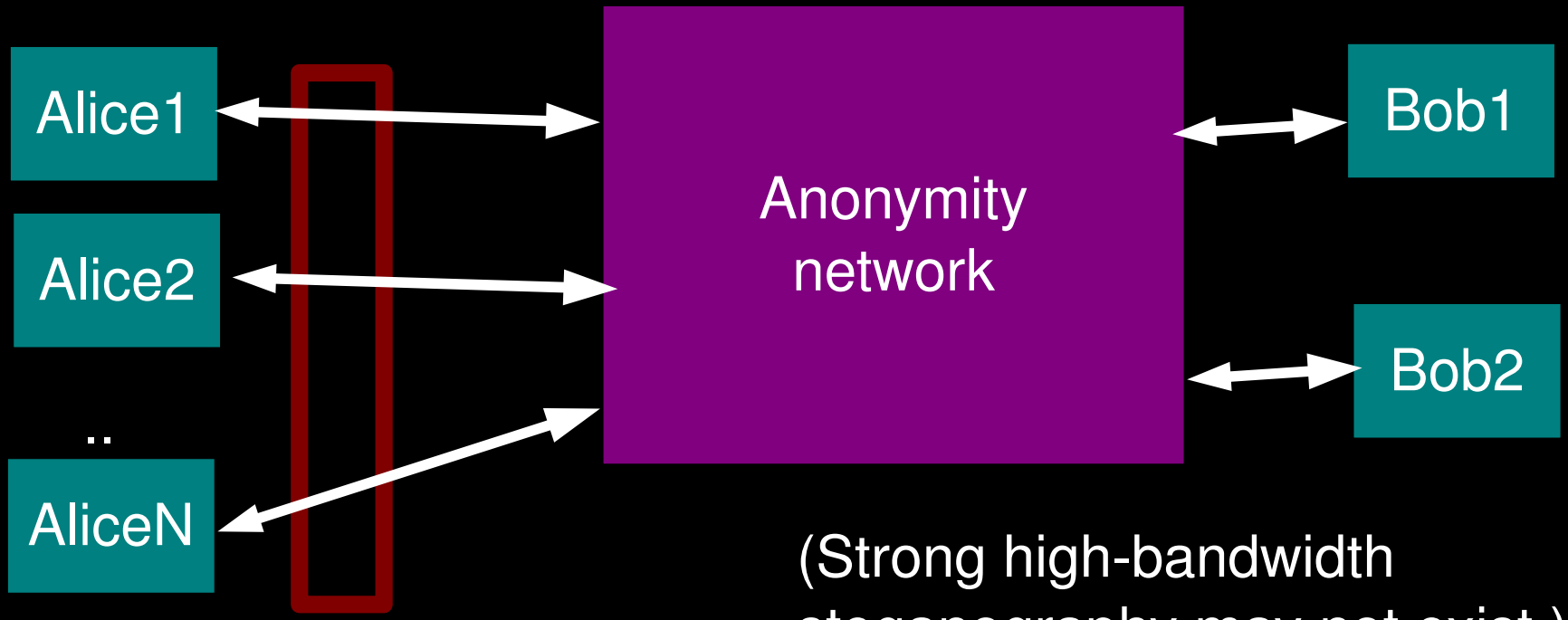
Formally: anonymity means indistinguishability within an "anonymity set"



Anonymity isn't cryptography: Cryptography just protects contents.



Anonymity isn't steganography:
Attacker can tell that Alice is talking; just not to whom.



(Strong high-bandwidth steganography may not exist.)

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?”

...since “weak” anonymity... isn't.

~~“You can't prove it was me!”~~

*Proof is a **very** strong word.*
With statistics,
suspicion becomes certainty.

Will others parties have
the ability and incentives
to keep their promises?

~~Promise you won't look!”~~

~~“Promise you won't remember!”~~

~~“Promise you won't tell!”~~

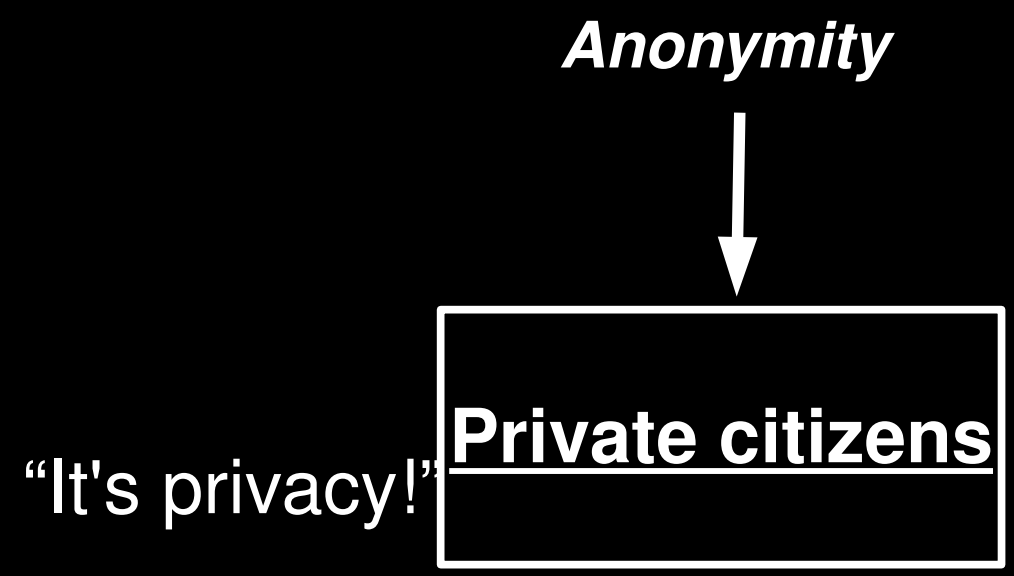
~~“I didn't write my name on it!”~~

Not what we're talking about.

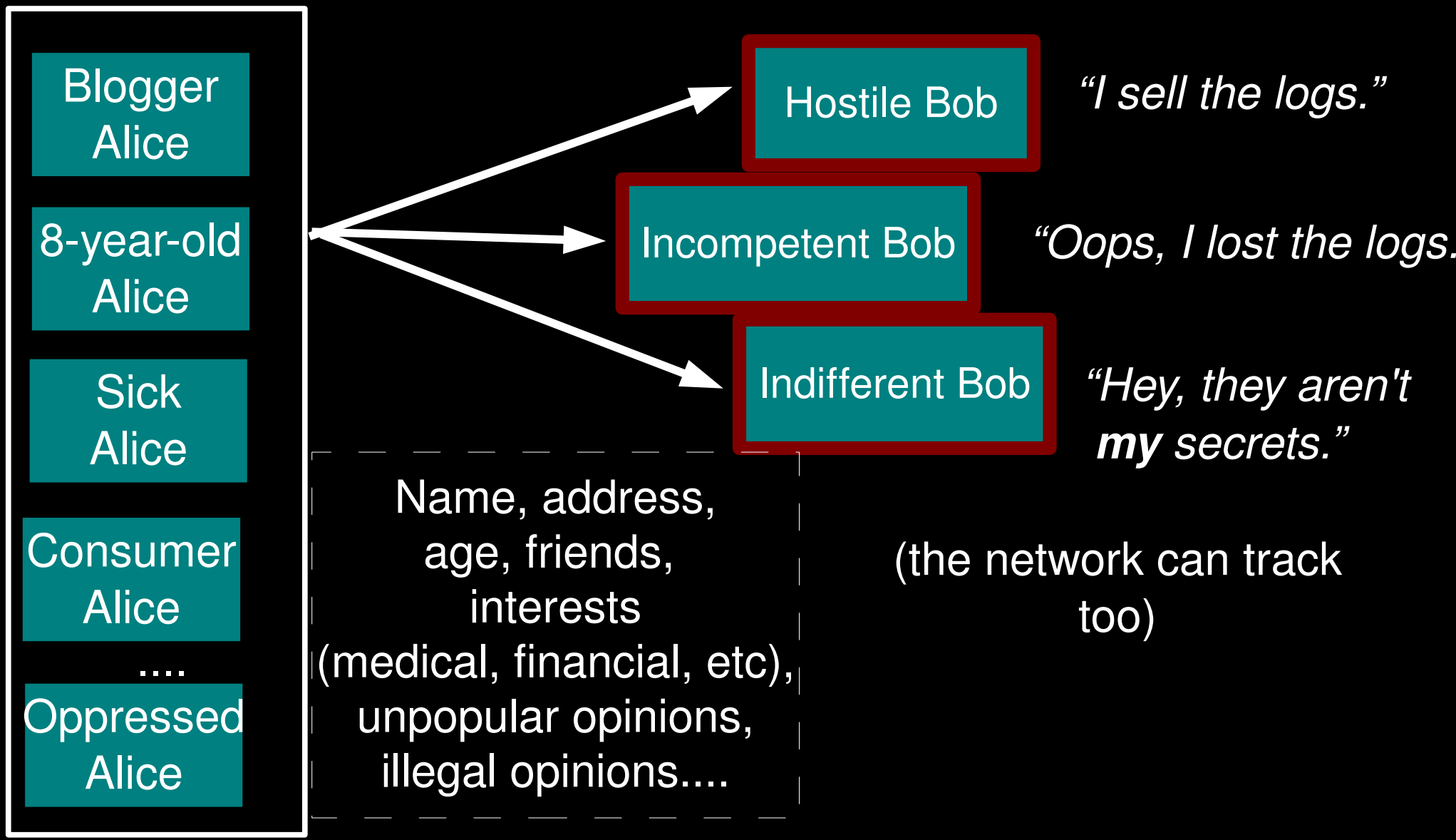
Nope!
(More info
later.)

~~“Isn't the Internet already anonymous?”~~

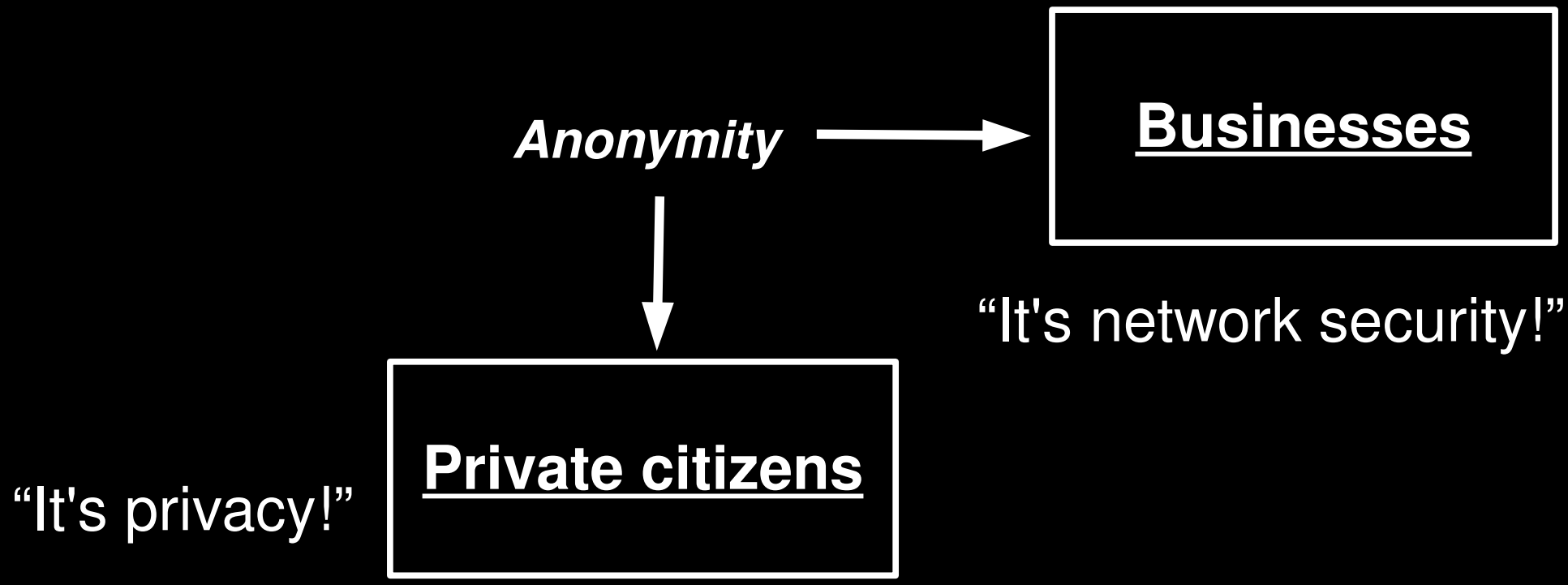
Anonymity serves different interests for different user groups.



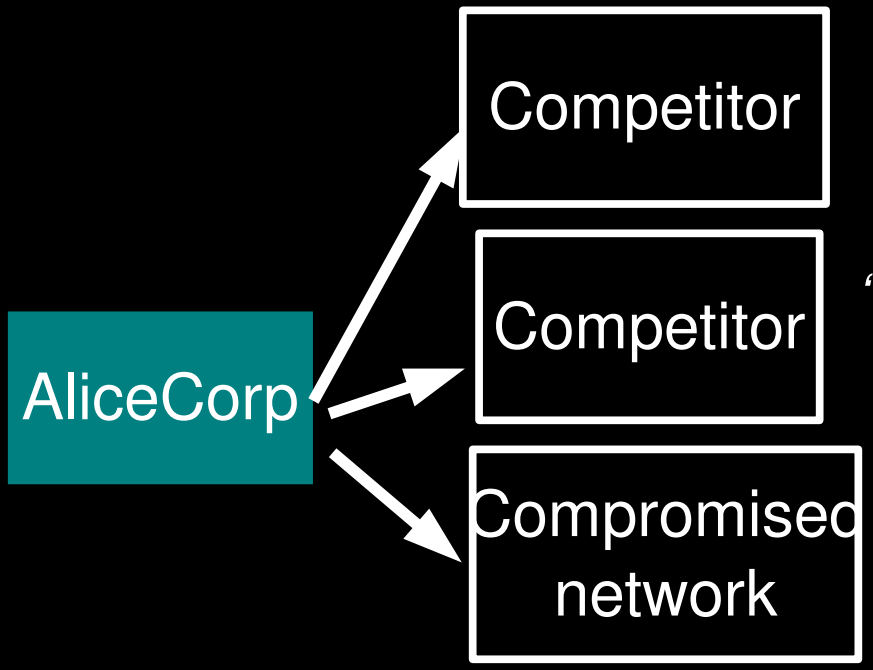
Regular citizens don't want to be watched and tracked.



Anonymity serves different interests for different user groups.



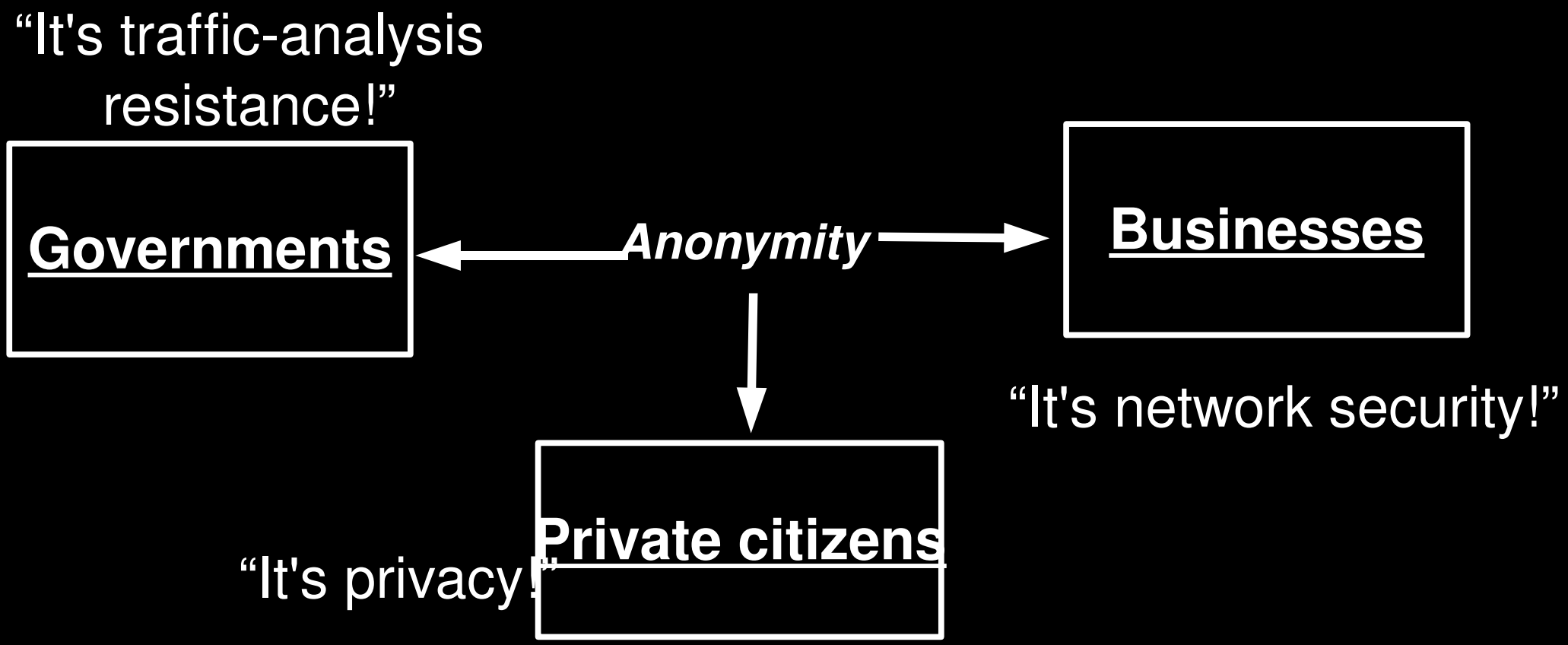
Businesses need to keep trade secrets.



“Oh, your employees are reading our patents/jobs page/product sheets?”
“Hey, it's Alice! Give her the 'Alice' version!”

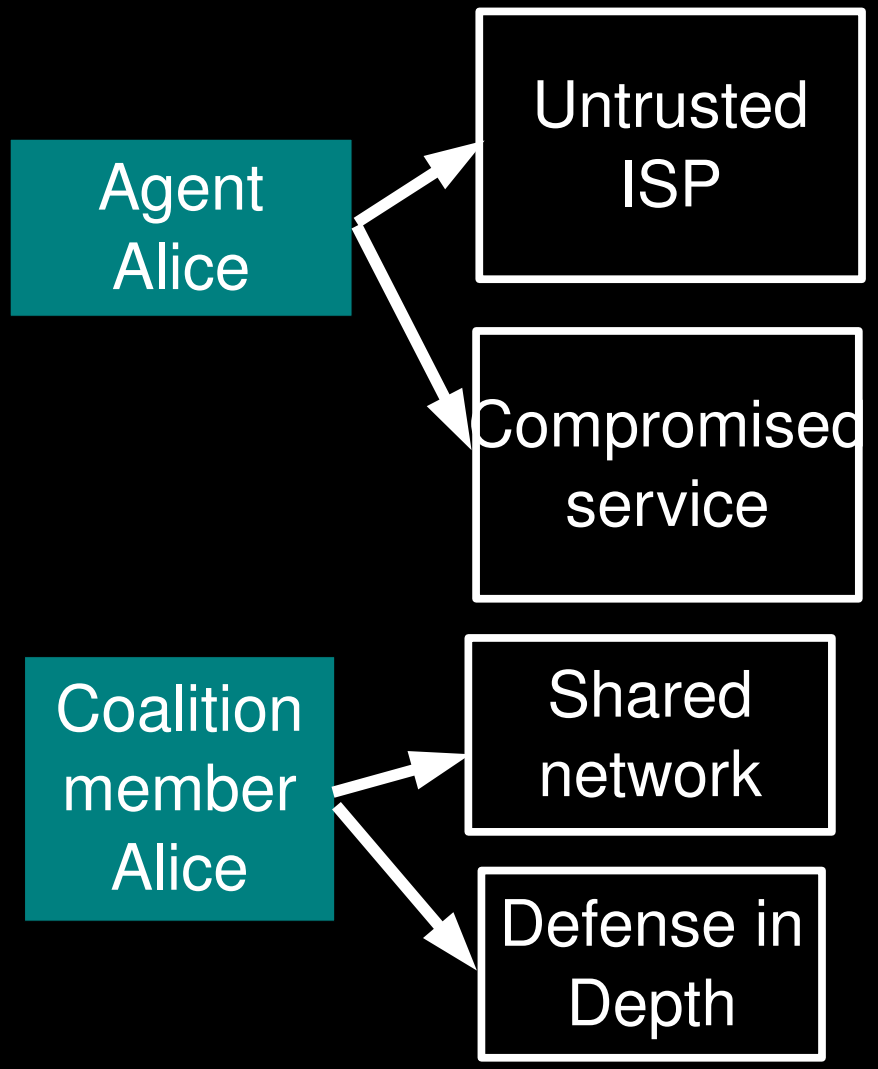
“Wanna buy a list of Alice's suppliers? What about her customers? What about her engineering department's favorite search terms?”

Anonymity serves different interests for different user groups.



Law enforcement needs anonymity to get the job done.

Governments need anonymity for their security



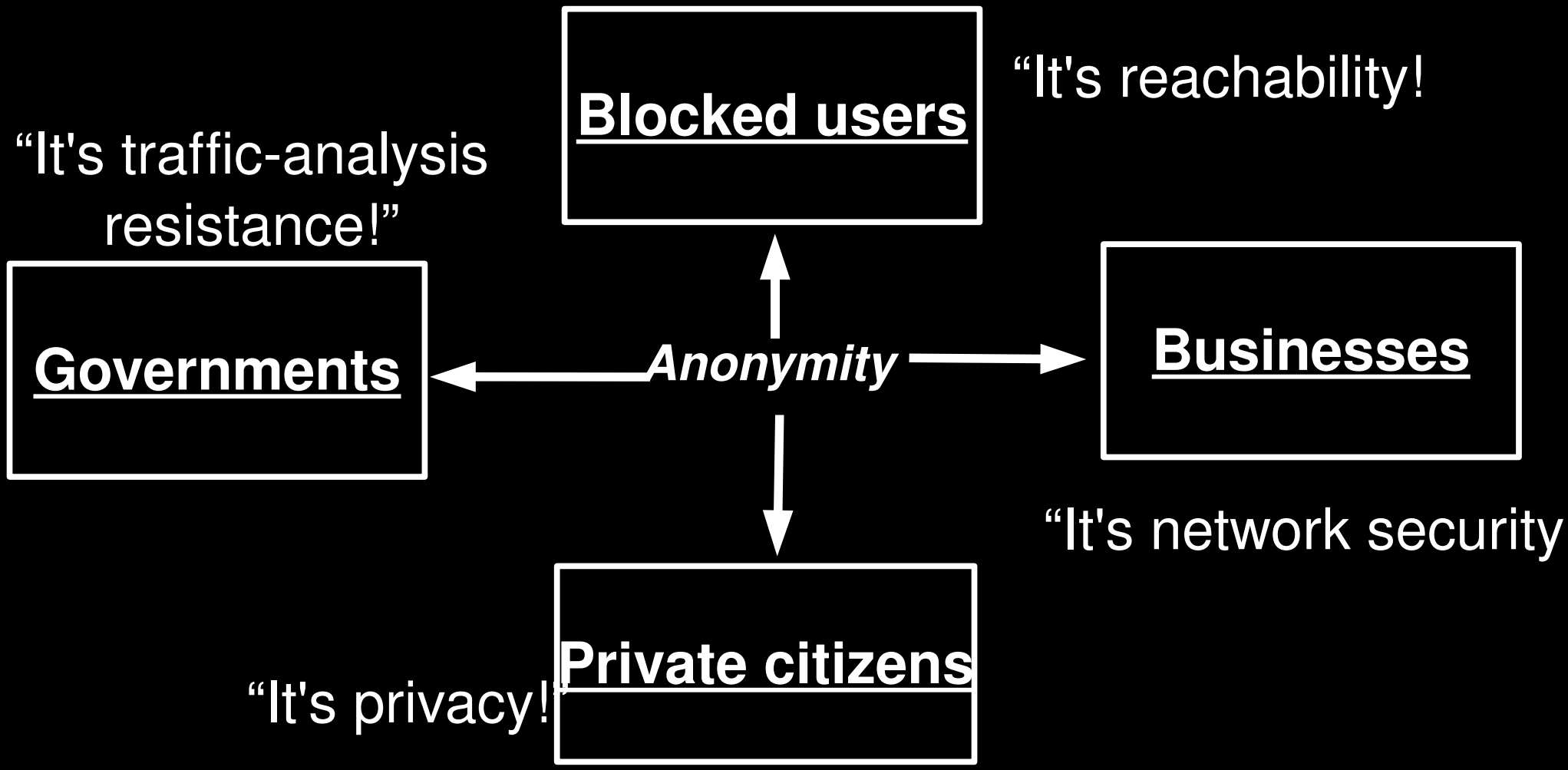
"What will you bid for a list of Baghdad IP addresses that get email from .gov?

"*What* does *the CIA Google for?*"

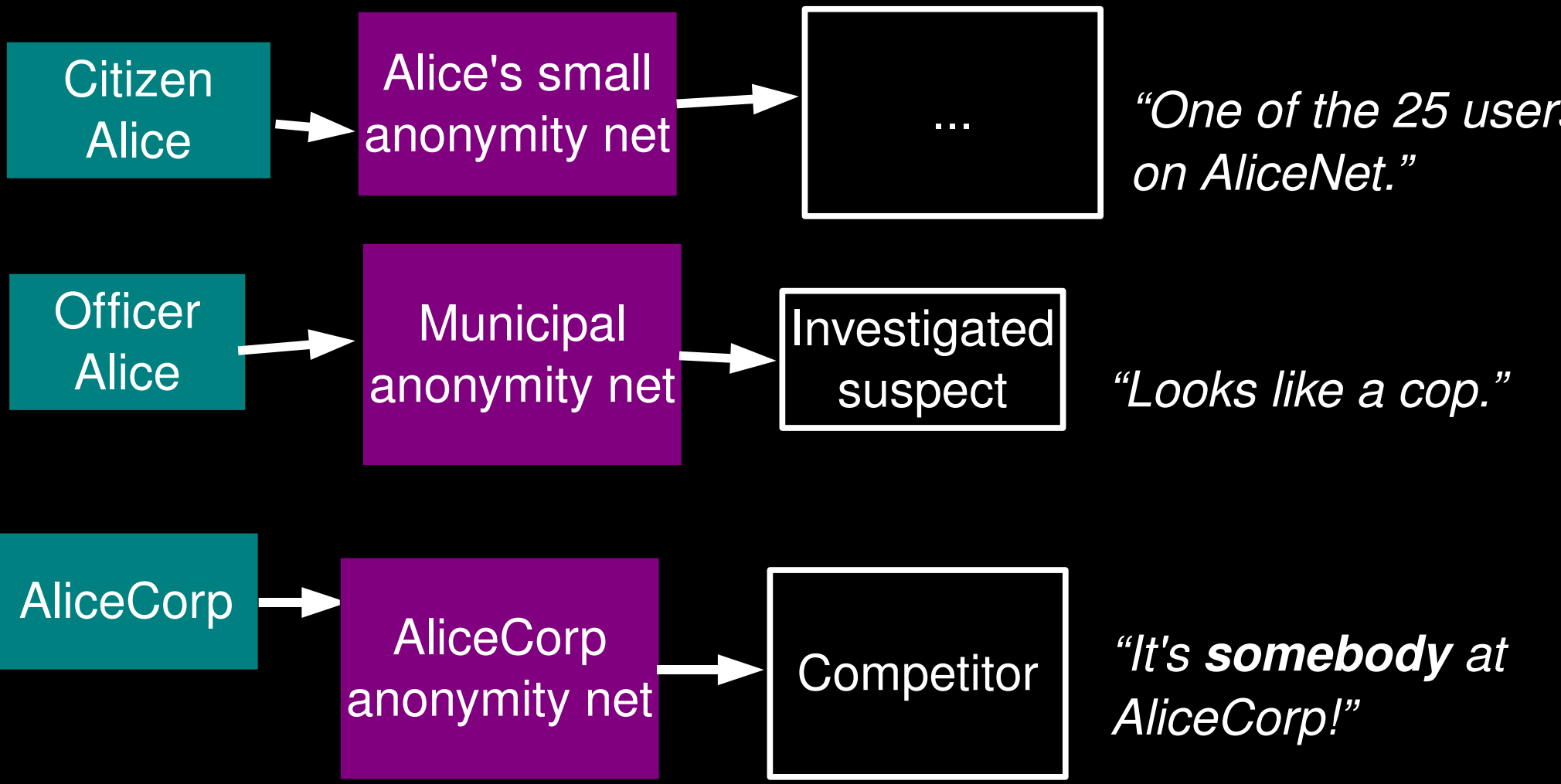
"Do I really want to reveal my internal network topology?"

"What about insiders?"

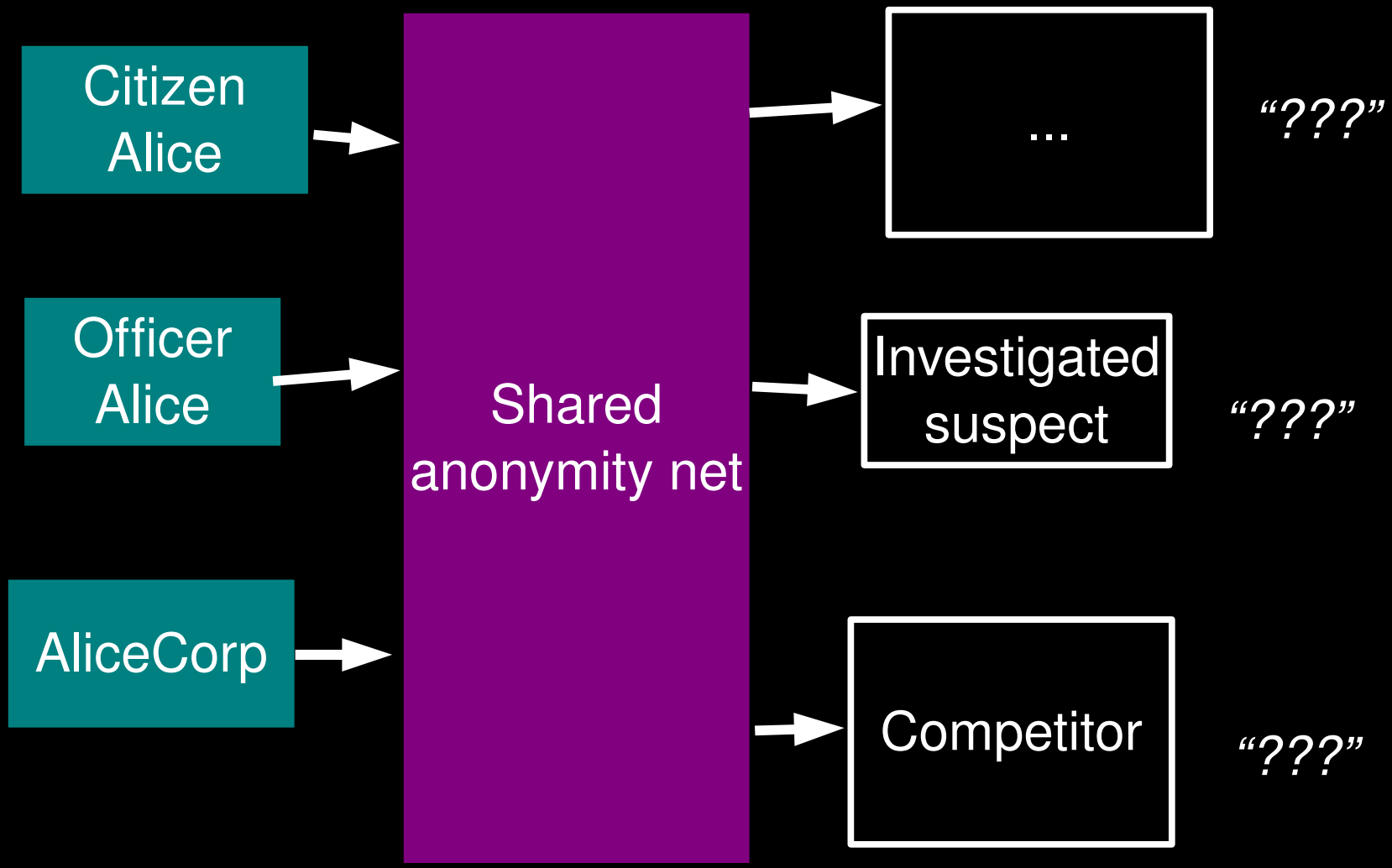
Anonymity serves different interests for different user groups.



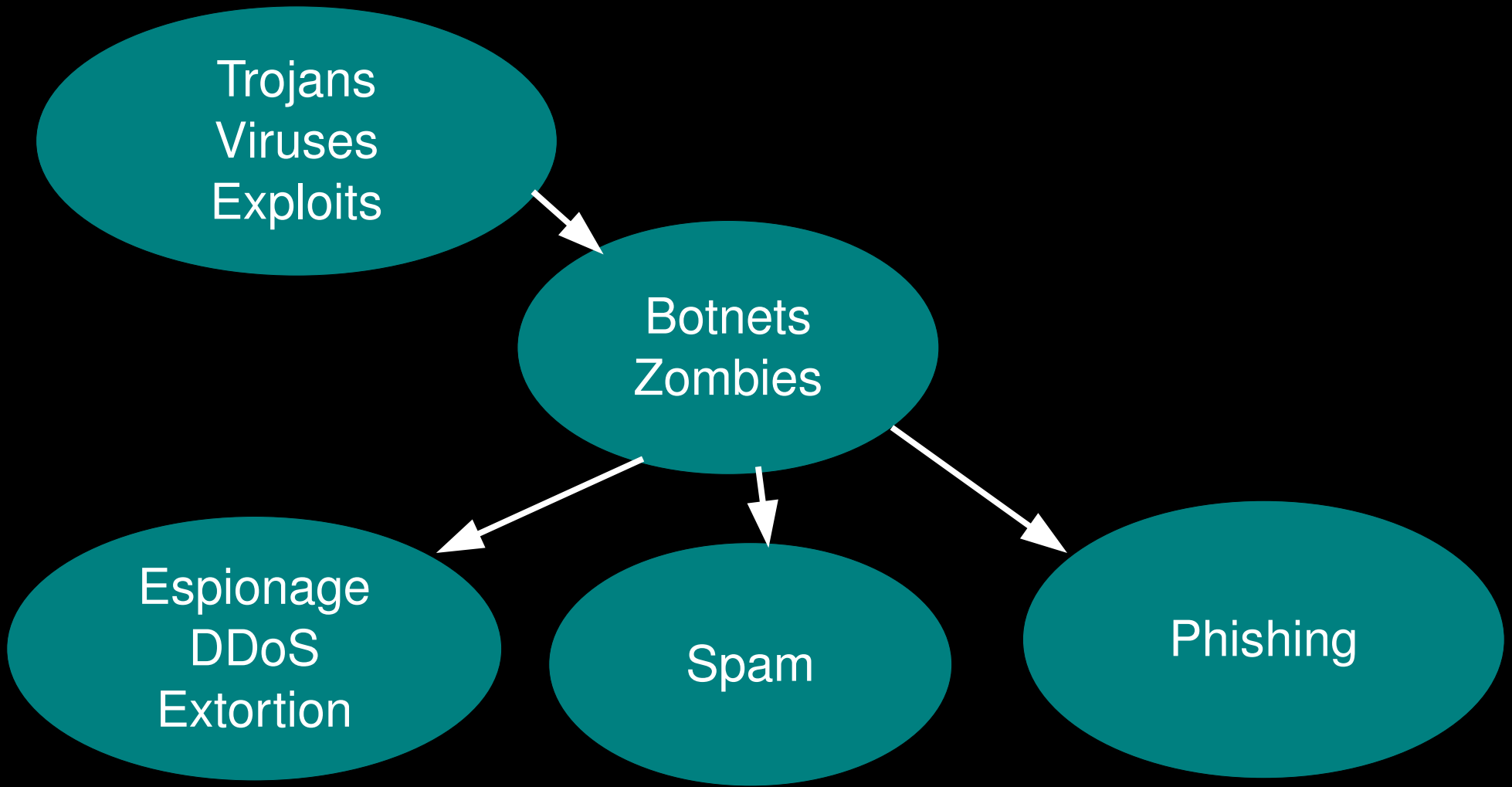
You can't get anonymity on your own: private solutions are ineffective...



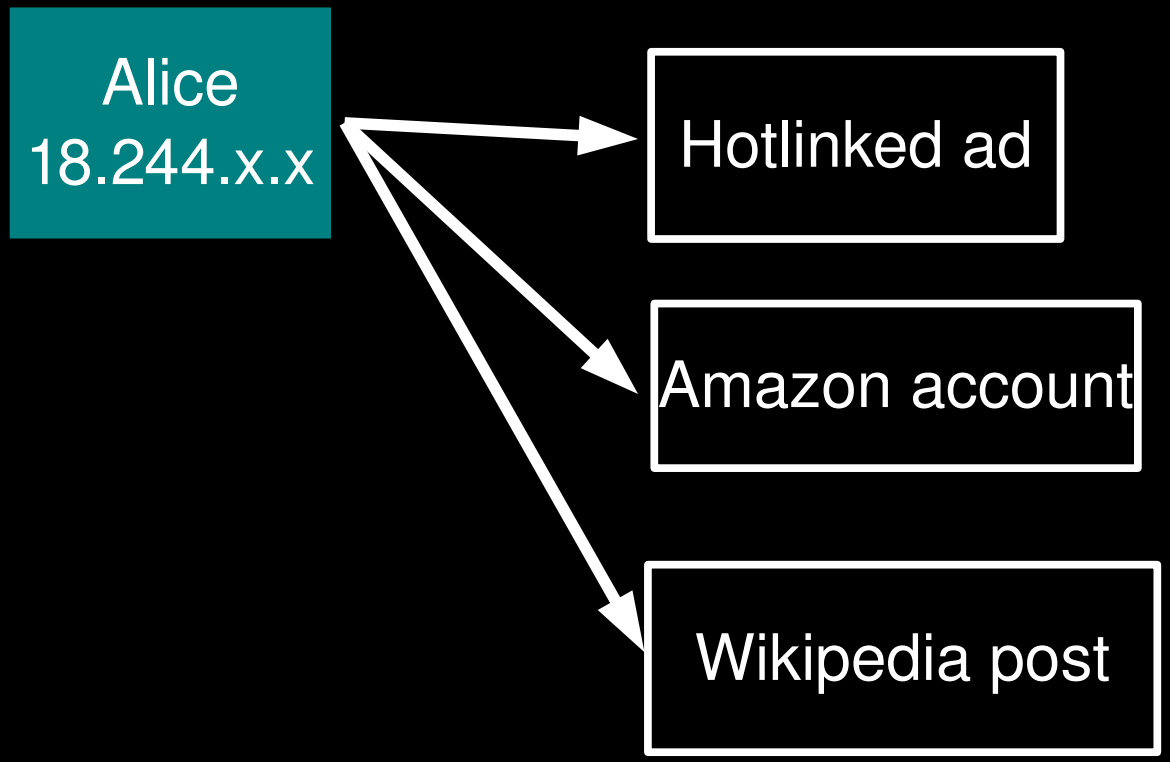
... so, anonymity loves company!



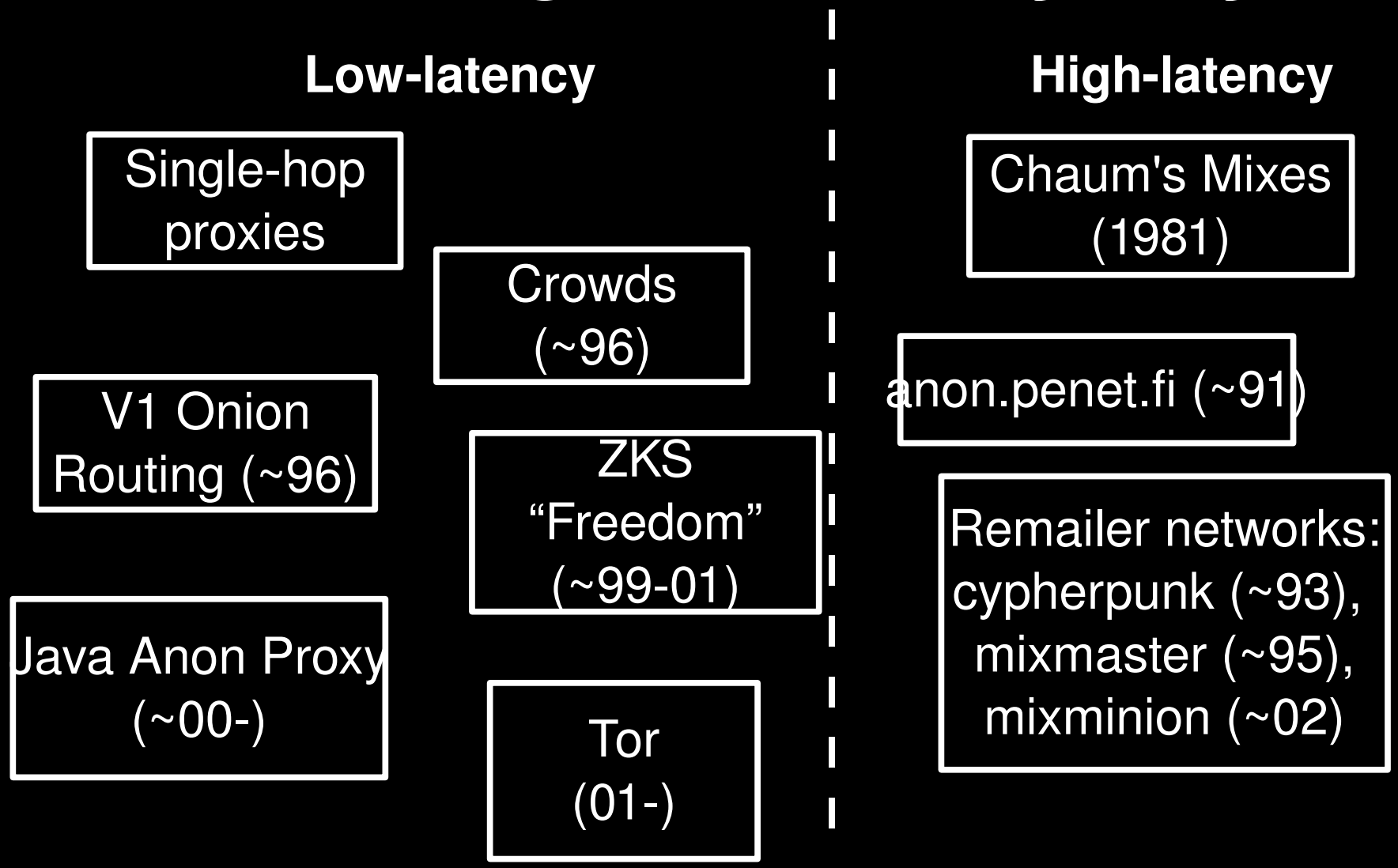
Current situation: Bad people on the Internet are doing fine



IP addresses can be enough to bootstrap knowledge of identity.



Tor is not the first or only design for anonymity.



...and more!

Outline

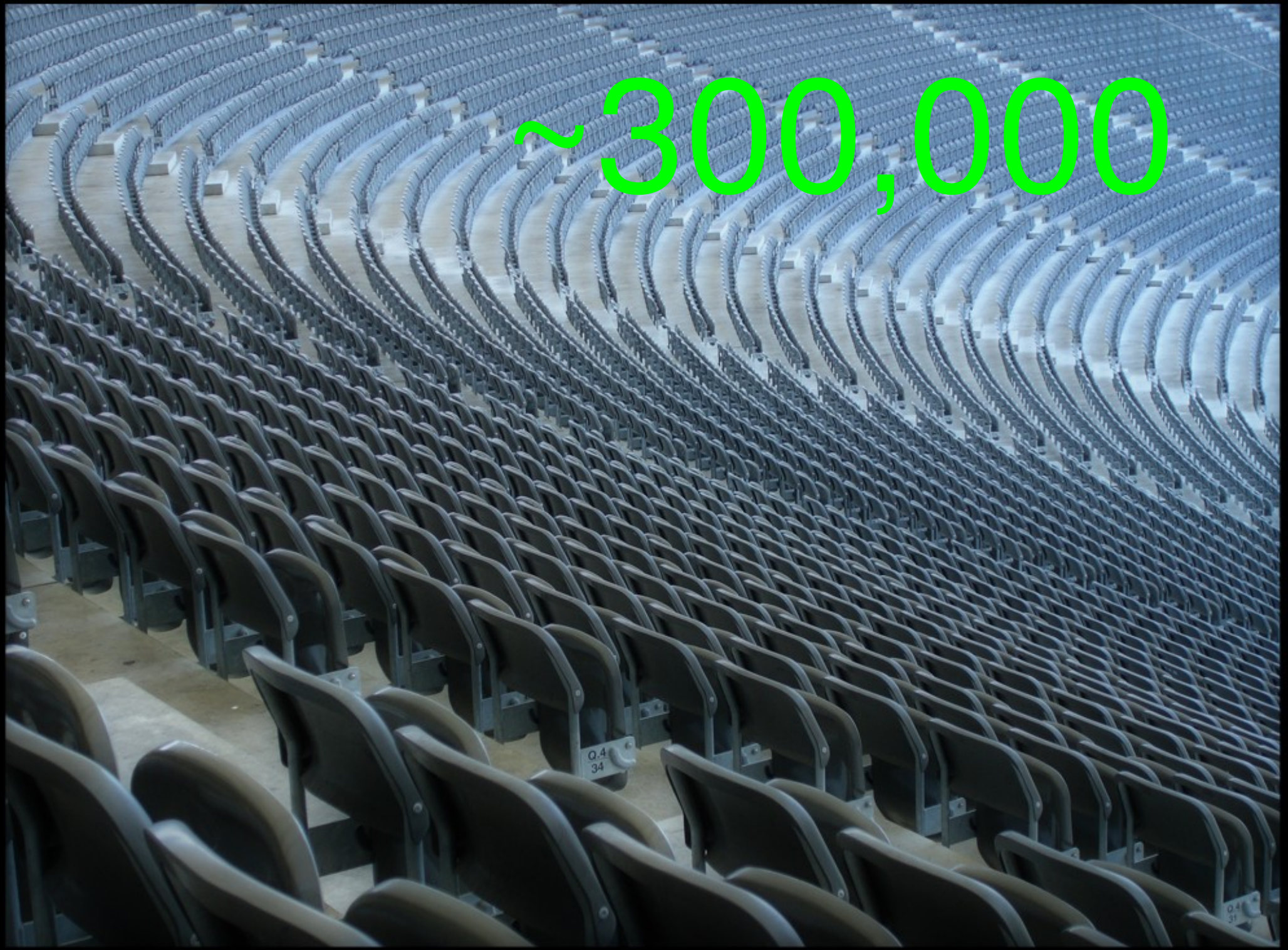
- Why anonymity?
- *Crash course on Tor*
- Future

What is Tor?

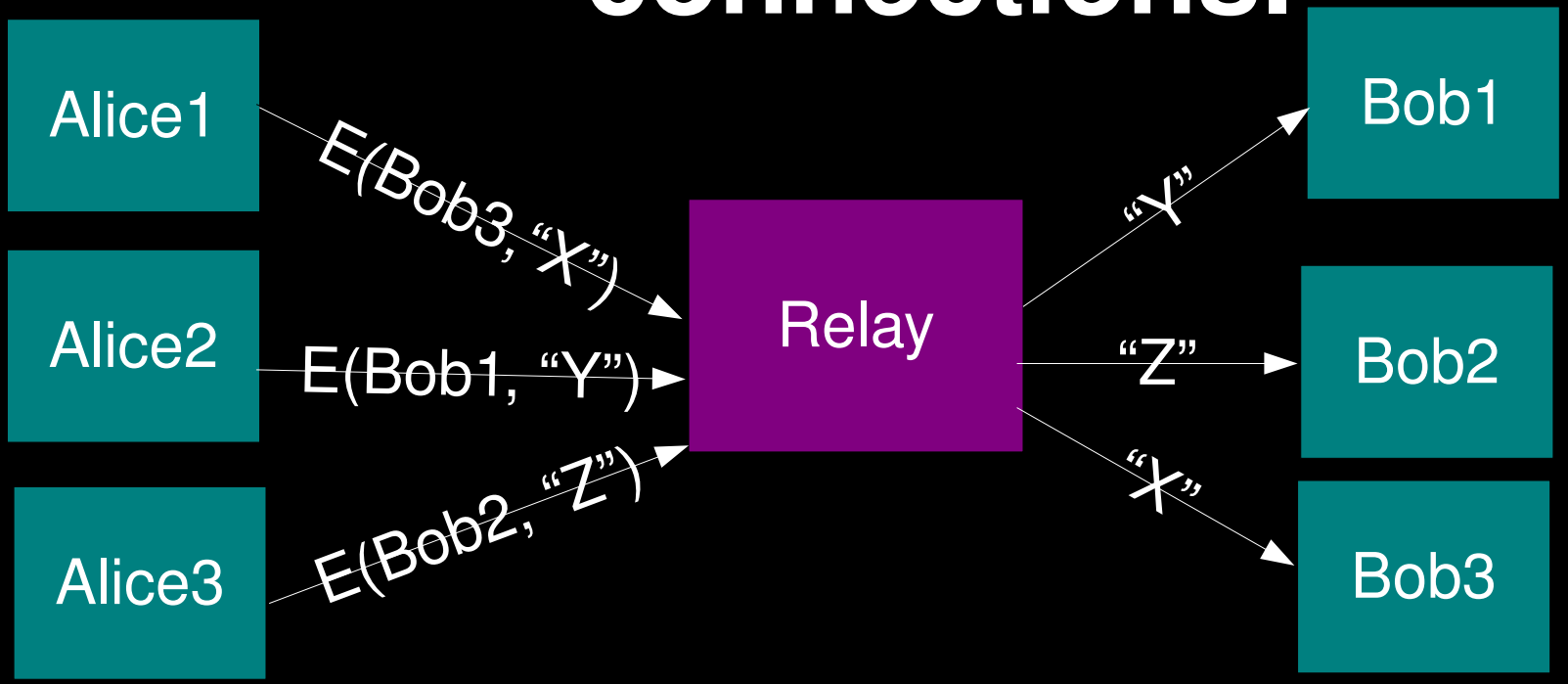
- online anonymity software and network
- open source, freely available
- active research environment

The Tor Project, Inc.

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

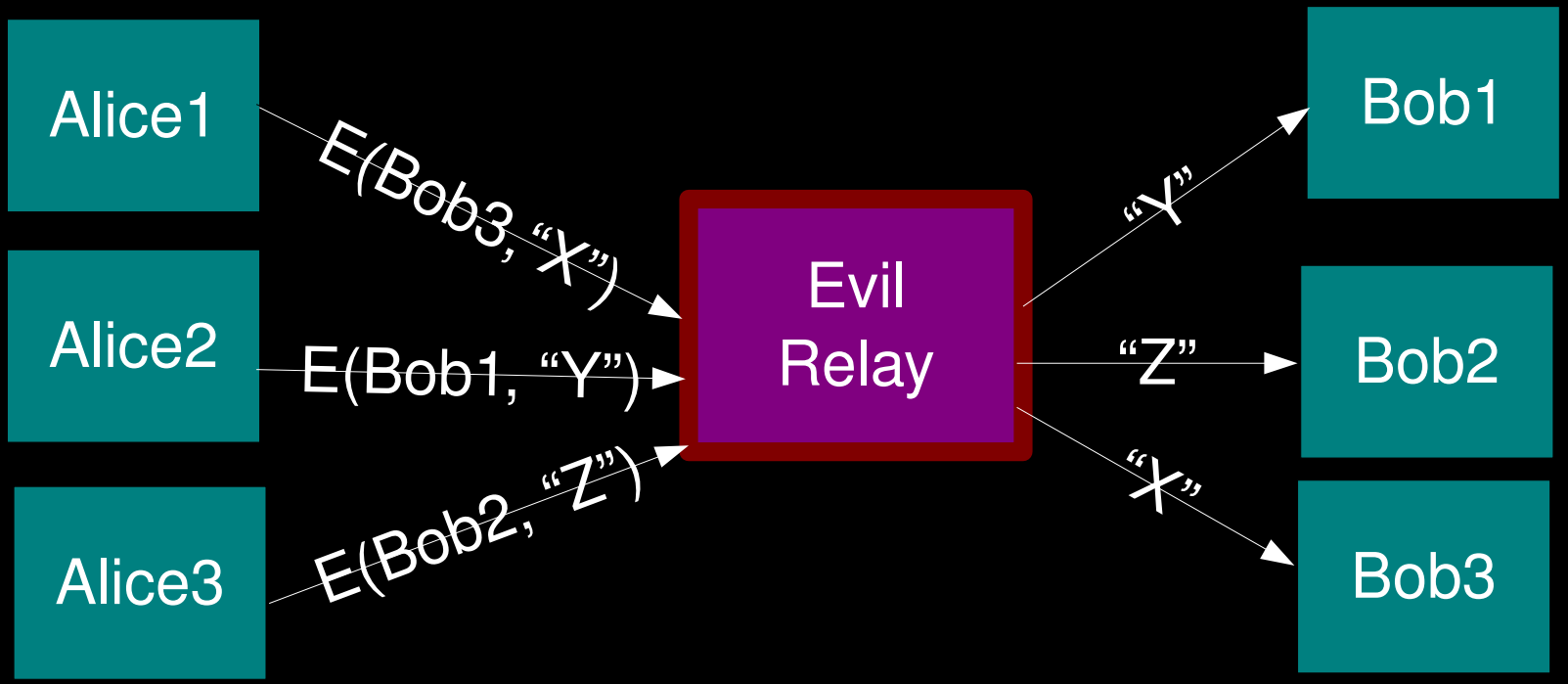

~300,000

The simplest designs use a single relay to hide connections.



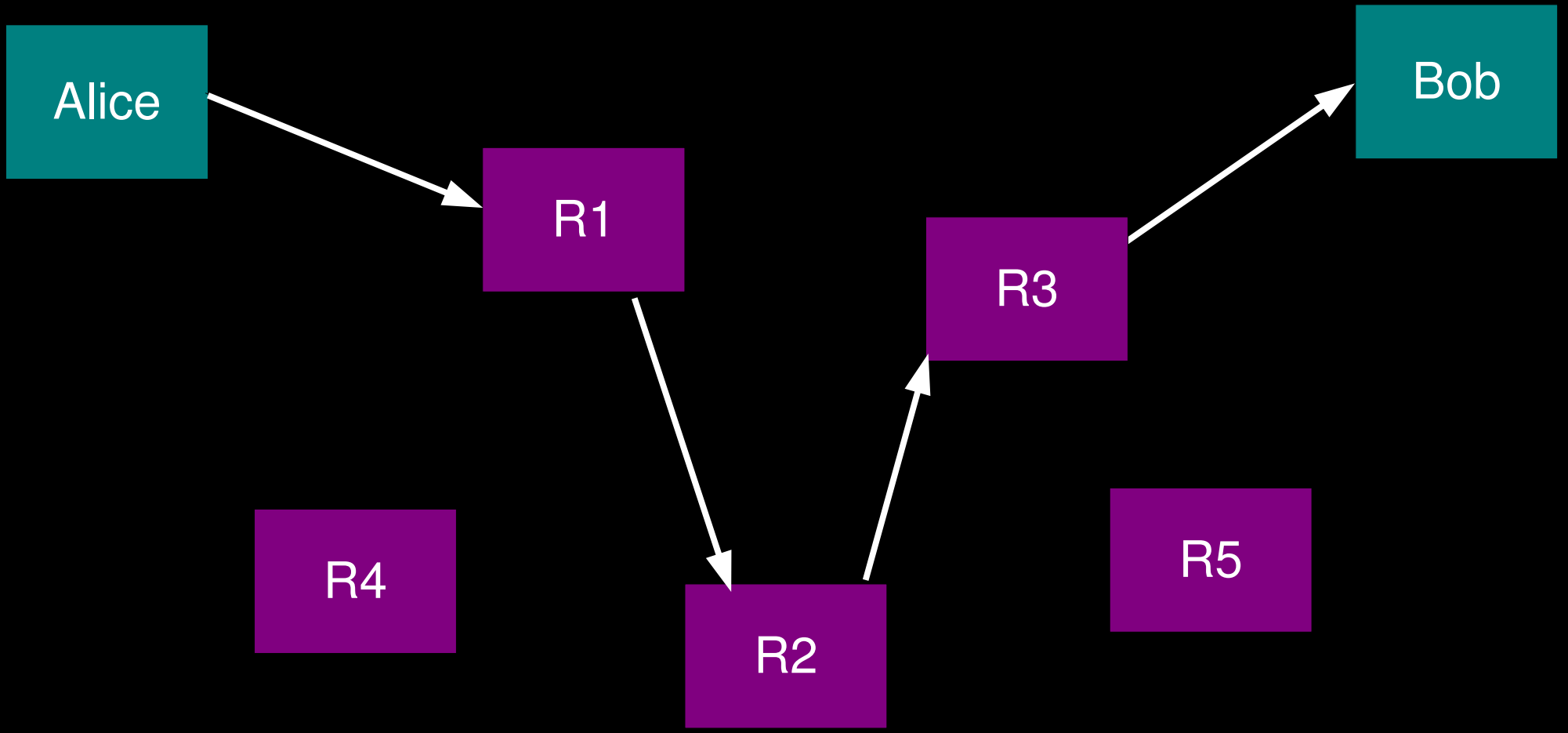
(example: some commercial proxy providers)

But a single relay is a single point of failure.

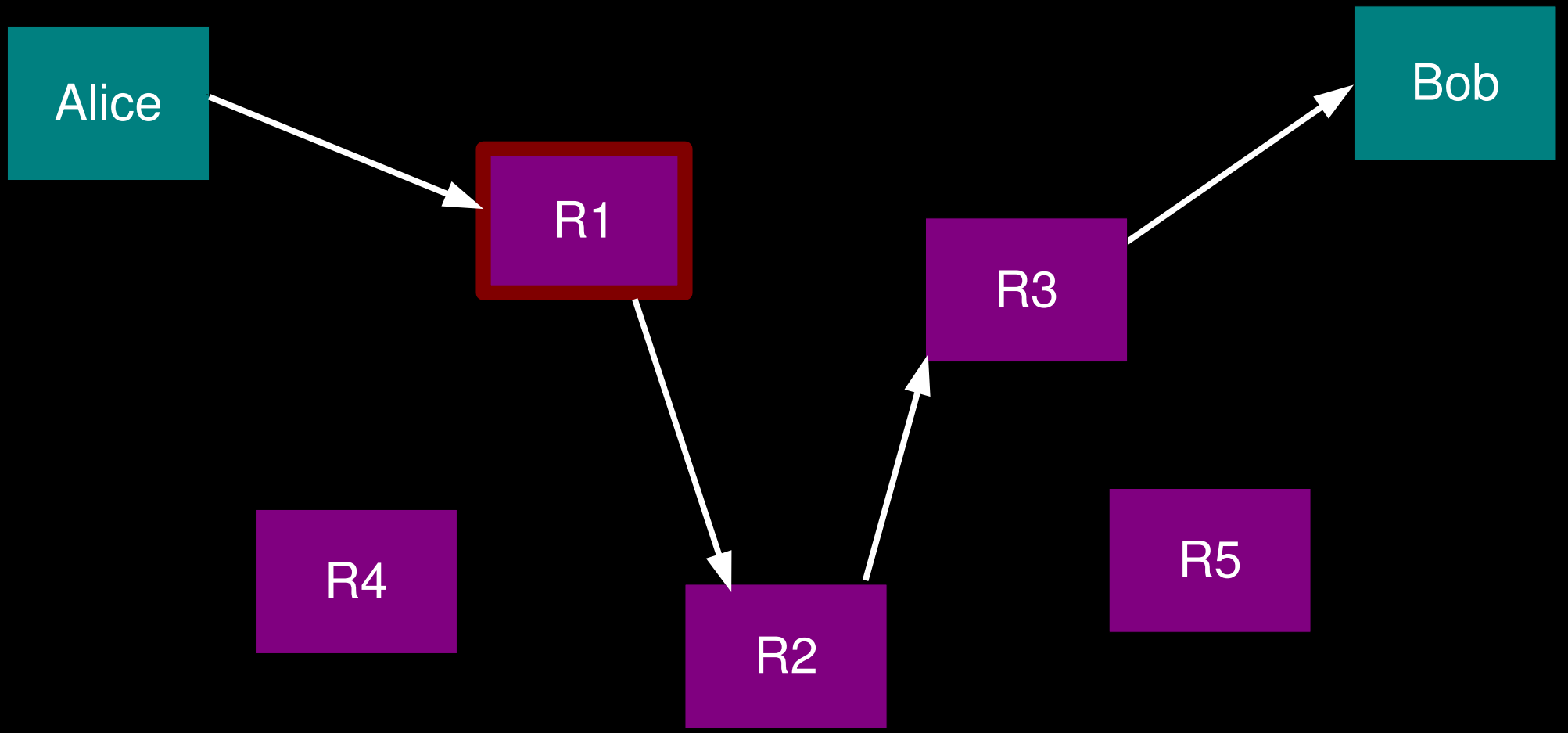


Eavesdropping the relay works too.

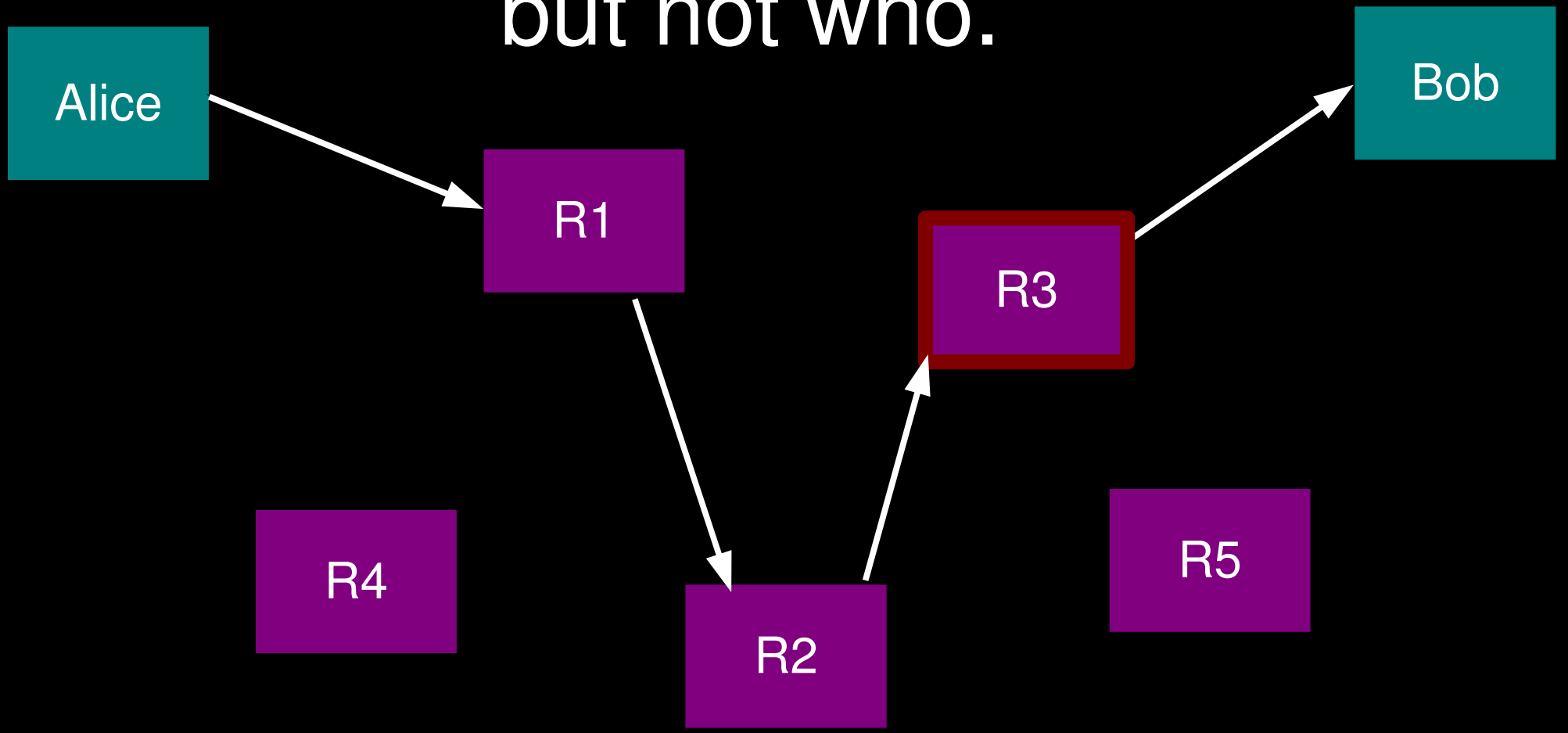
So, add multiple relays so that no single one can betray Alice.



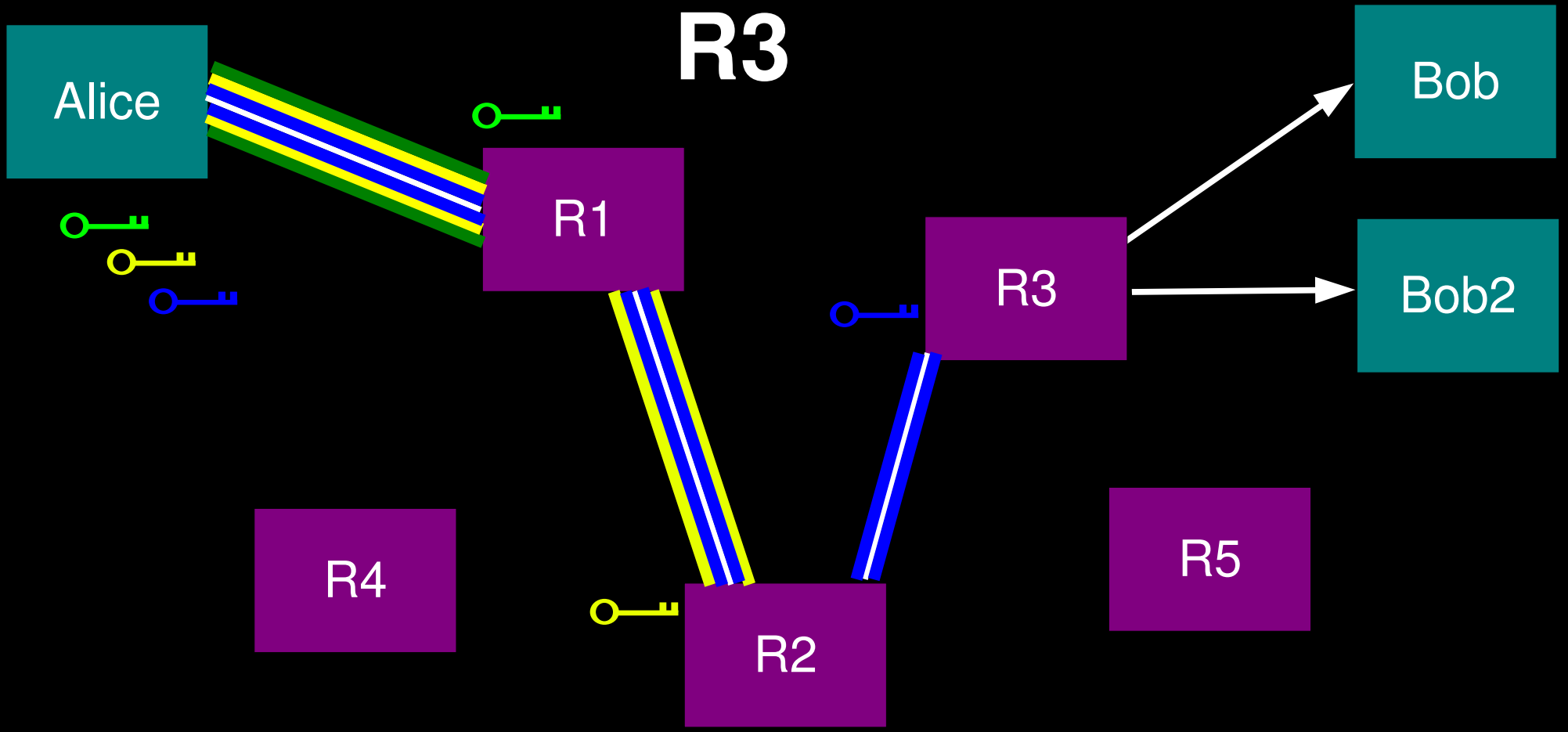
A corrupt first hop can tell that Alice is talking, but not to whom.



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



Who uses Tor?

- Normal people
- Law Enforcement
- Human Rights Activists
- Business Execs
- Militaries
- Abuse Victims

- Tor doesn't magically encrypt the Internet
- Operating Systems and Applications leak your info
- Browser Plugins, Cookies, Extensions, Shockwave/Flash, Java, Quicktime, and PDF all conspire against you

Outline

- Why anonymity?
- Crash course on Tor
- *Future*

Community

- Many tools make a big splash in the press
  - Censors need to feel in control; publicity removes the appearance of control
- Increase community diversity
  - Strong social network
- Funding
  - Donations, grants, contracts

3-Year Development Roadmap

- Improve Performance
- Client Safety
- Ease of Use and Understanding
- Core Research & Development

https://torproject.org/press/ for details

Copyrights

- who uses tor? http://www.flickr.com/photos/mattw/2336507468/ , Matt Westervelt, CC-BY-SA
- danger!, http://flickr.com/photos/hmvh/58185411/sizes/o/, hmvh, CC-BY-SA
- 300k, http://flickr.com/photos/tochis/1169807846/sizes/ , tochis, CC-BY-NC