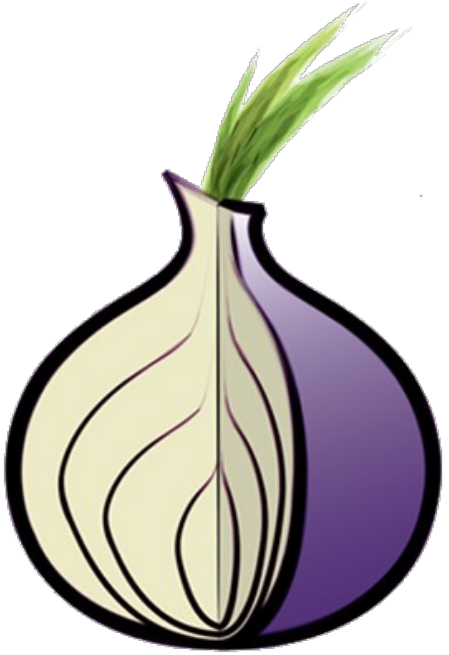
The Tor Project



Anonymity Online

Erinn Clark
erinn@torproject.org
Московский Государственный Университет 2010

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

The Tor Project, Inc.

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

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

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

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 Tor?

- Online anonymity: software, network, protocol

What is Tor?

- Online anonymity: software, network, protocol
- Free software

What is Tor?

- Online anonymity: software, network, protocol
- Free software
- Community of researchers, developers, and relay operators

What is Tor?

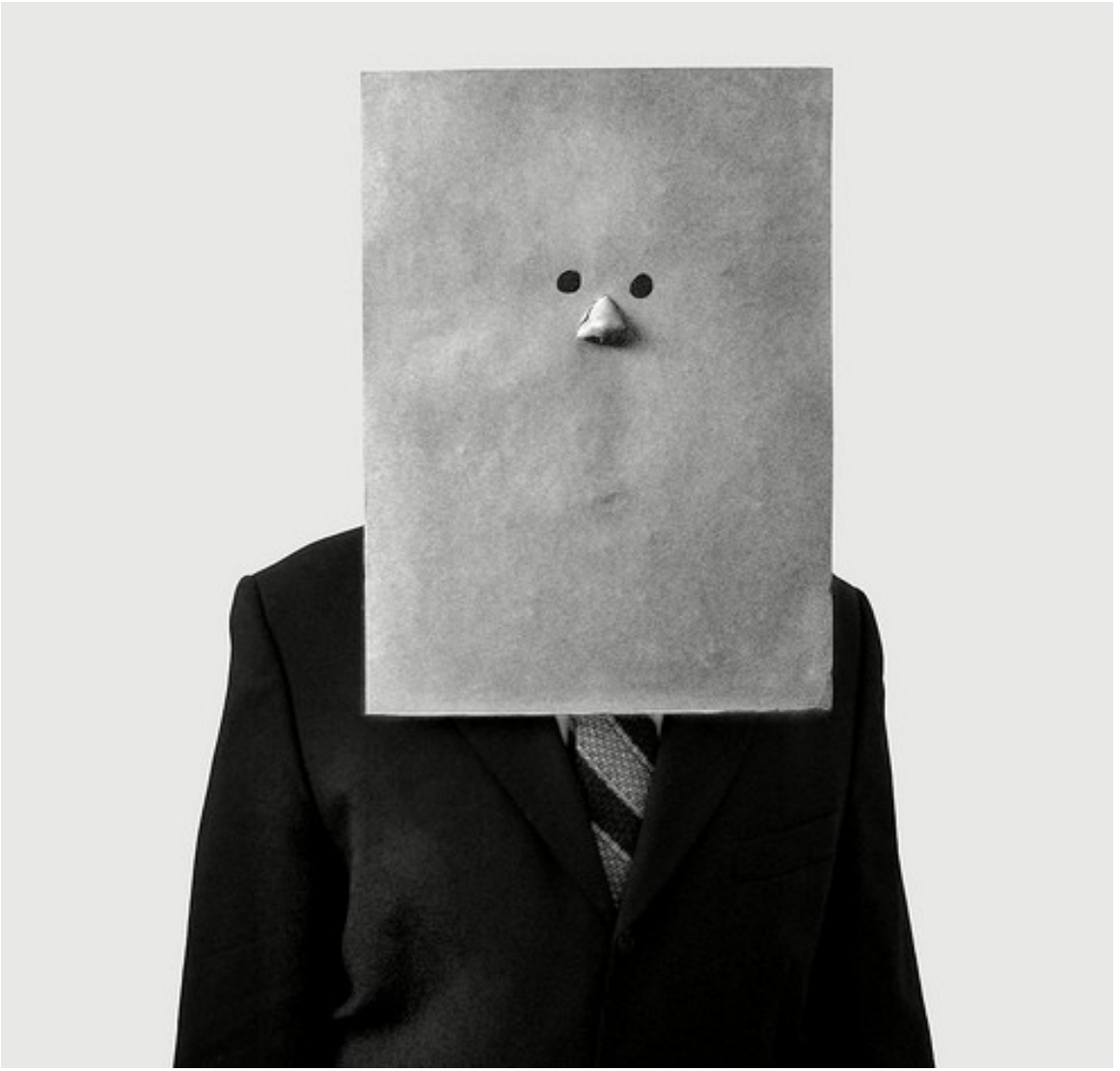
- Online anonymity: software, network, protocol
- Free software
- Community of researchers, developers, and relay operators
- Funding from US DoD, EFF, Voice of America, Google, NLNet, Human Rights Watch, ...

Каждое личное существование держится на тайне, и, быть может, отчасти поэтому культурный человек так нервно хлопочет о том, чтобы уважалась личная тайна.

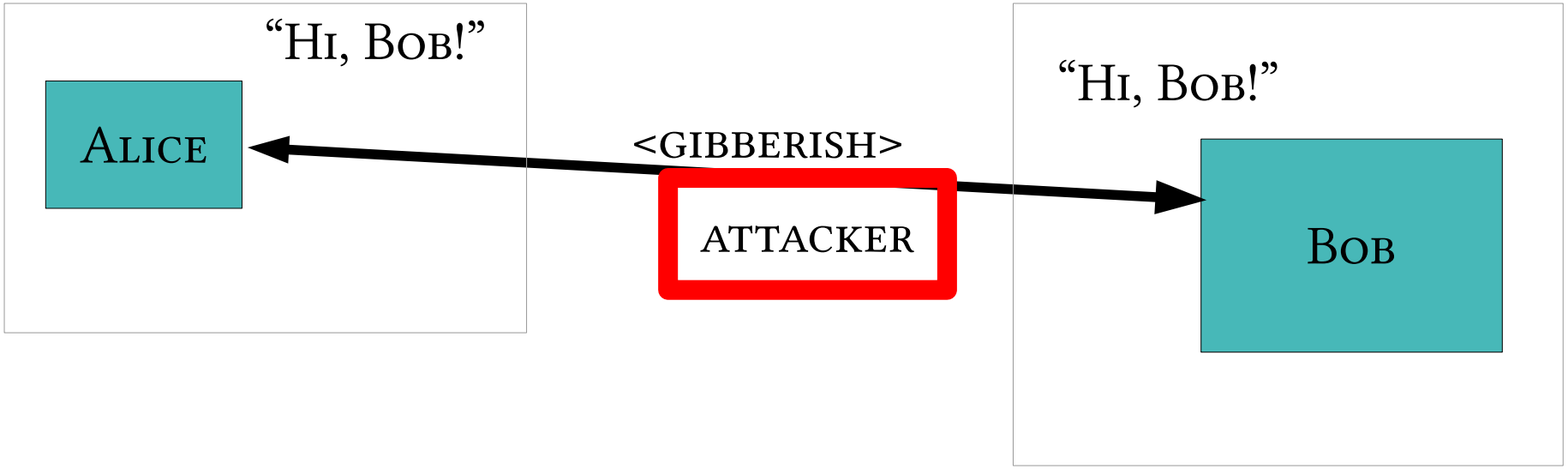
- Антон Чехов

Дама с собачкой

What is anonymity?



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!"

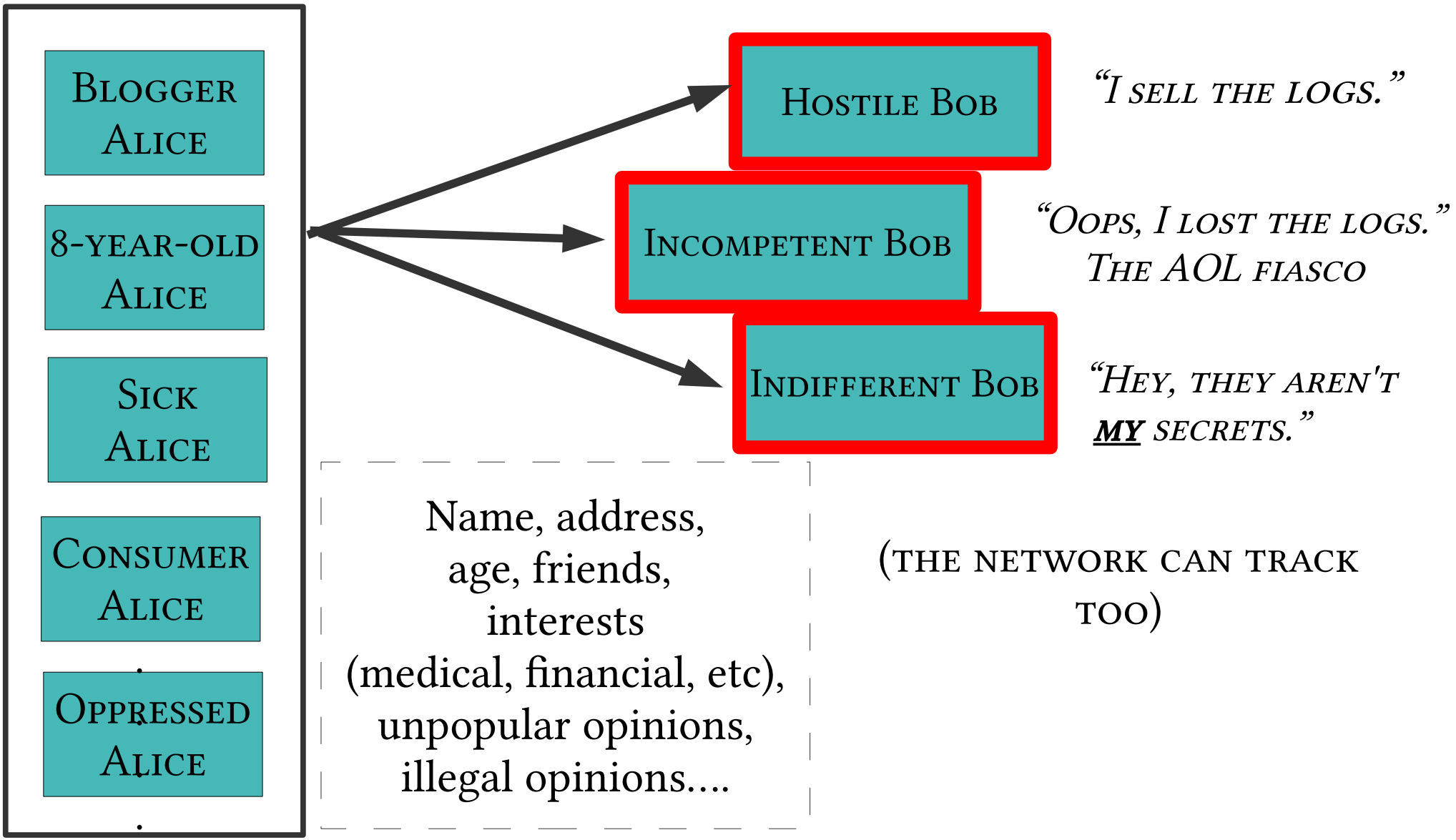
"Promise you won't remember!"

"Promise you won't tell!"

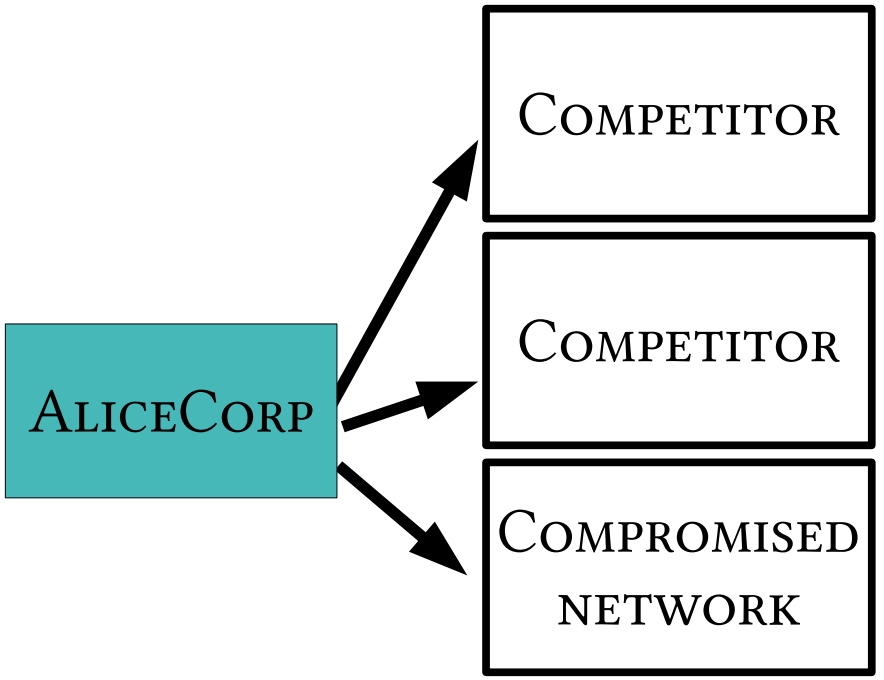
"I didn't write my name on it!"

"Isn't the Internet already anonymous?"

Regular citizens don't want to be watched and tracked



Businesses need to keep trade secrets

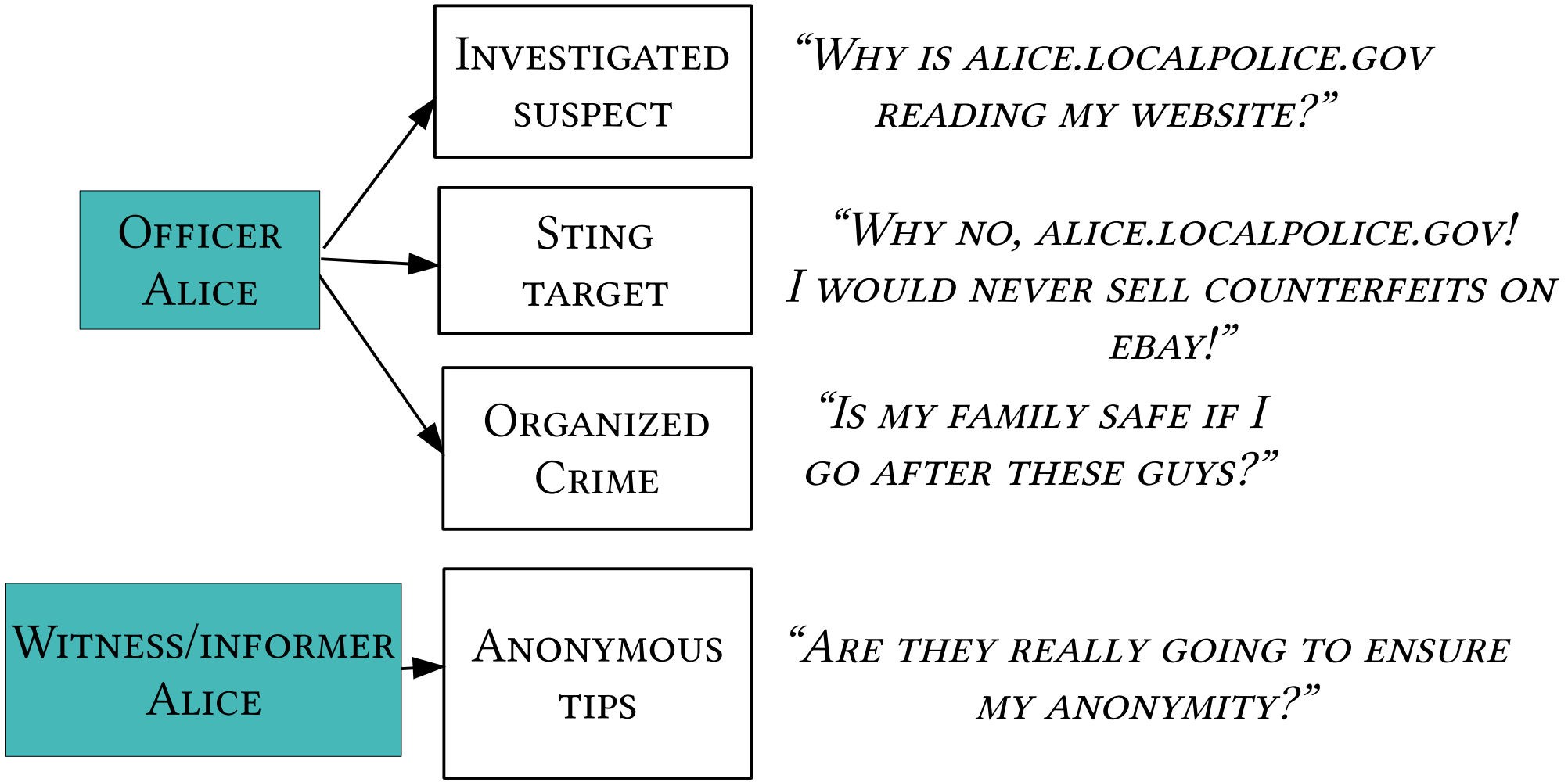


"Oh, your employees are reading our patents/jobs page/product sheets?"

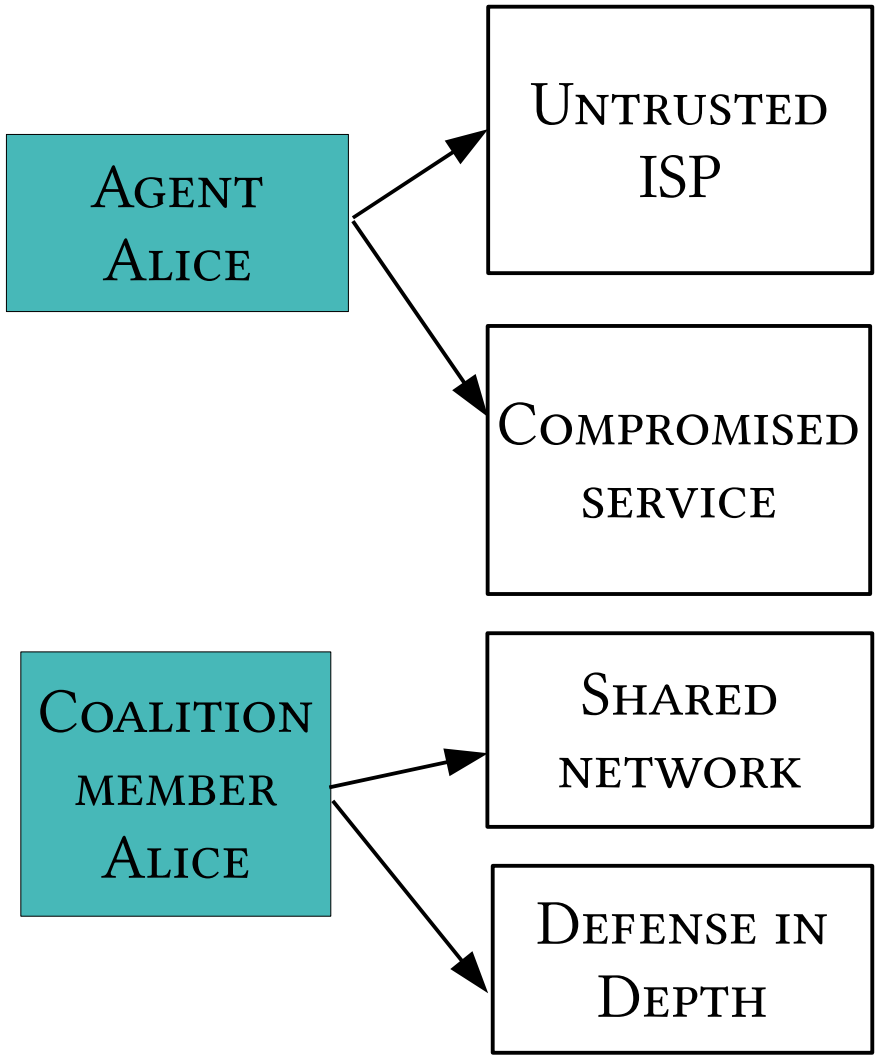
"Hey, it's Alice! Give her the 'Alice' version!"

"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?"

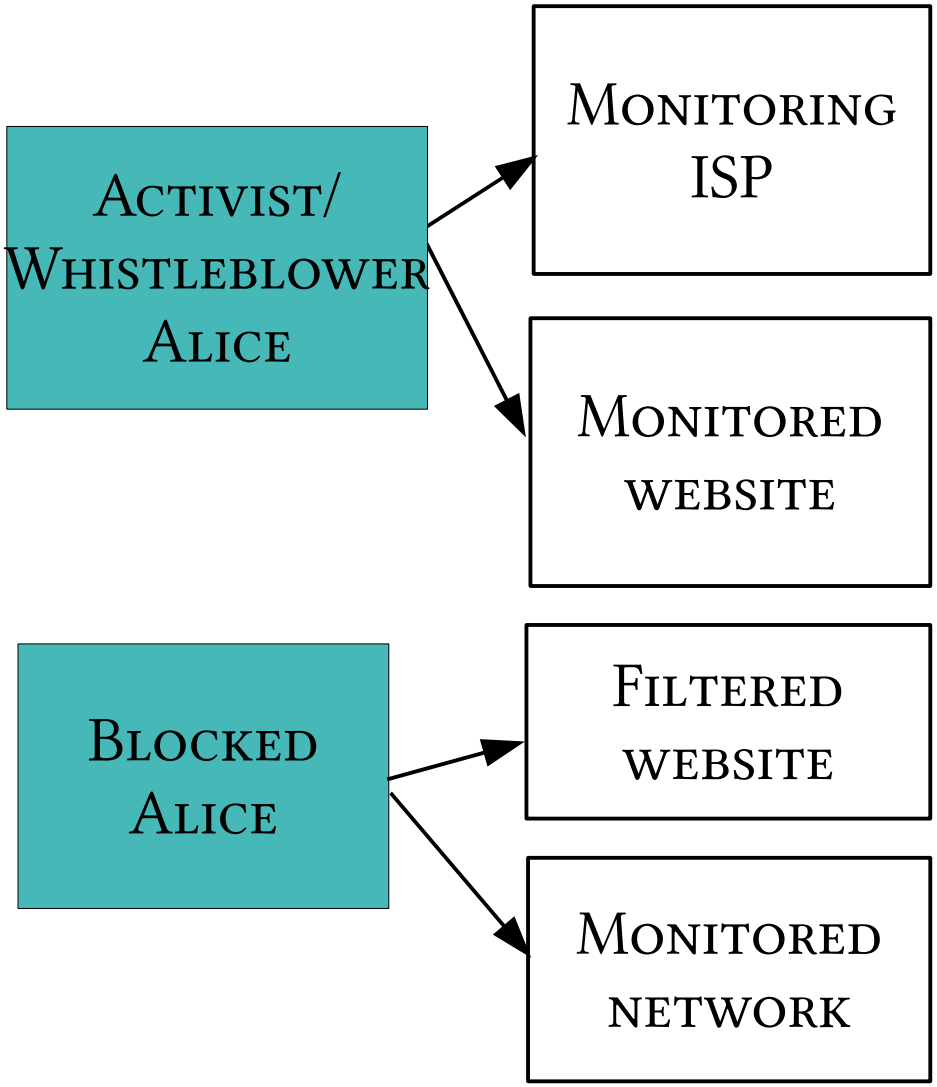
"Somebody in that hotel room just checked his Navy.mil mail!"

"What does FBI Google for?"

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

"What about insiders?"

Journalists and activists need Tor for their personal safety



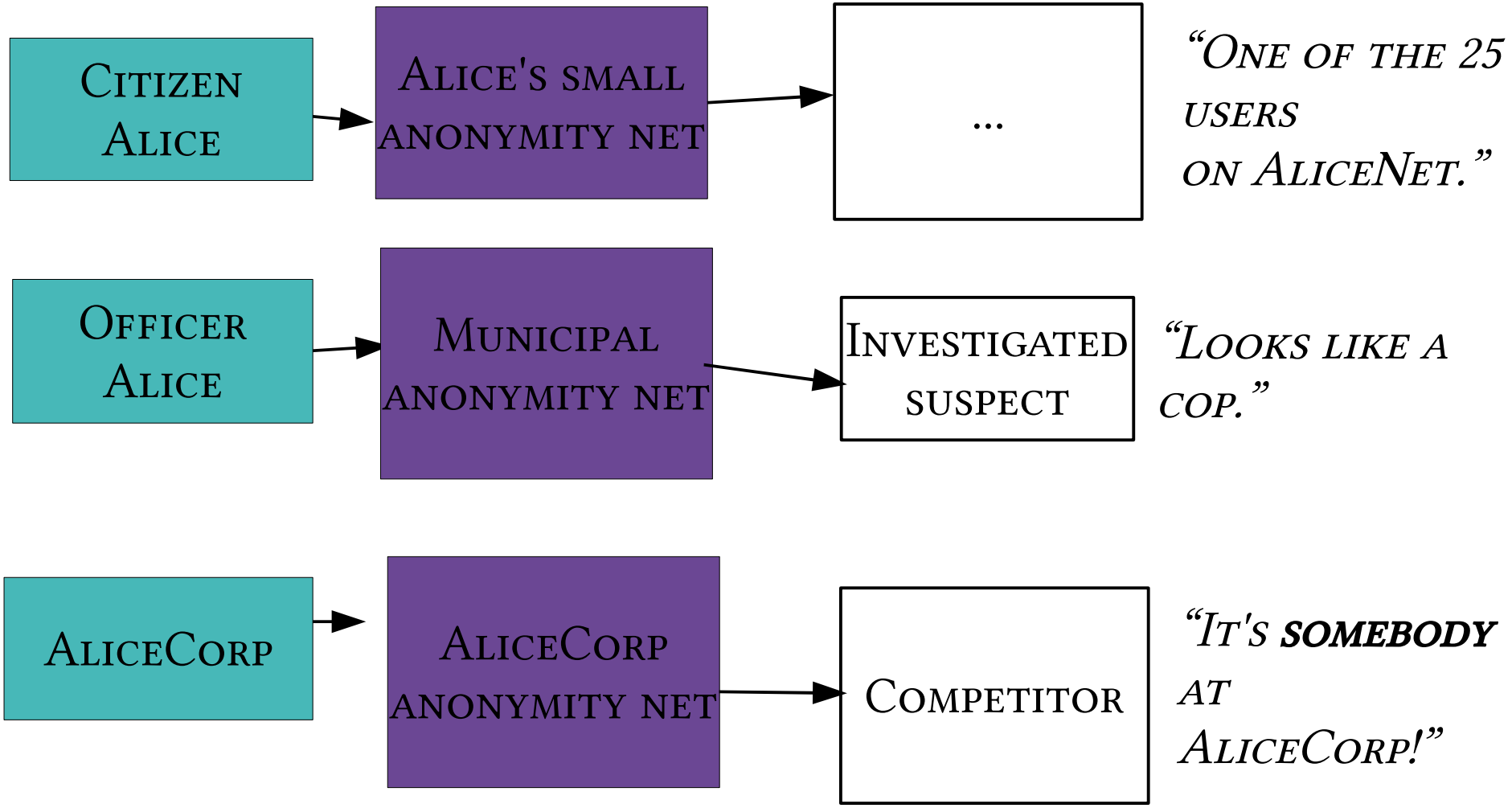
"Did you just post to that website?"

"Where are the bloggers connecting from?"
"I run livejournal and track my users"
"Of course I tell China about my users"

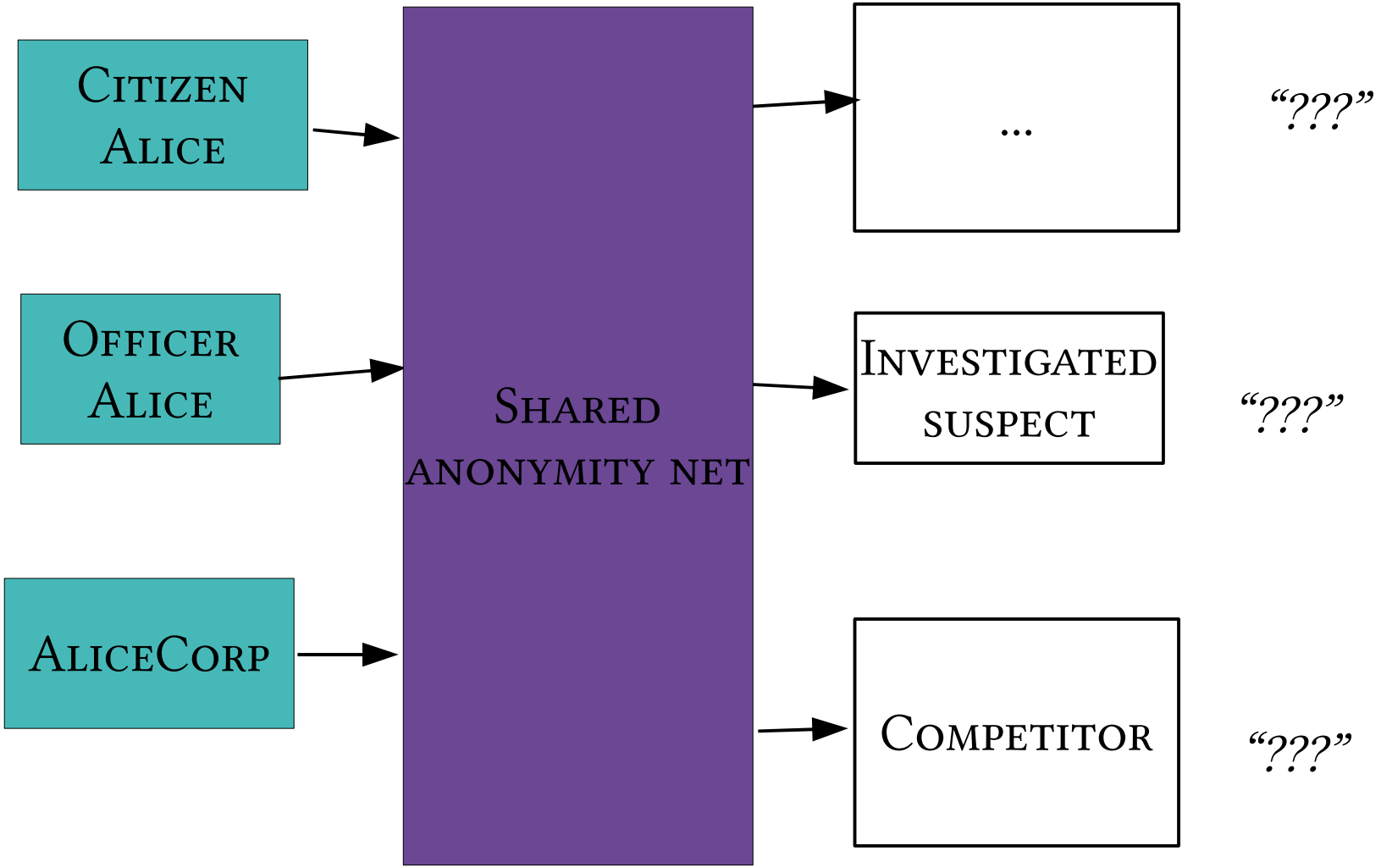
"What does the Global Voices website say today?"
"I want to tell people what's going on in my country"

"I think they're watching. I'm not even going to try."

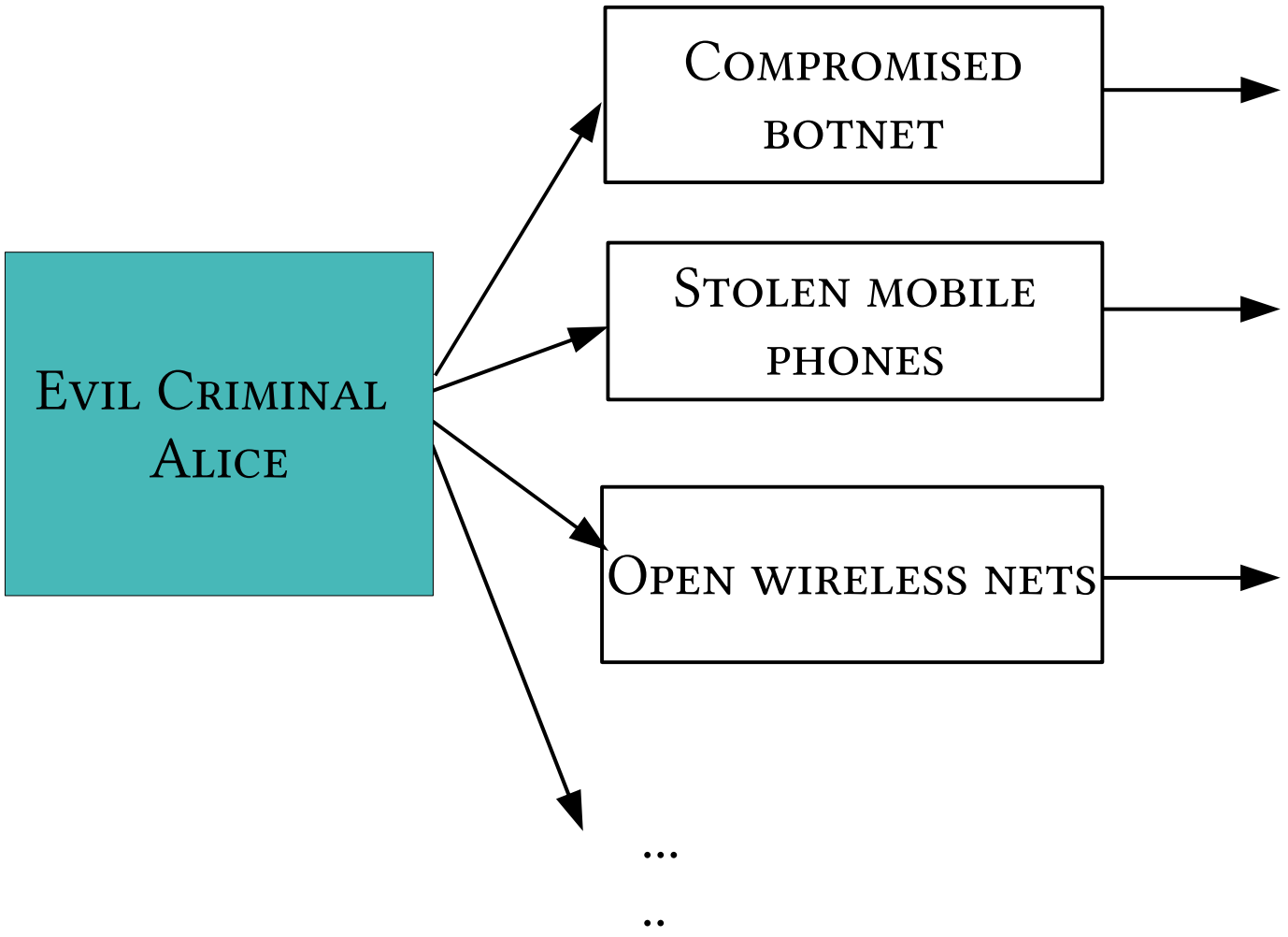
You can't get anonymity on your own: private solutions are ineffective...



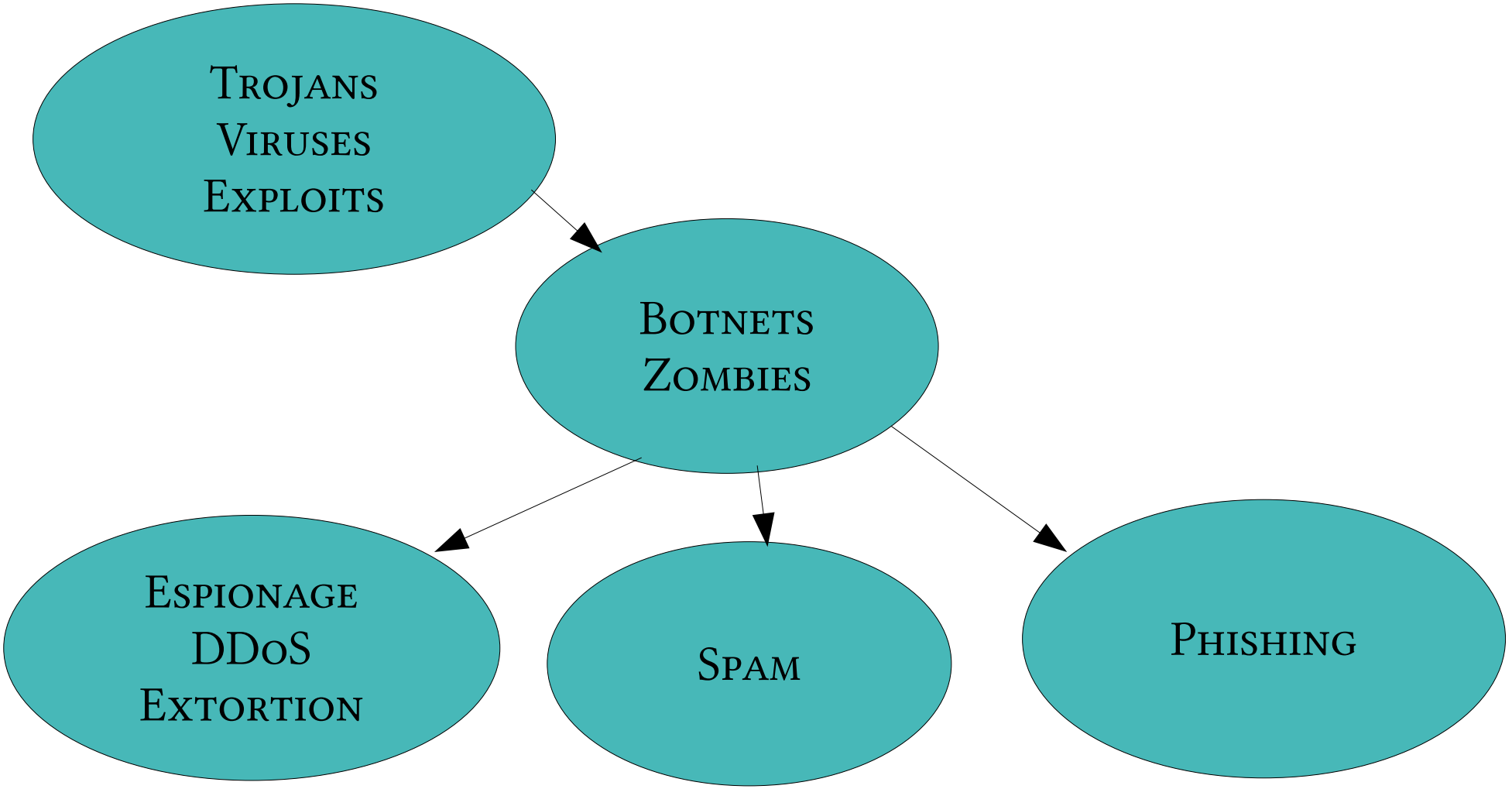
... so, anonymity loves company!



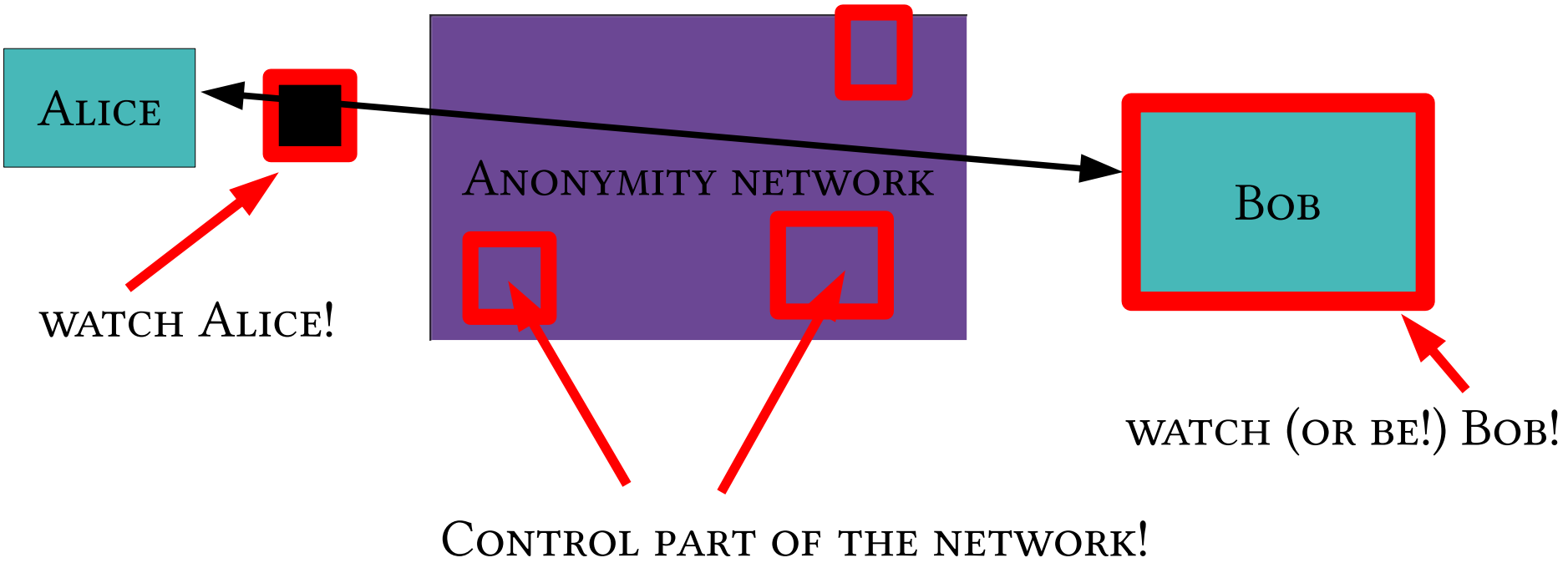
Yes, bad people need anonymity too. But they are *already* doing well.



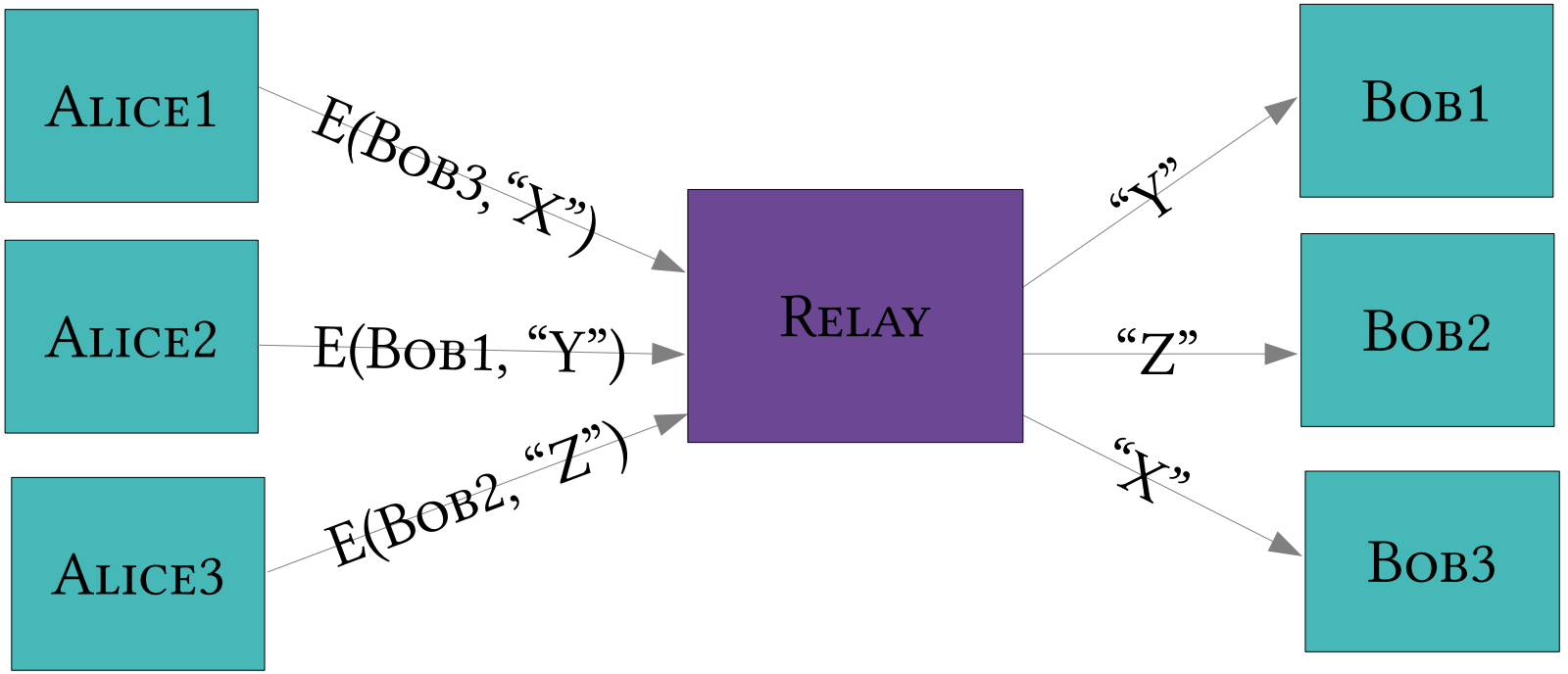
Current situation: Bad people on the Internet are doing fine



Threat model: what can the attacker do?

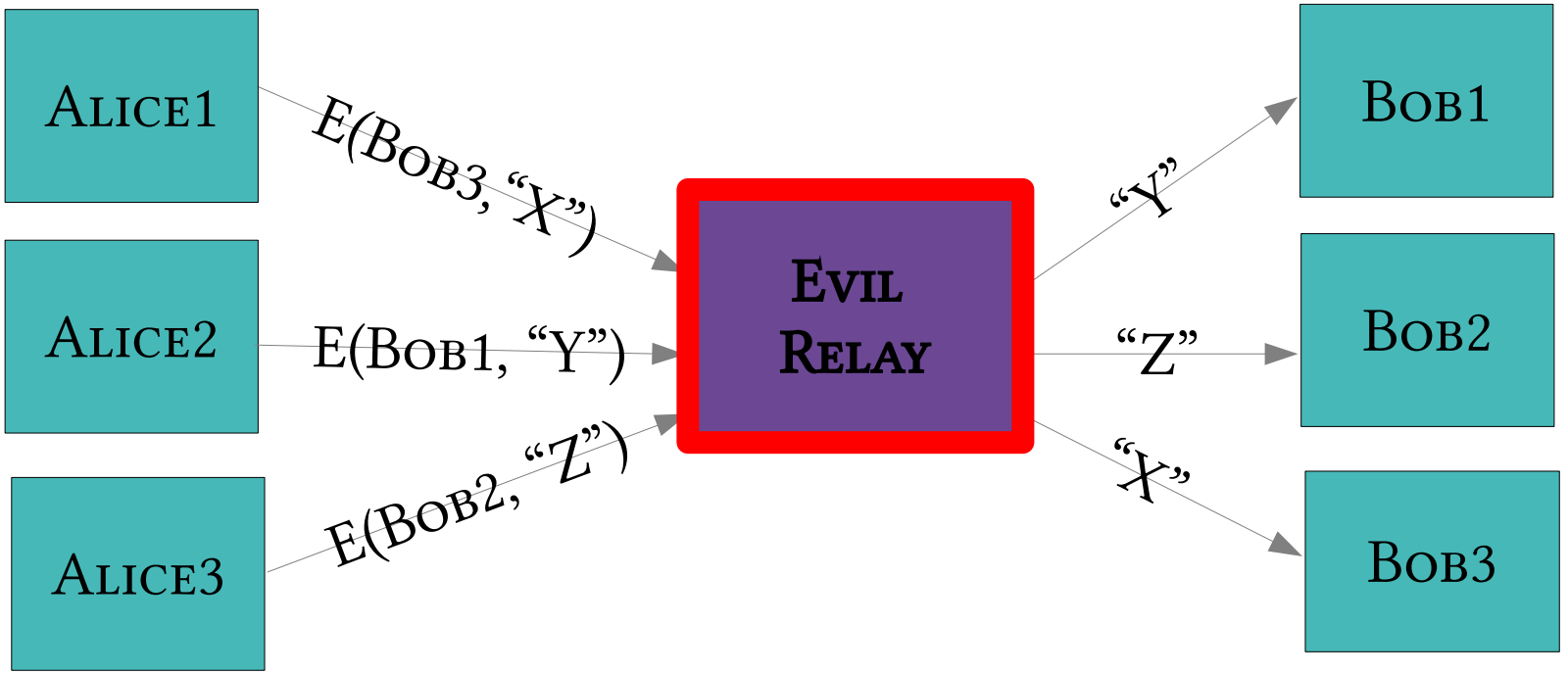


The simplest designs use a single relay to hide connections

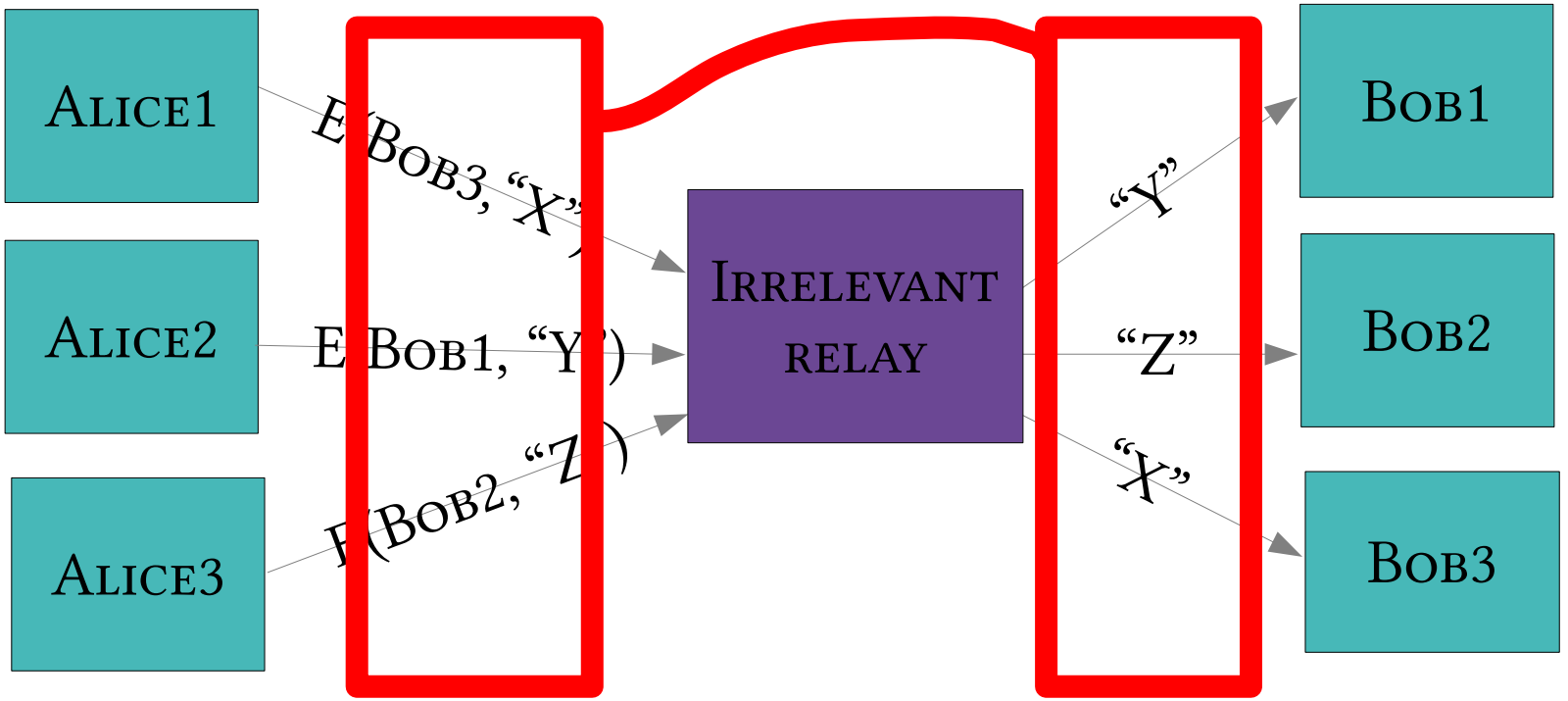


(example: some commercial proxy providers)

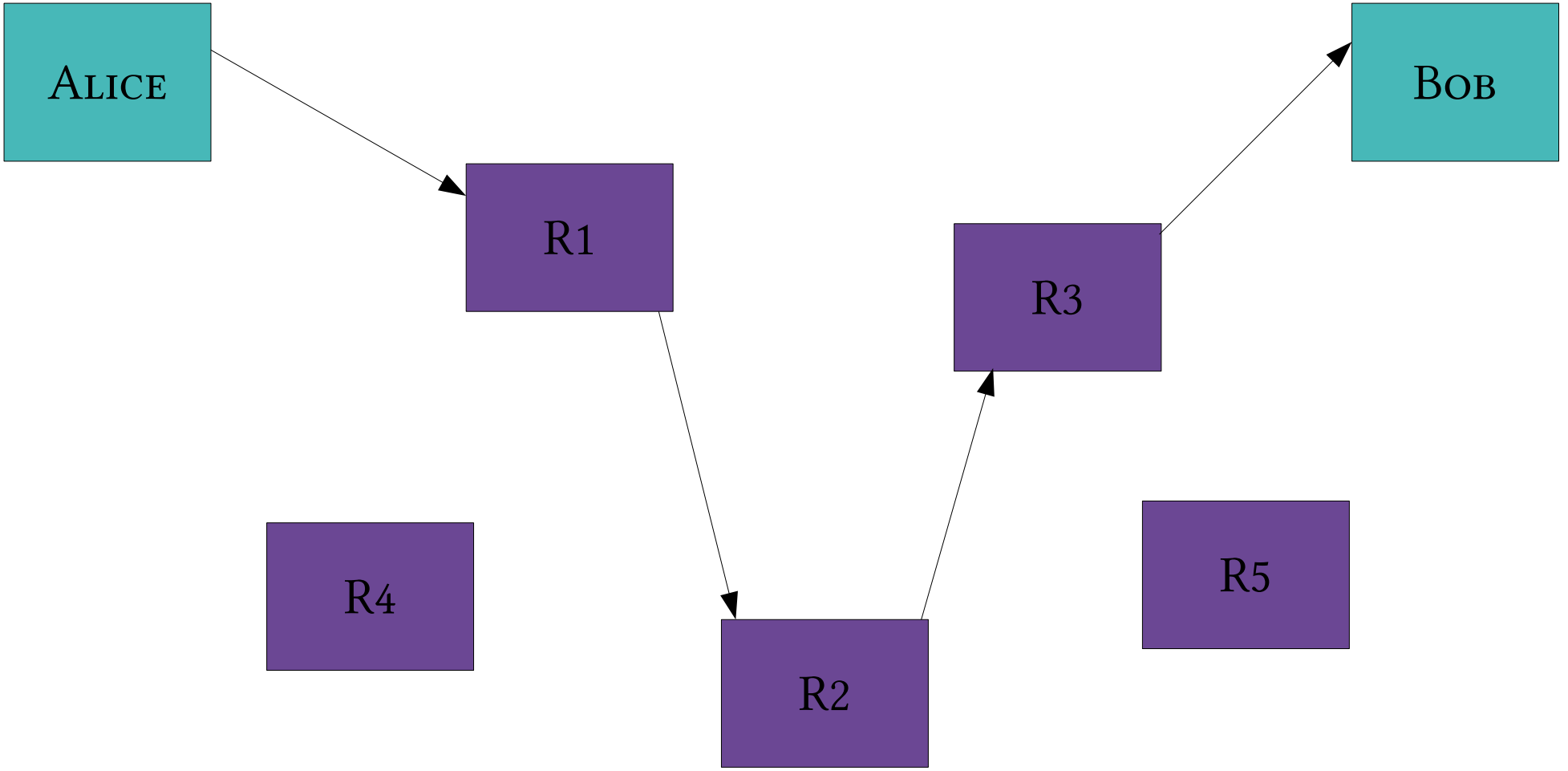
But a single relay (or eavesdropper!) is a single point of failure



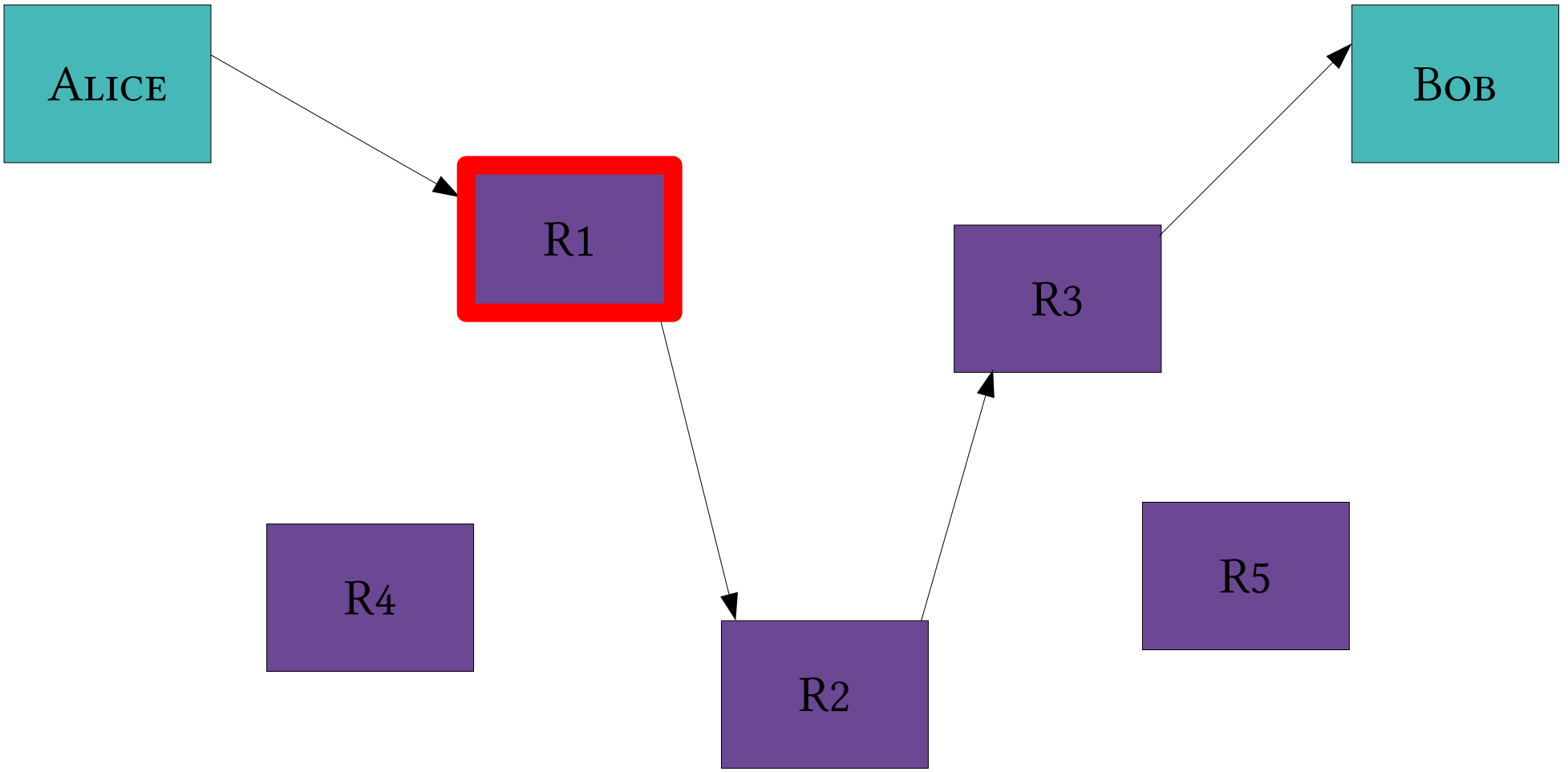
… OR A SINGLE POINT OF BYPASS



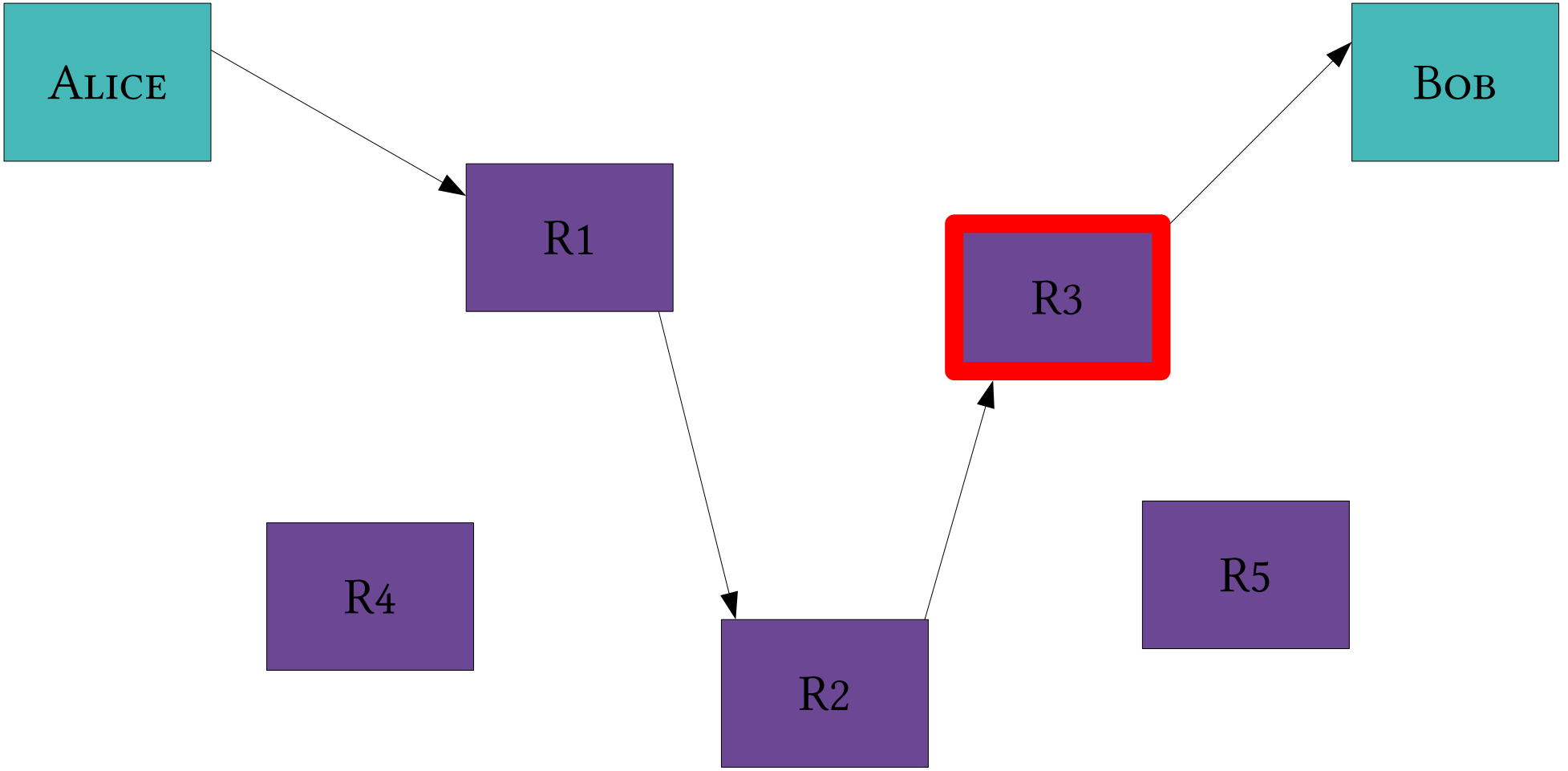
So, add multiple relays so that no single one can betray Alice



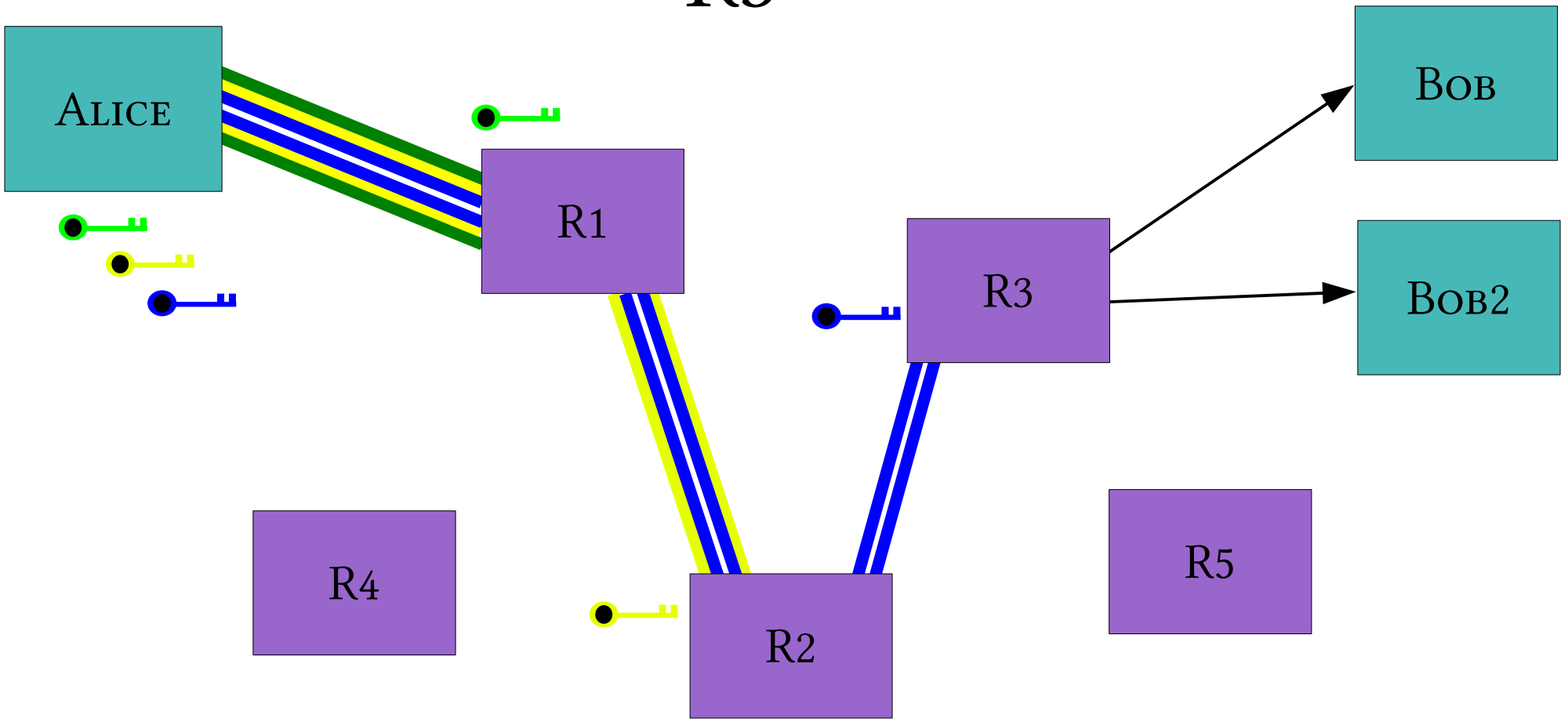
A corrupt first hop can tell that Alice is talking, but not to whom



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



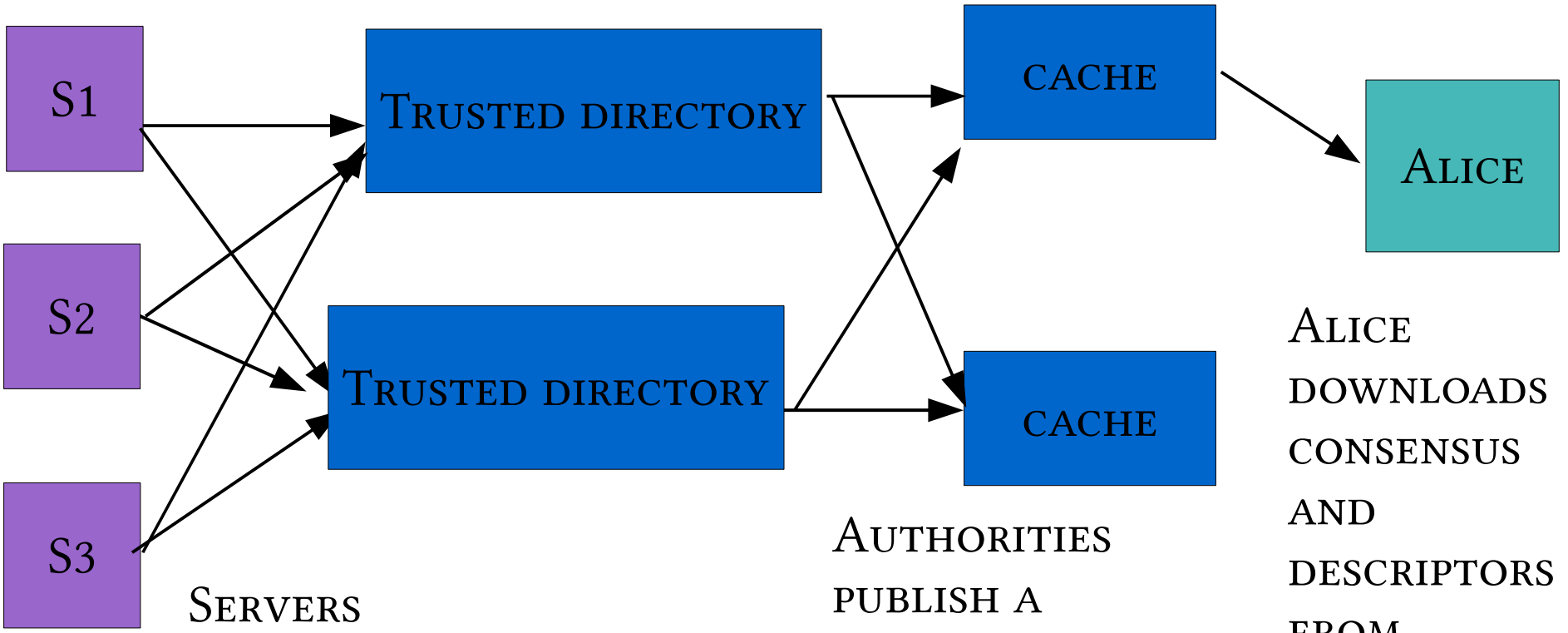
What we spend our time on

- Performance and scalability
- Maintaining the whole software ecosystem
- Blocking-resistance (circumvention)
- Basic research on anonymity
- Reusability and modularity
- Advocacy, education, and trainings around the world
- Metrics, data, and analysis

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



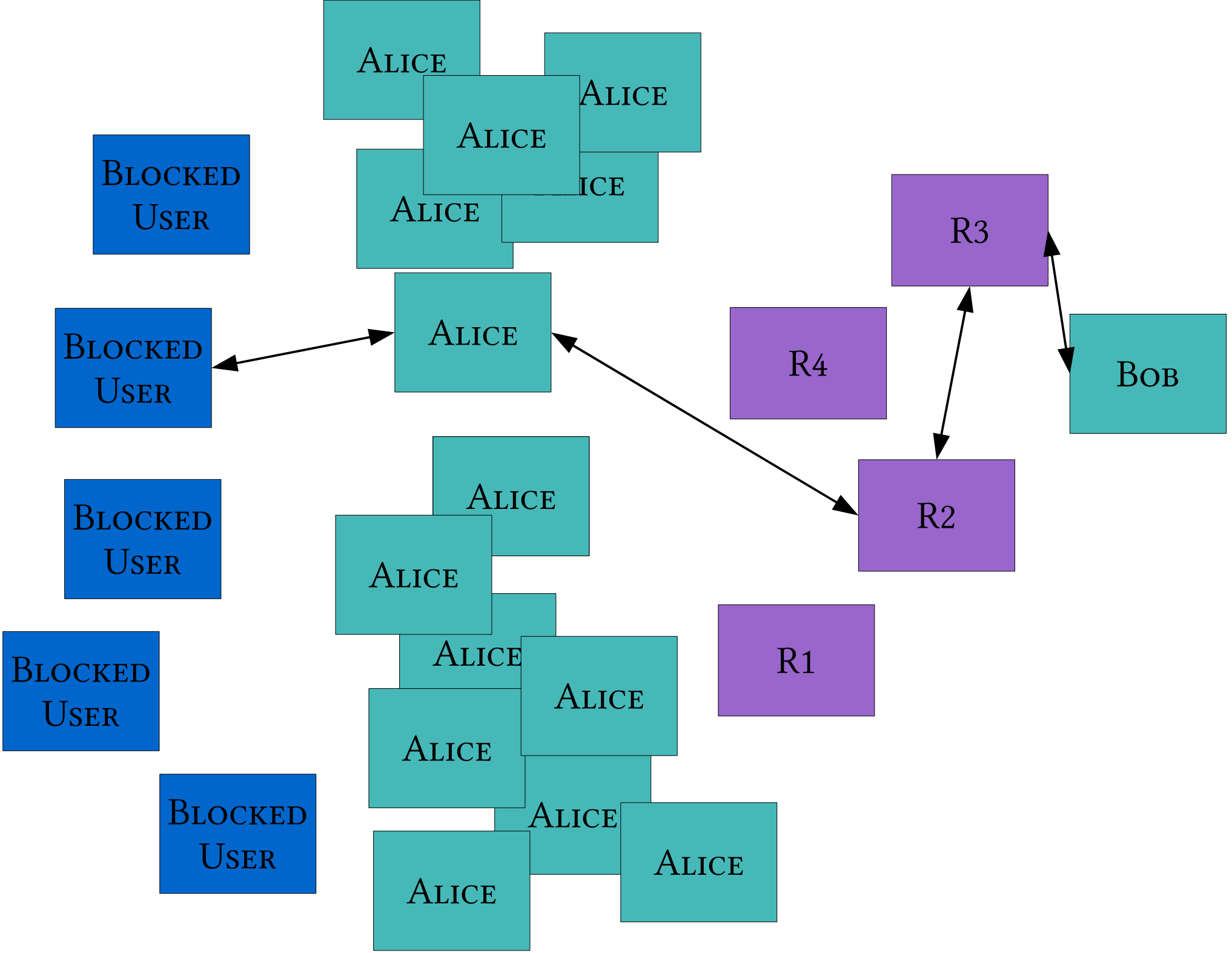
Servers publish self-signed descriptors.

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
Alice
Alice
Alice
Alice
Alice
Alice
Alice
R3
R4
Bob
R2
R1

"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

But the network layer is not the only problem

Browsers, plugins, and ignorance can de-anonymize you too

- Browsers are unique
- Plugins and various applications almost always ignore proxy settings
- Plaintext over Tor still plaintext

Javascript, cookies, history, etc

- Javascript refresh attack
- Cookies, History, browser window size, user-agent, language, HTTP auth, ...
- Mostly problems when you toggle from Tor to non-Tor or back
- Mike Perry's Torbutton Firefox extension tackles many of these

Bittorrent over Tor isn't a good idea

- Many popular clients ignore proxy settings...
- ... since they use UDP and we use TCP
- Some clients write your IP address into the information they send to the tracker
- Relay can also watch the traffic

Лука Мудищев - дворянин! (lukamud) wrote in ru_root,
@ 2010-01-13 11:46:00

Как я поймал хулигана использующего сеть Tor

Перед Новым Годом ко мне обратились с просьбой поймать злоумышленника, который сначала террори
электронной почте, отправляя письма похабного содержания через веб-интерфейсы бесплатных почтов
начал постить хулиганские комменты в корпоративном блоге в ЖЖ.

Одним из самых распространенных вариантов использования tor является связка Tor, Vidalia, Firefox+T

Установив Tor, и внимательно посмотрев на вкладку «Параметры соединения» я заметил, что в настройк
не прописывается поле «FTP прокси», т.е. запросы по протоколу FTP браузер отправляет напрямую, а н
сервер, слушающий на порту 8118 и отправляющий запросы через сеть tor! Это обусловлено скорее вс
поддерживает протокол FTP? Это наблюдалось в последних версиях ПО установленного на ОС MS Winc
Debian, Ubuntu.

Возникла идея подсунуть злоумышленнику ссылочку по протоколу FTP на объект, физически размещен
ftp-сервере, к логам которого у меня имеется доступ. Для этого в один из постов корпоративного блога
ссылочка на однопиксельное изображение вида <img ="ftp://<url_к_картинке_на_сервере_где_у
_меня_есть_доступ_к_логам">.

В тот же вечер был засечен реальный (не Tor) IP-адрес злоумышленника, но радоваться было рано, он
выделенной крупному московскому провайдеру. На следующий день мы имели и корпоративный IP-адр
злоумышленника.

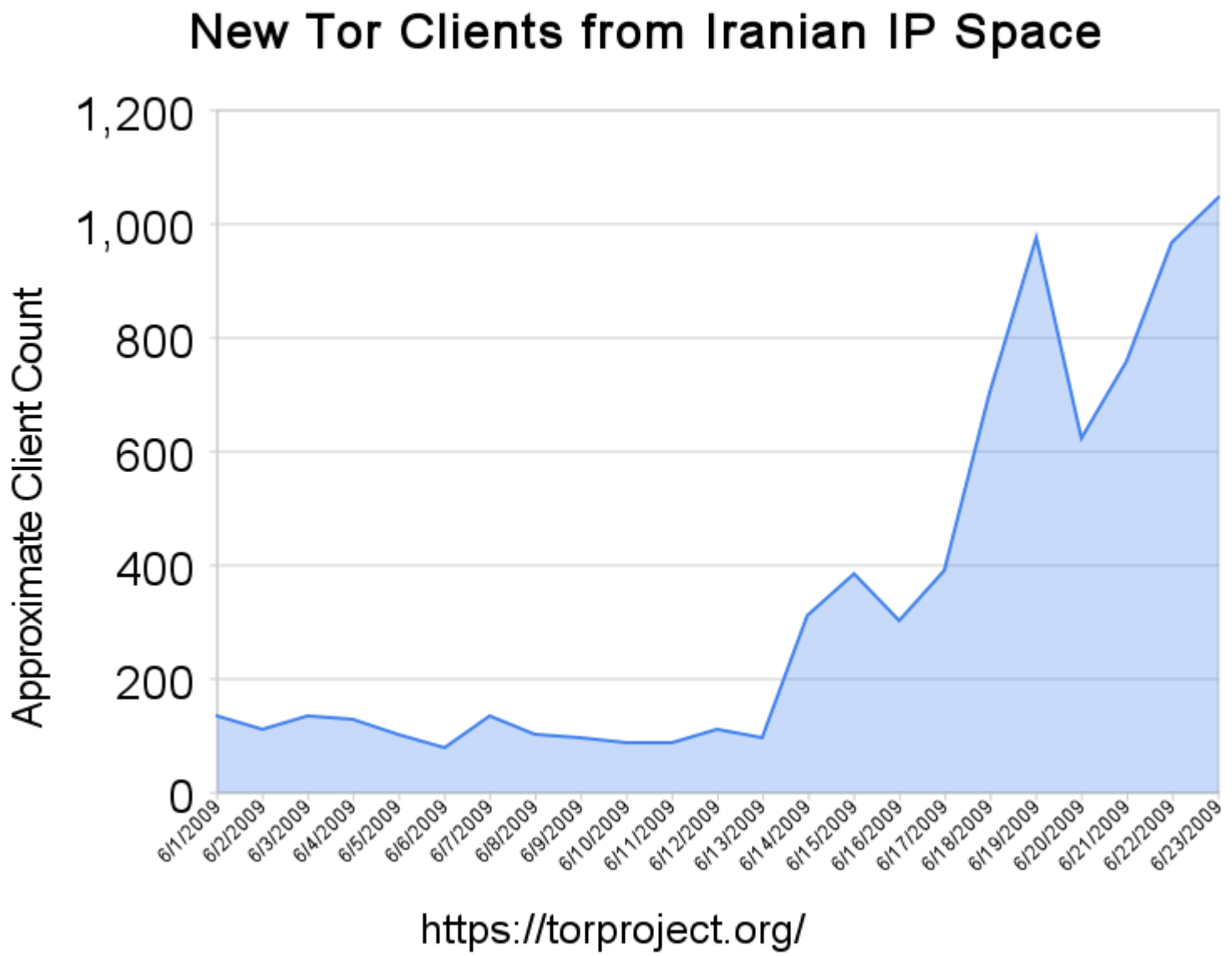
Who uses Tor and why?

Who uses Tor and why?

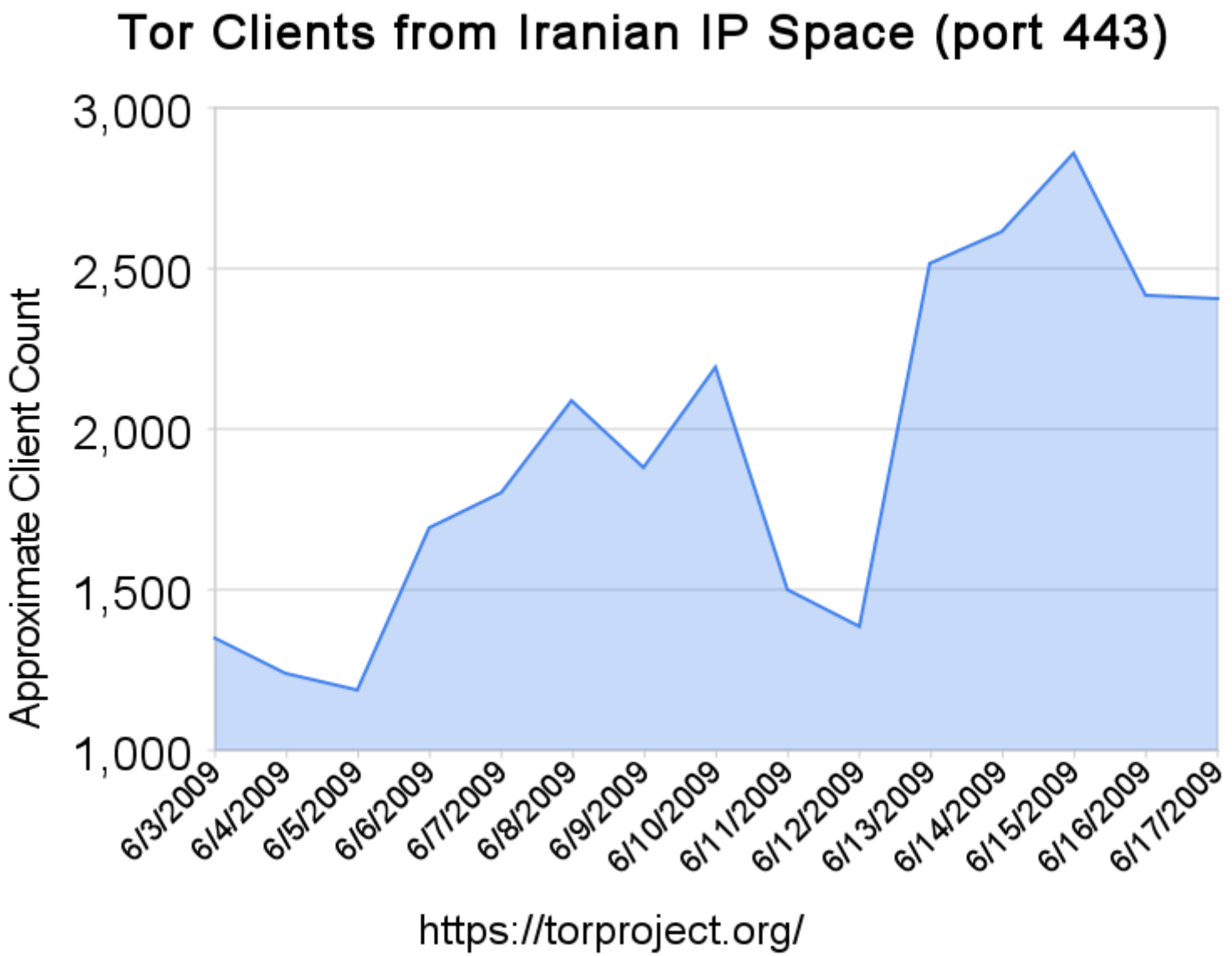
- Normal people
- Law enforcement
- Human rights activists
- Business executives
- Militaries
- Abuse victims
- Whistleblowers

Estimated 500,000 daily Tor users

Tor and Circumvention



Tor and Circumvention



Tor and Circumvention

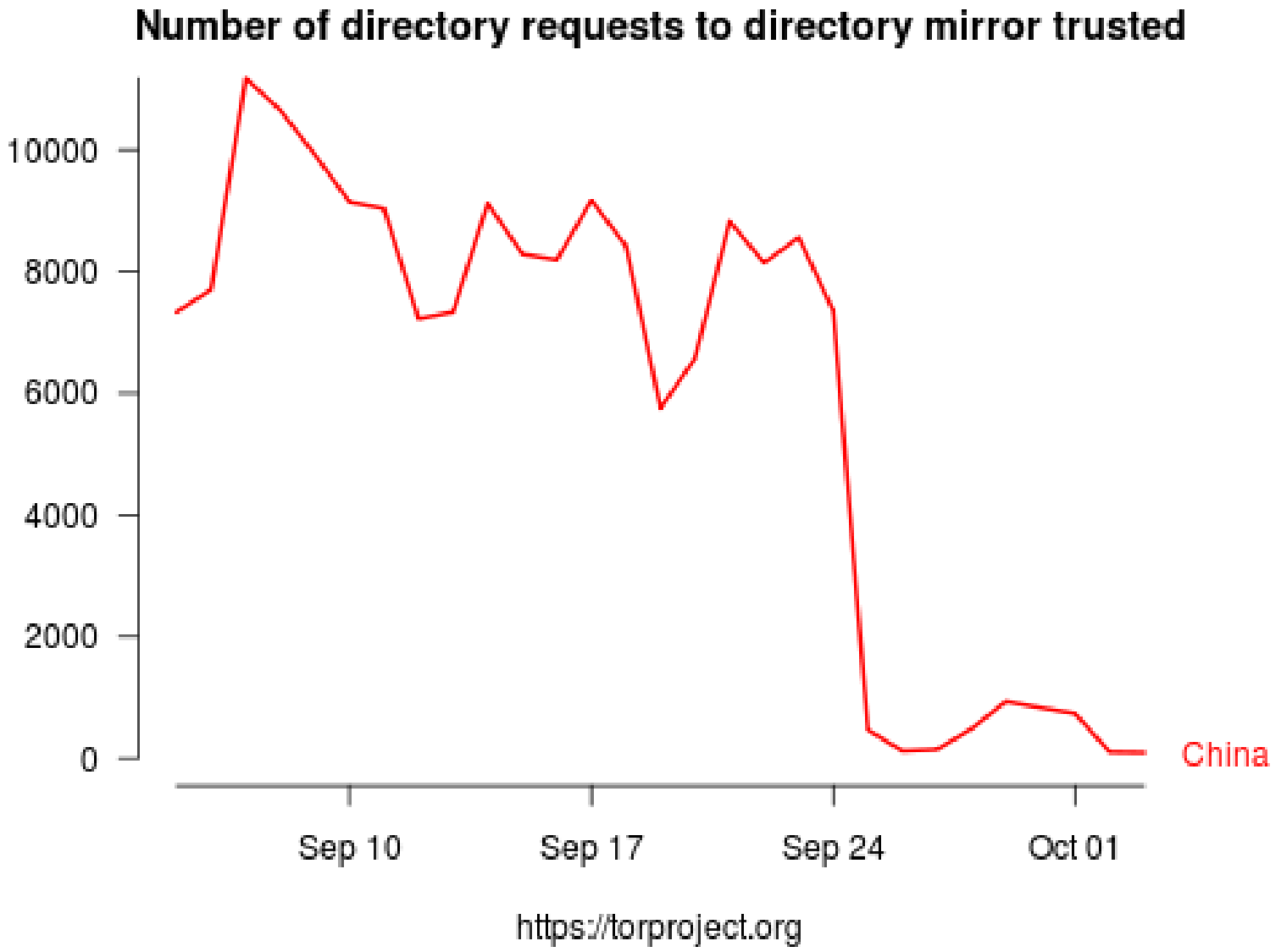
What happened around September 25th, 2009?

Tor and Circumvention

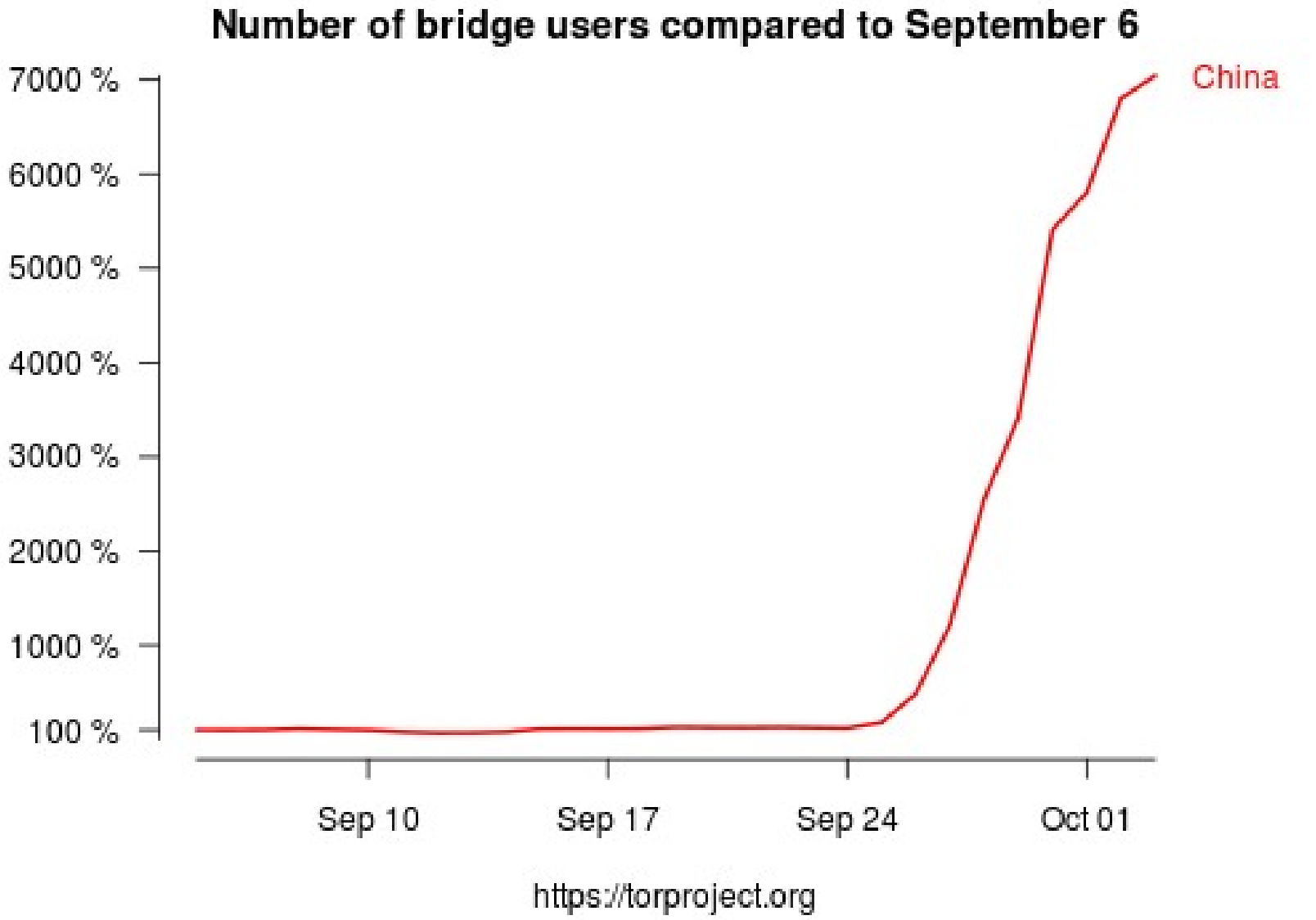
What happened around September 25th, 2009?

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

Tor and Circumvention



Tor and Circumvention



Want to help?

- Run a bridge
- Run a relay
- Help us hack on stuff!

More information at https://www.torproject.org/

Credits and Links

- Irving Penn / Steinberg In Nose Mask Recreation: Summer Luu via Flickr
  http://www.flickr.com/photos/summerluu/2388805263/

- "How Unique is Your Browser?"
  https://panopticlick.eff.org/browser-uniqueness.pdf

- Tor Metrics Portal
  https://metrics.torproject.org/