Tor, a quick overview

Linus Nordberg
<linus@torproject.org>

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 US DoD, Electronic Frontier Foundation, Voice of America, Google, NLnet, Human Rights Watch and more

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

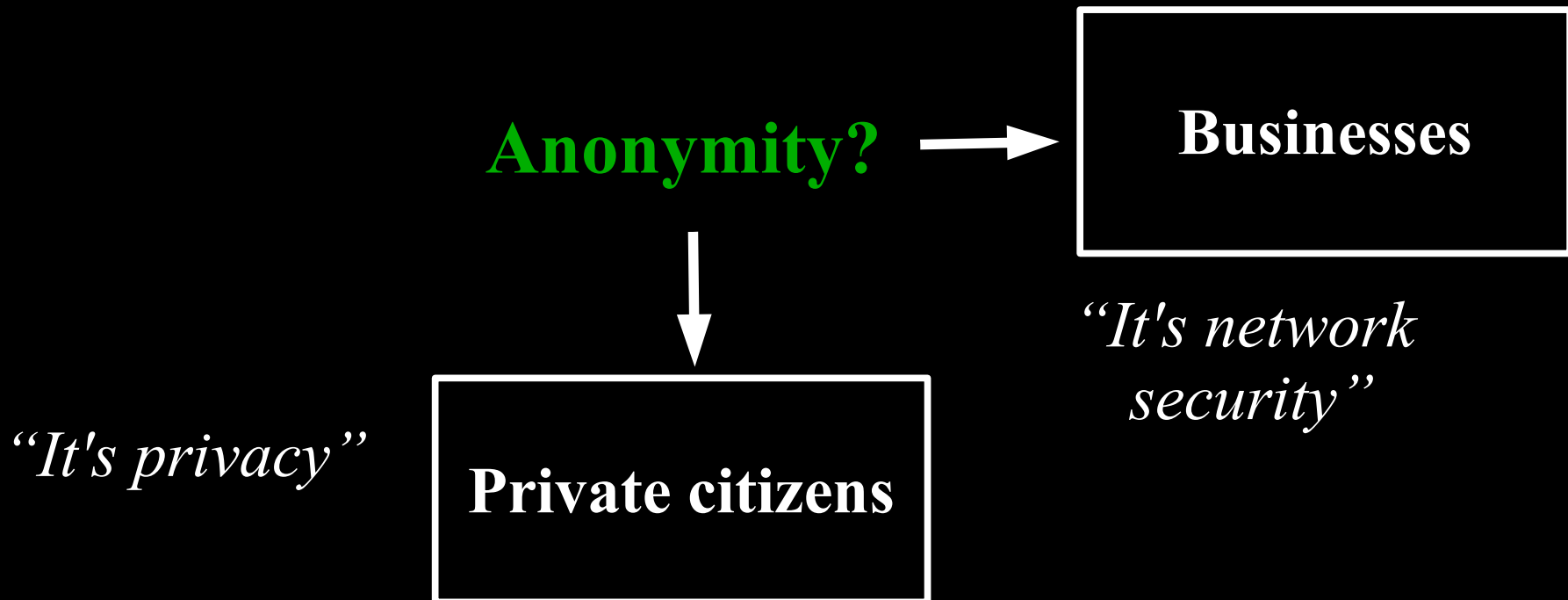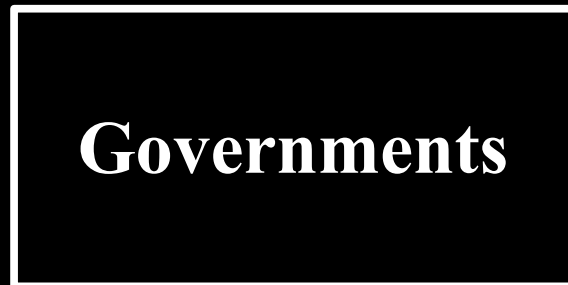# Anonymity serves different interests for different user groups

Anonymity?

$\downarrow$

"It's privacy"

Private citizens

Anonymity serves different interests for different user groups

Anonymity? → **Businesses**

↓

Private citizens

"It's privacy"

"It's network security"

6

Anonymity serves different interests for different user groups

"It's traffic-analysis resistance!"
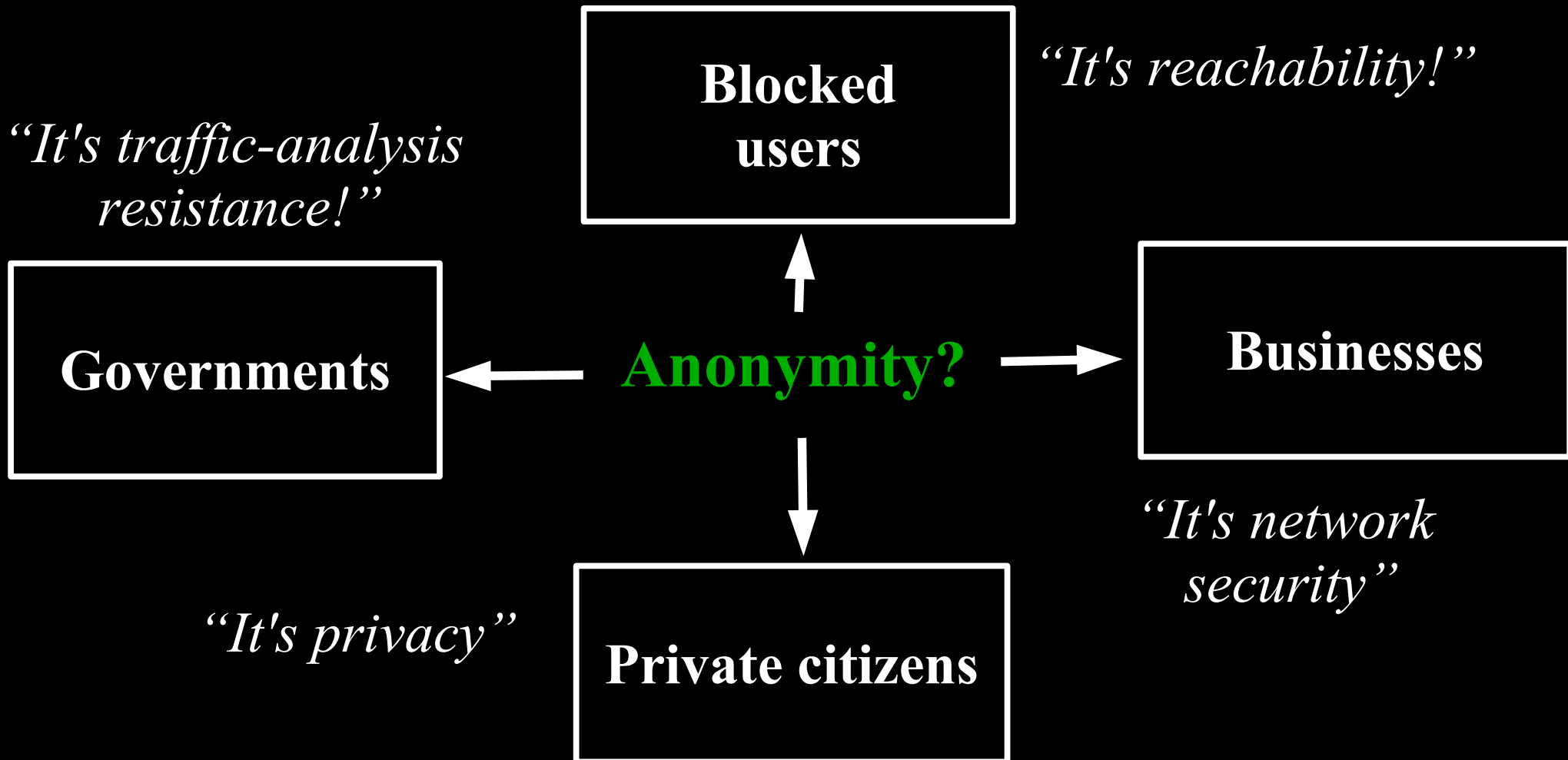
Governments ← **Anonymity?** → **Businesses**

"It's privacy"

↓

Private citizens

"It's network security"

Anonymity serves different interests for different user groups

"It's traffic-analysis resistance!"

"It's reachability!"

Blocked users

Governments ← **Anonymity?** → **Businesses**

"It's network security"

"It's privacy"

Private citizens

Encryption alone doesn't protect against traffic-analysis
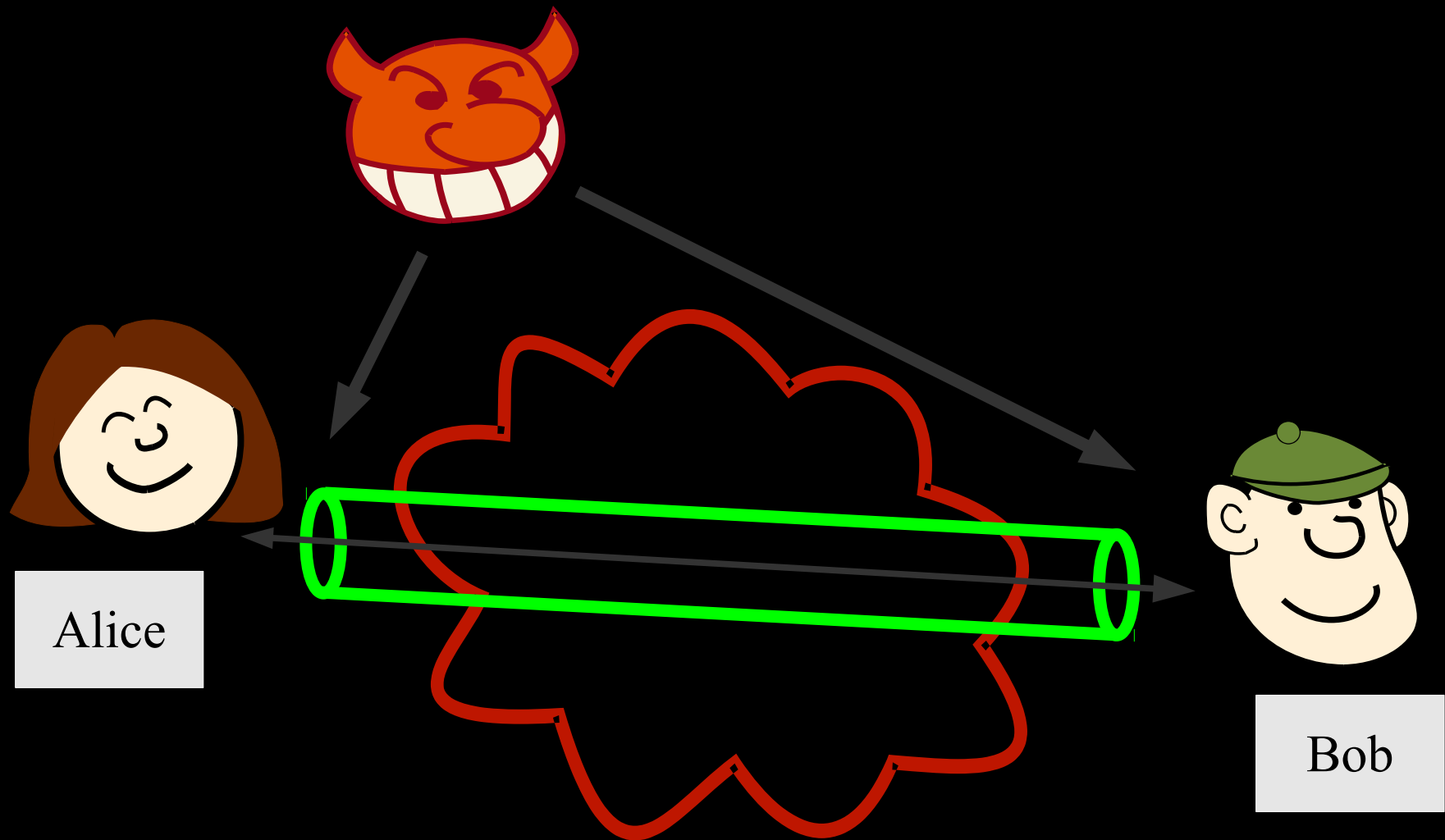
Alice

Bob

Regular citizens don't want to be watched and tracked

Sick Alice

Web serarch
Vårdguiden.se
Netdoktor.se
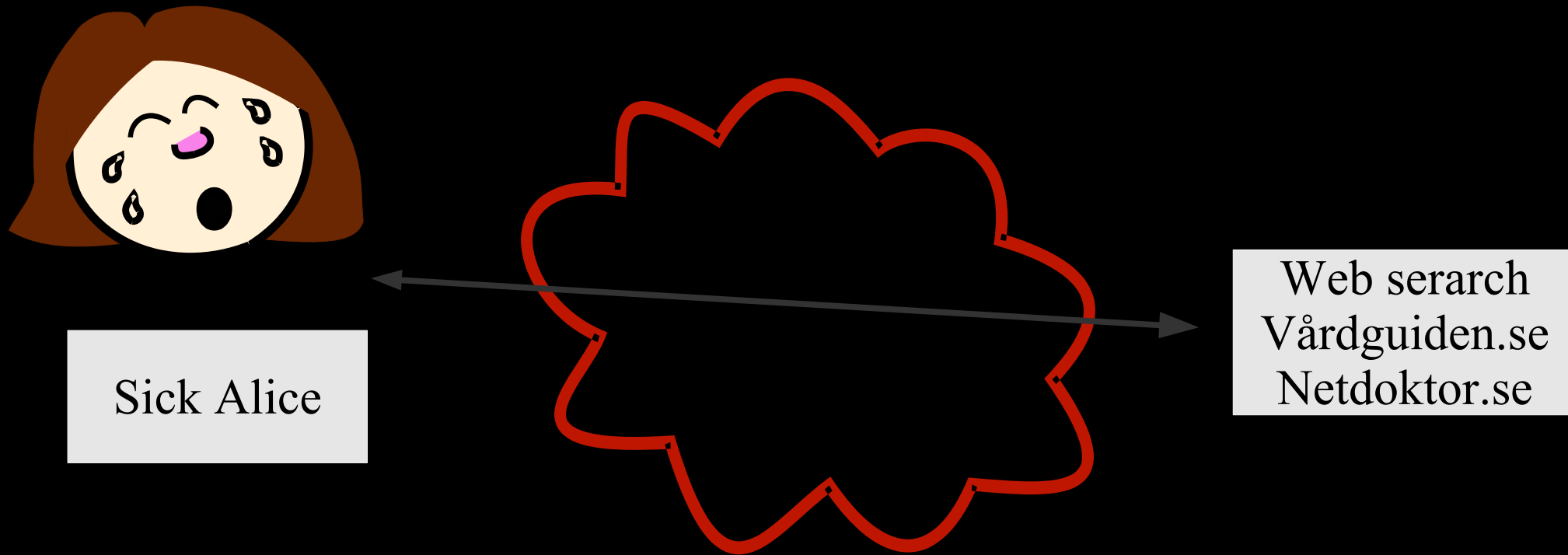
Regular citizens don't want to be watched and tracked
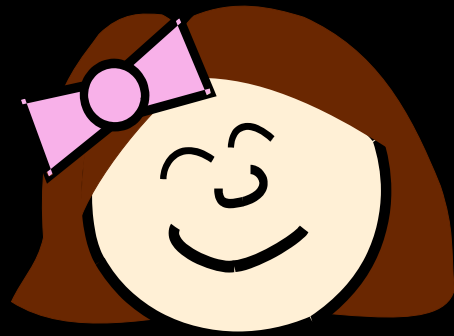
8-year-old
Alice
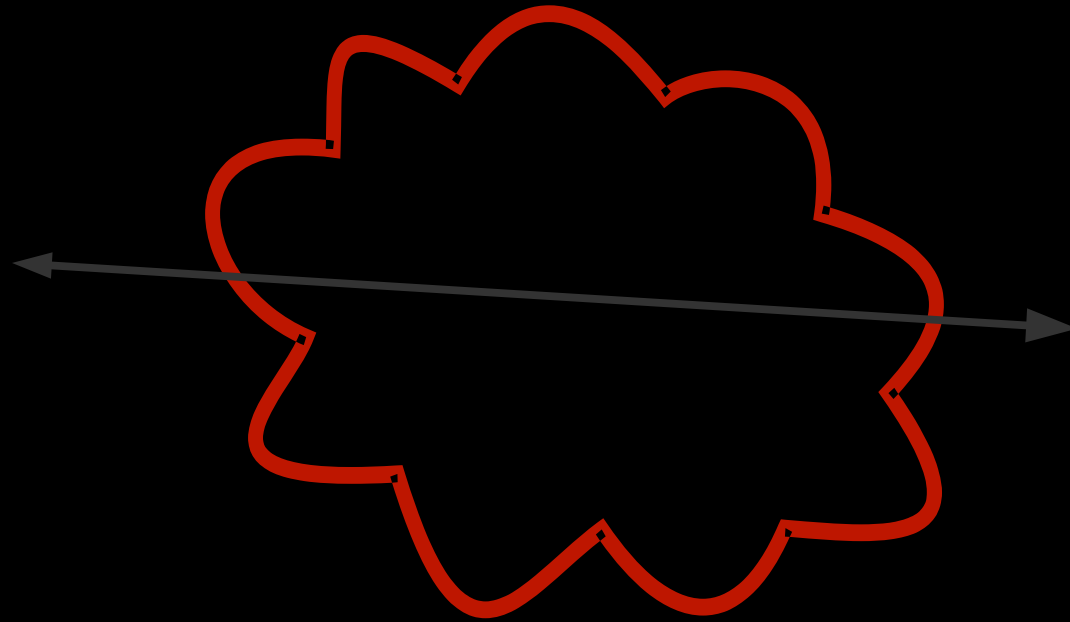
Web services
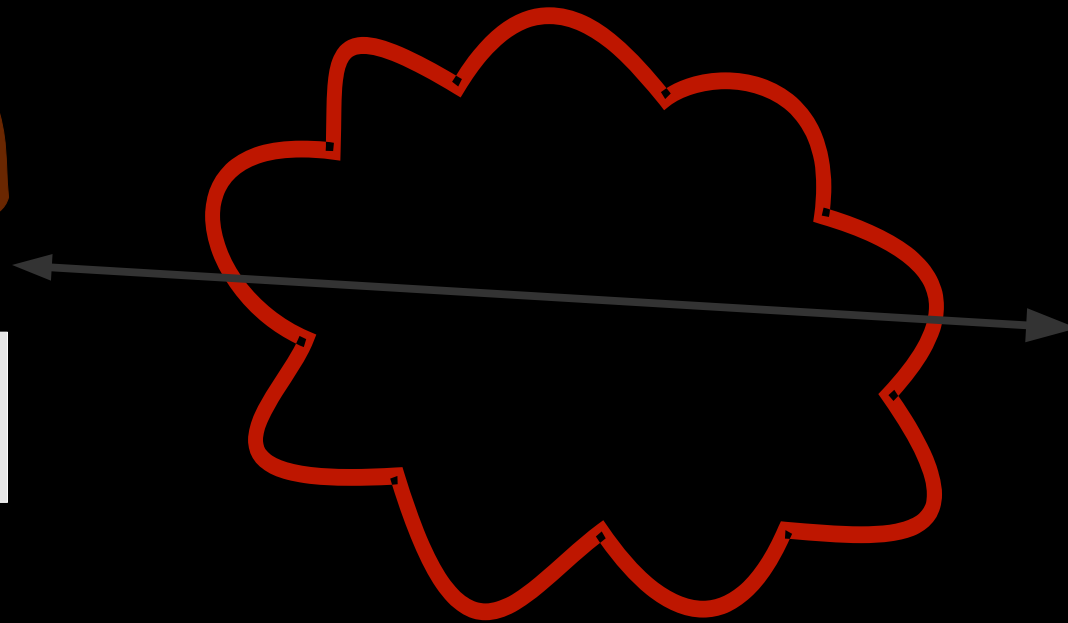
Regular citizens don't want to be watched and tracked
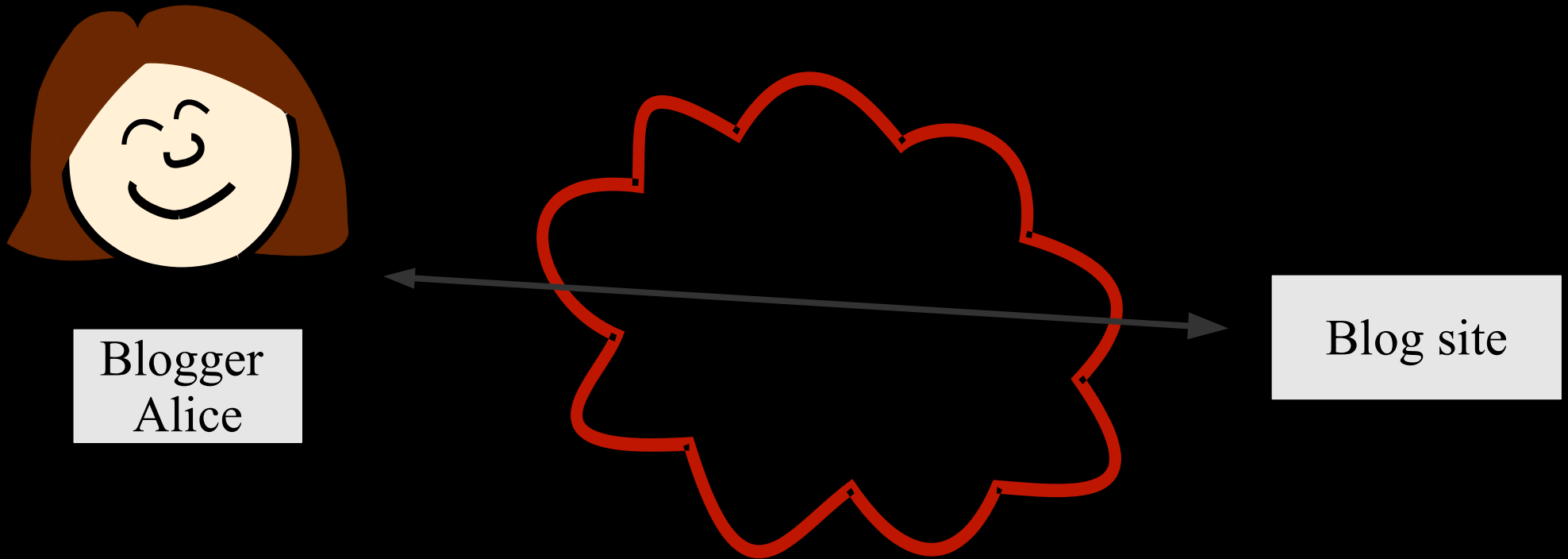
Blogger Alice

Blog site

Regular citizens don't want to be watched and tracked

Employed Alice

Web search
Vårdguiden.se
Netdoktor.se
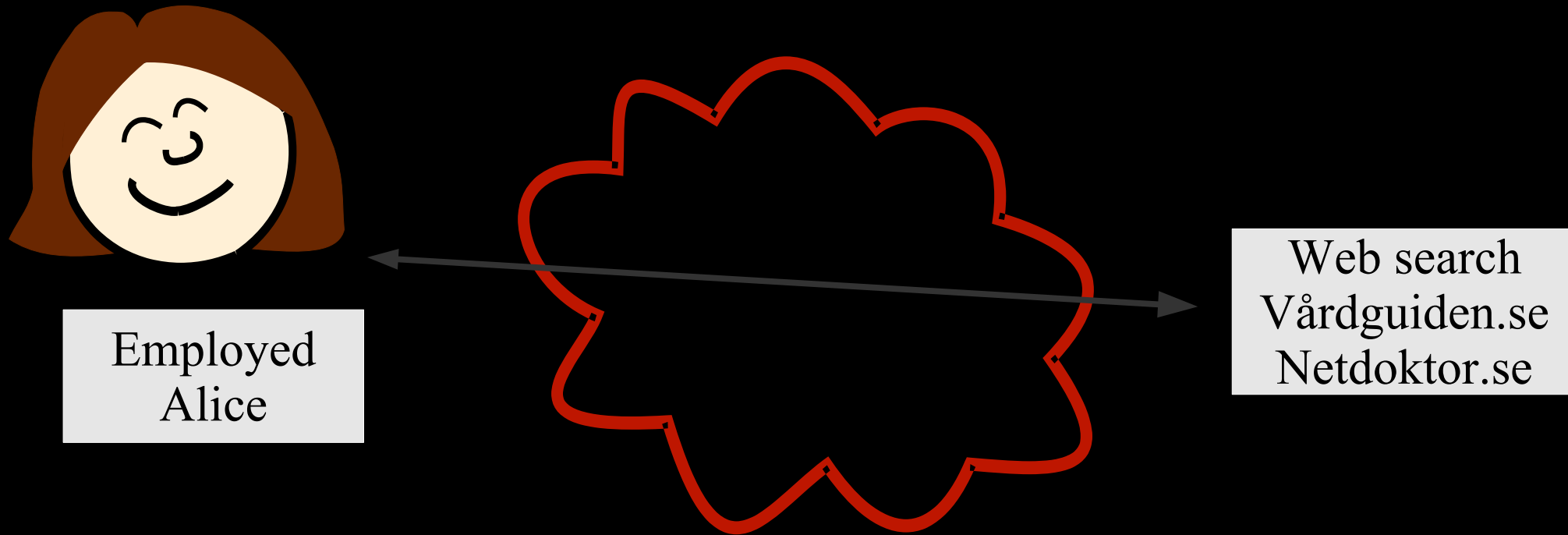
Regular citizens don't want to be watched and tracked
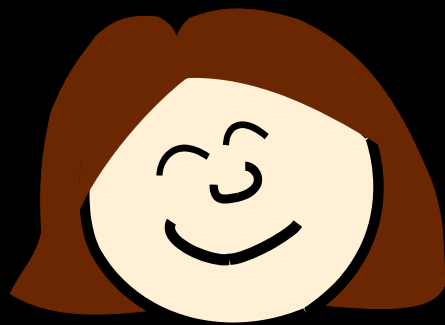
Consumer
Alice

Amazon.com
Cdon.se
Bokus.com
Prisjakt.nu
Pricerunner.se
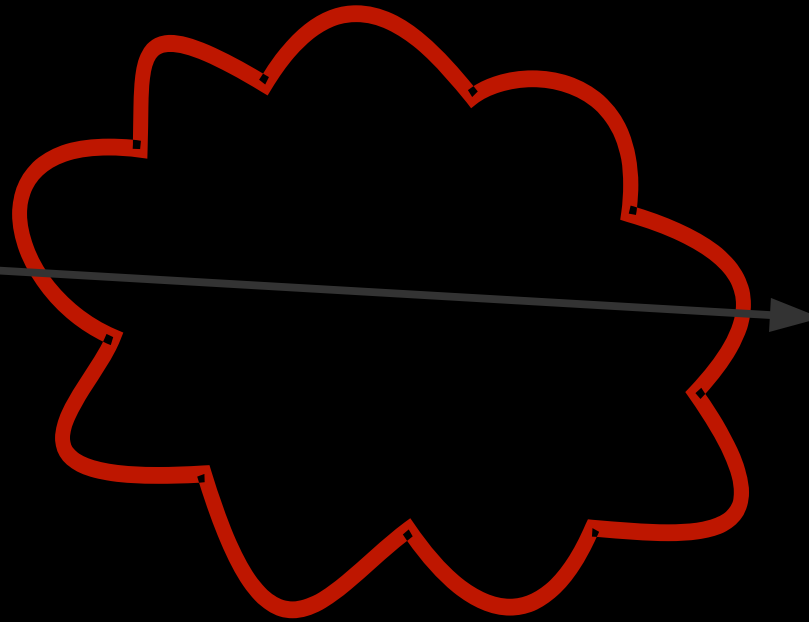
Business need to keep trade secrets
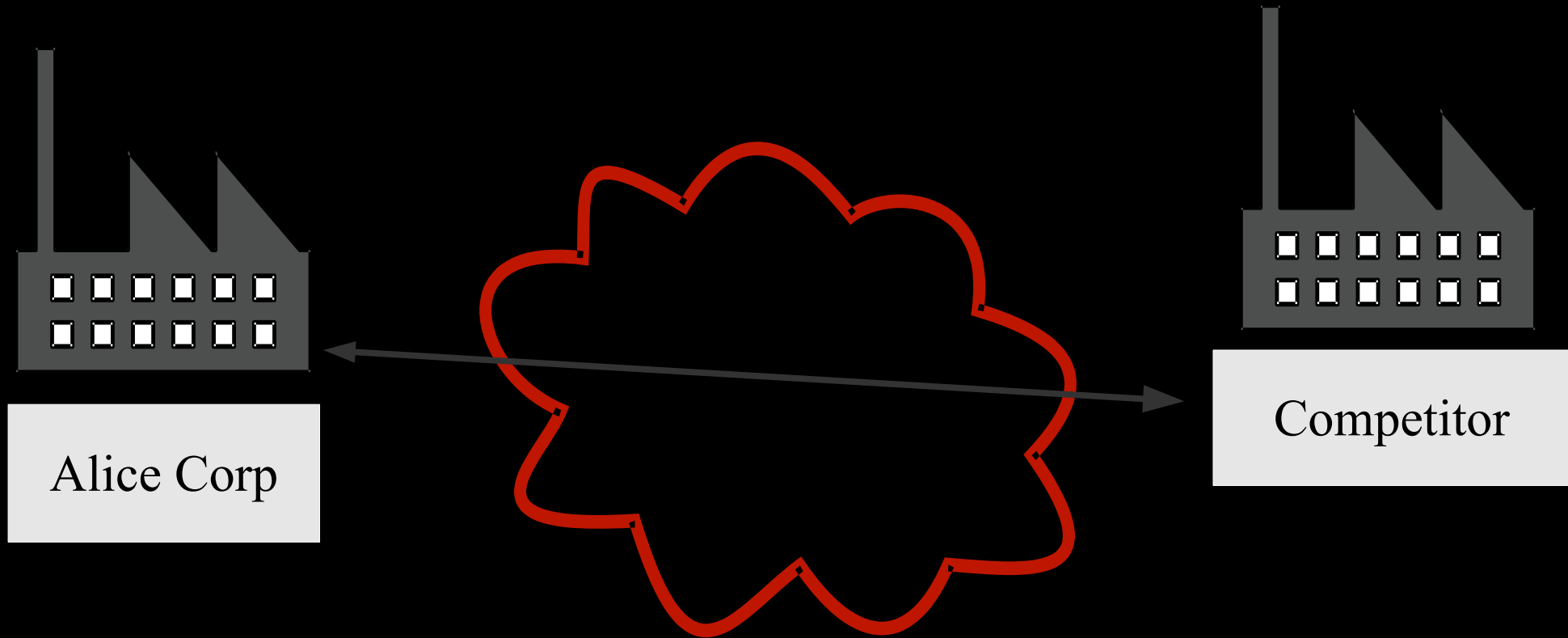
Alice Corp

Competitor

Business need to keep trade secrets

Alice Corp

Web search
Suppliers
Customers
Media
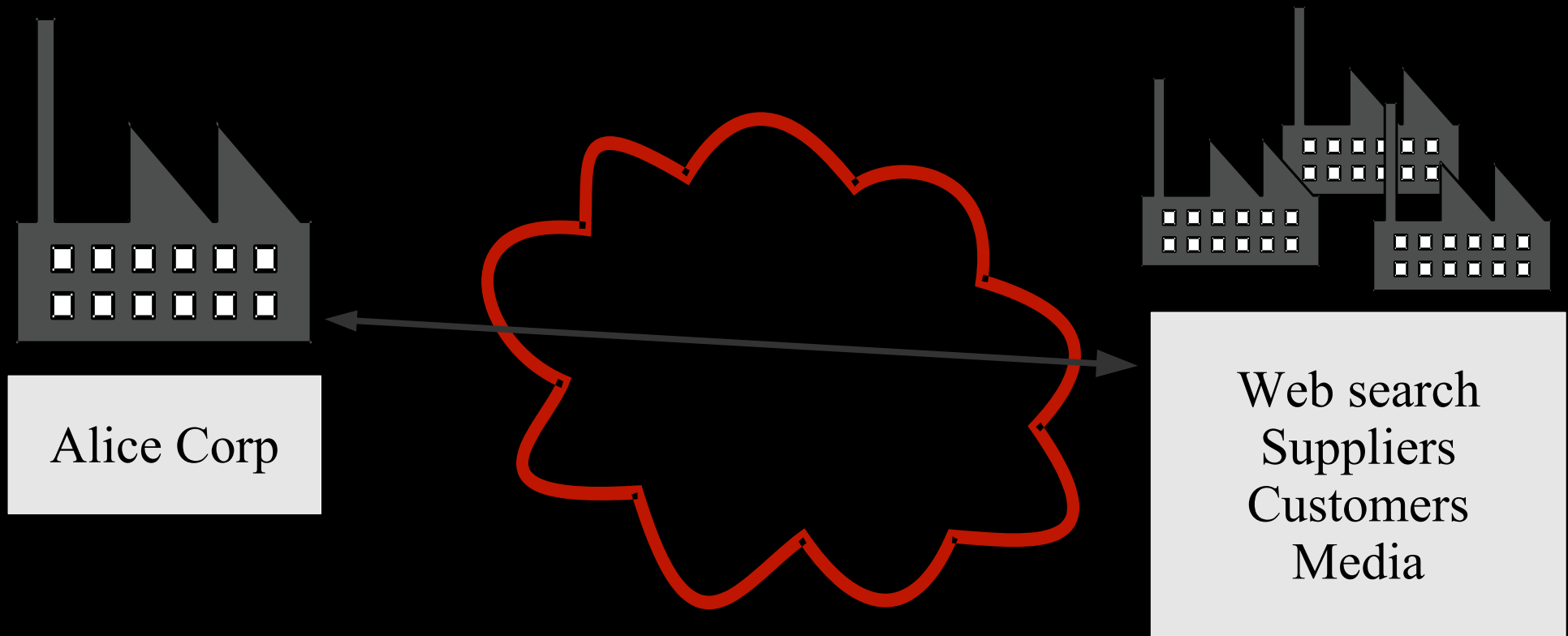
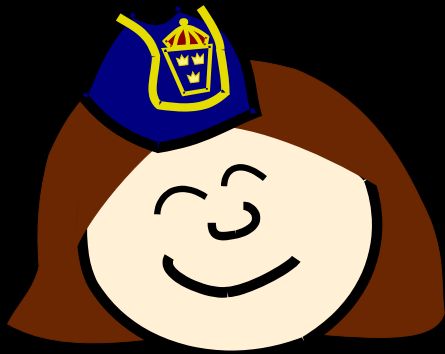# Law enforcement needs anonymity to get the job done
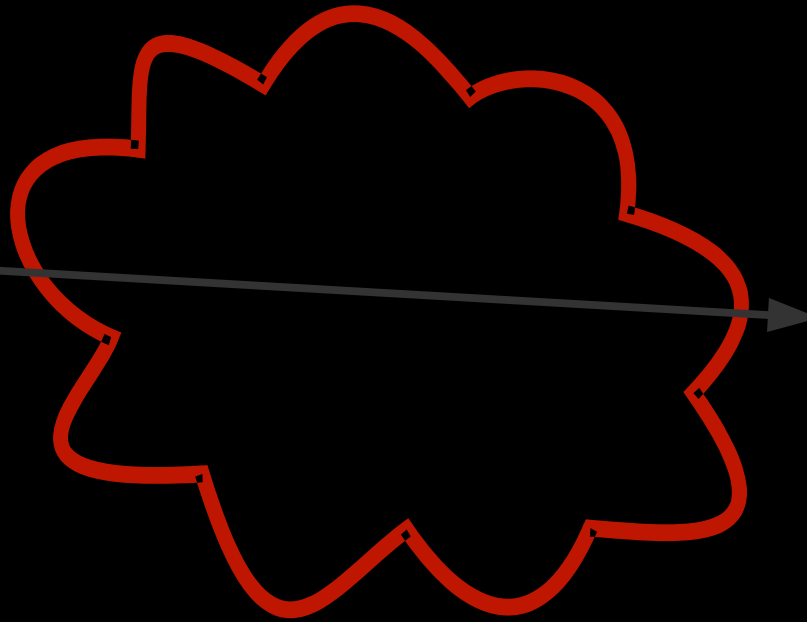
Police Alice

Suspected Bob

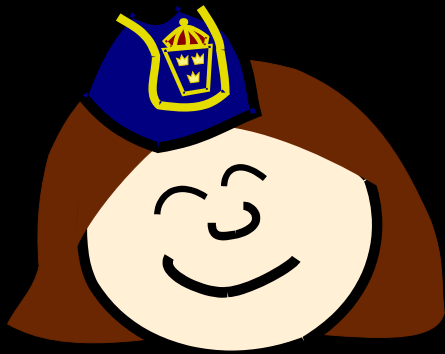# Law enforcement needs anonymity to get the job done
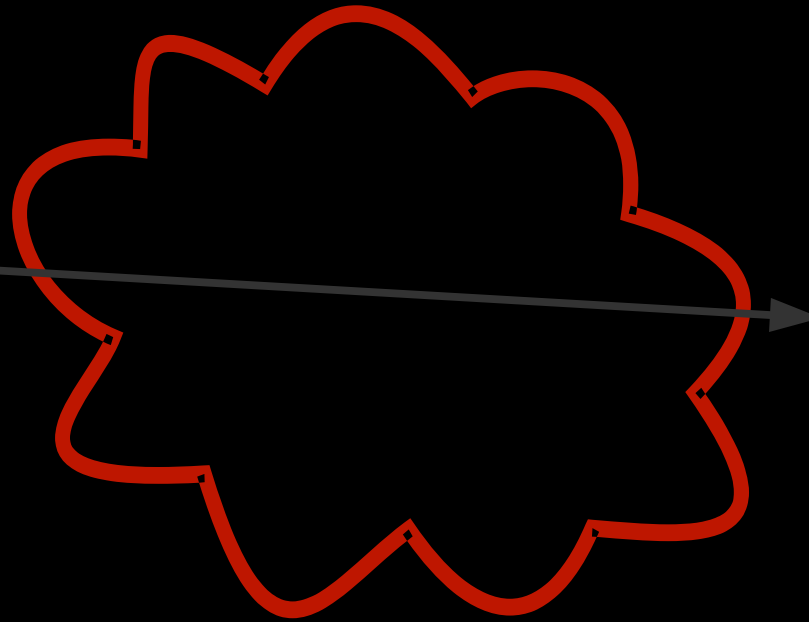

Police
Alice

Bob, selling
illegal drugs

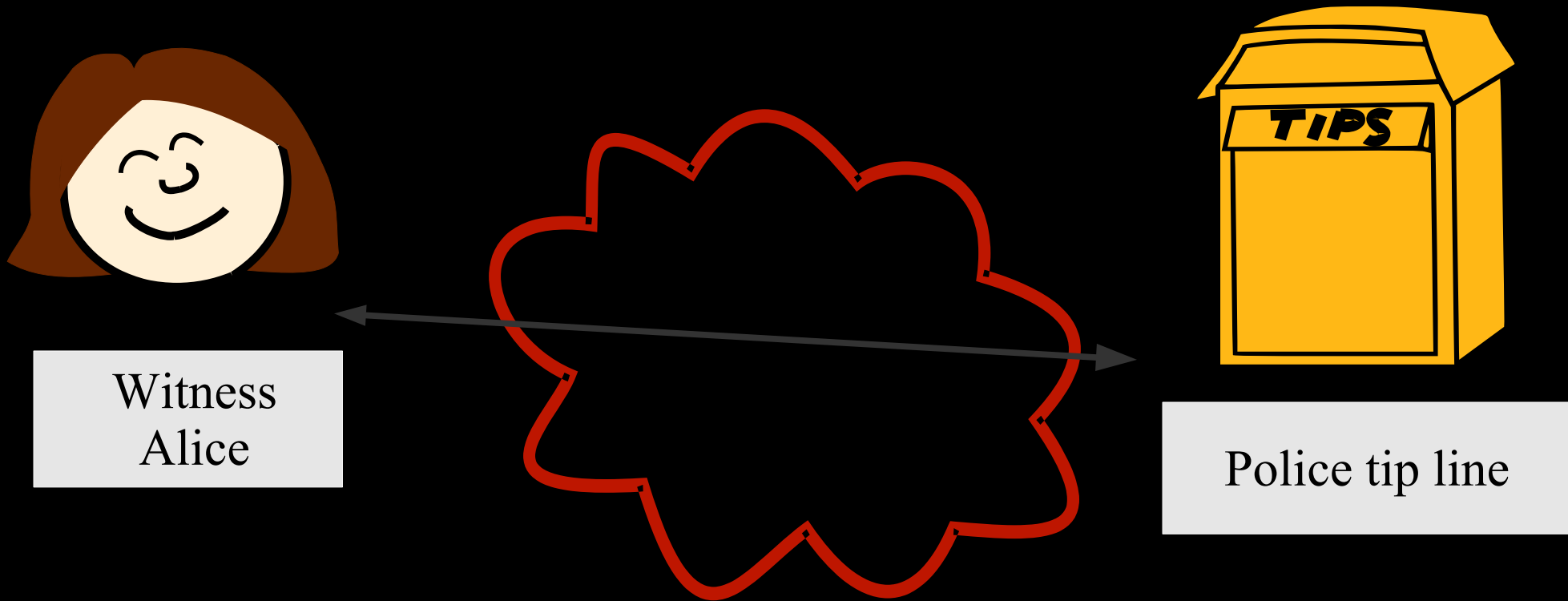# Law enforcement needs anonymity to get the job done
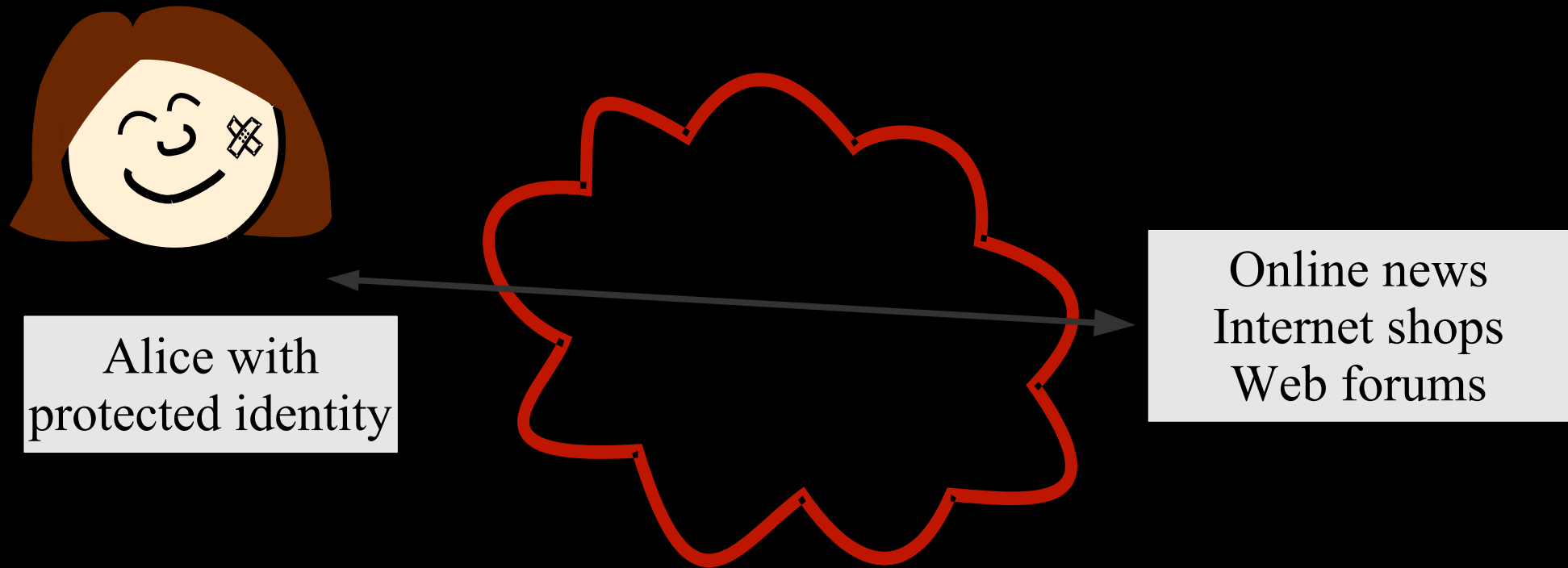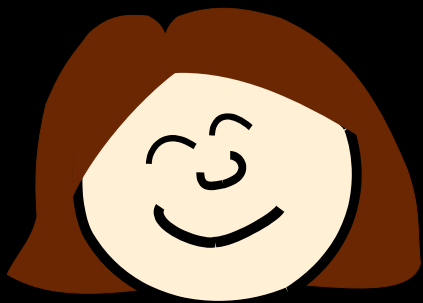
Police
Alice

Bob Corleone
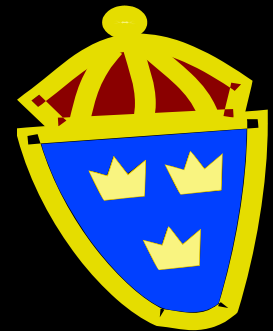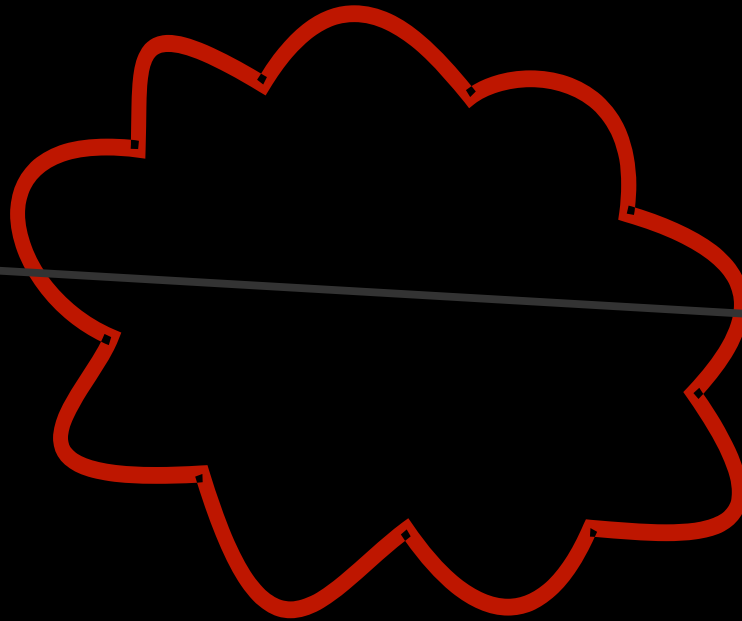
Law enforcement needs anonymity to get the job done

Witness
Alice

TIPS

Police tip line

Law enforcement needs anonymity to get the job done

Alice with protected identity

Online news
Internet shops
Web forums

Governments need anonymity for their security

Ambassador Alice abroad

Foreign ministry at home

Governments need anonymity for their security

Agent Alice

Defence agency
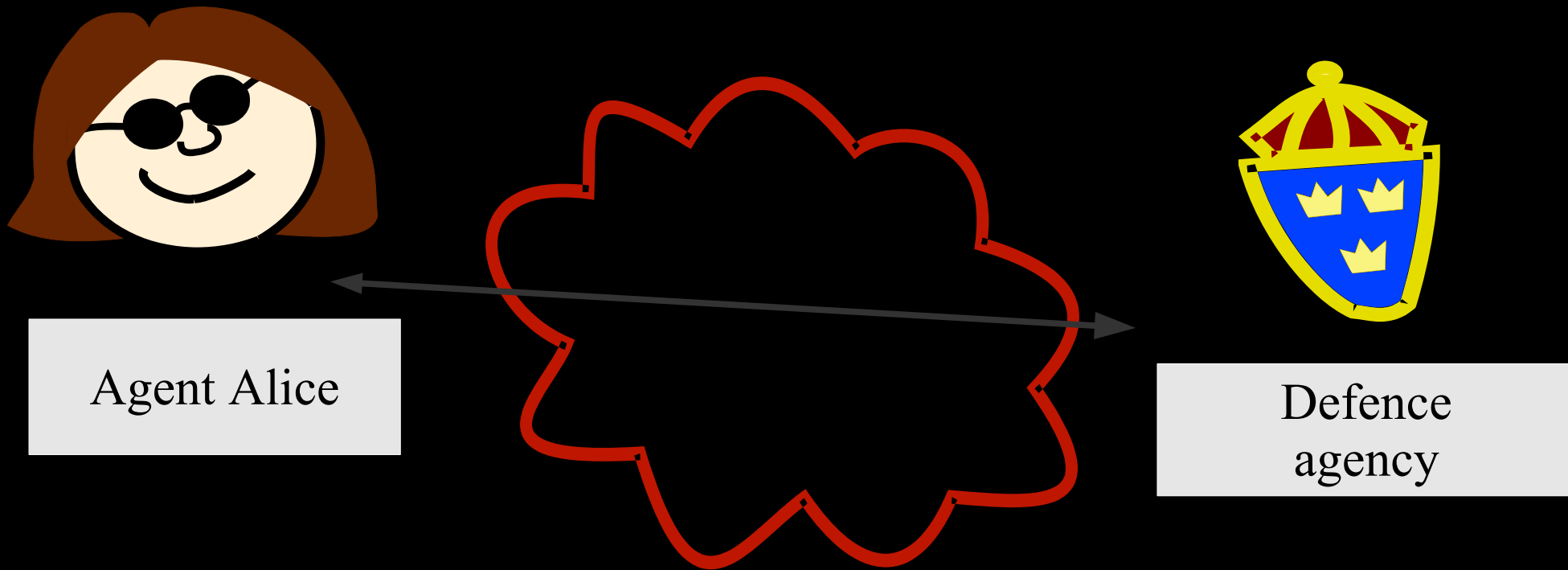
Journalists and their sources need Tor for their personal safety
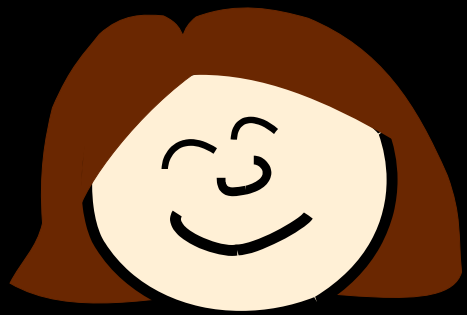
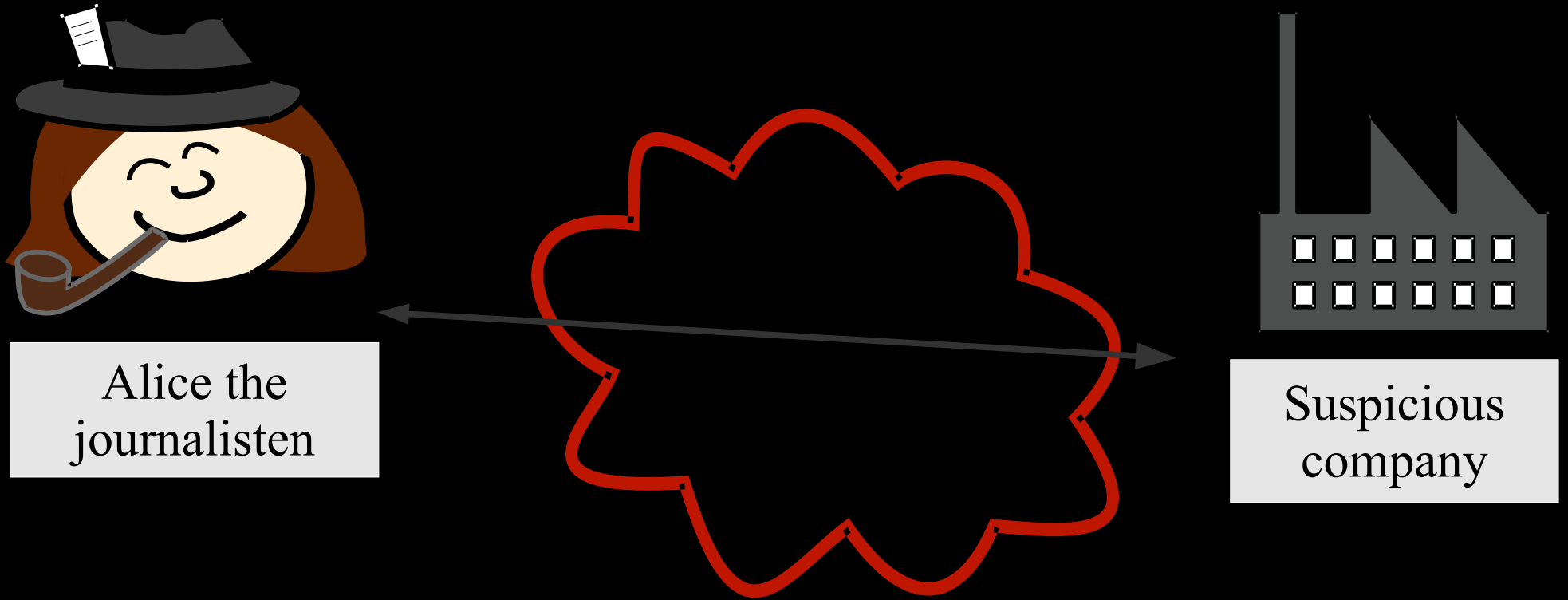
Alice the source

Bob the journalist

Journalists and their sources need Tor for their personal safety
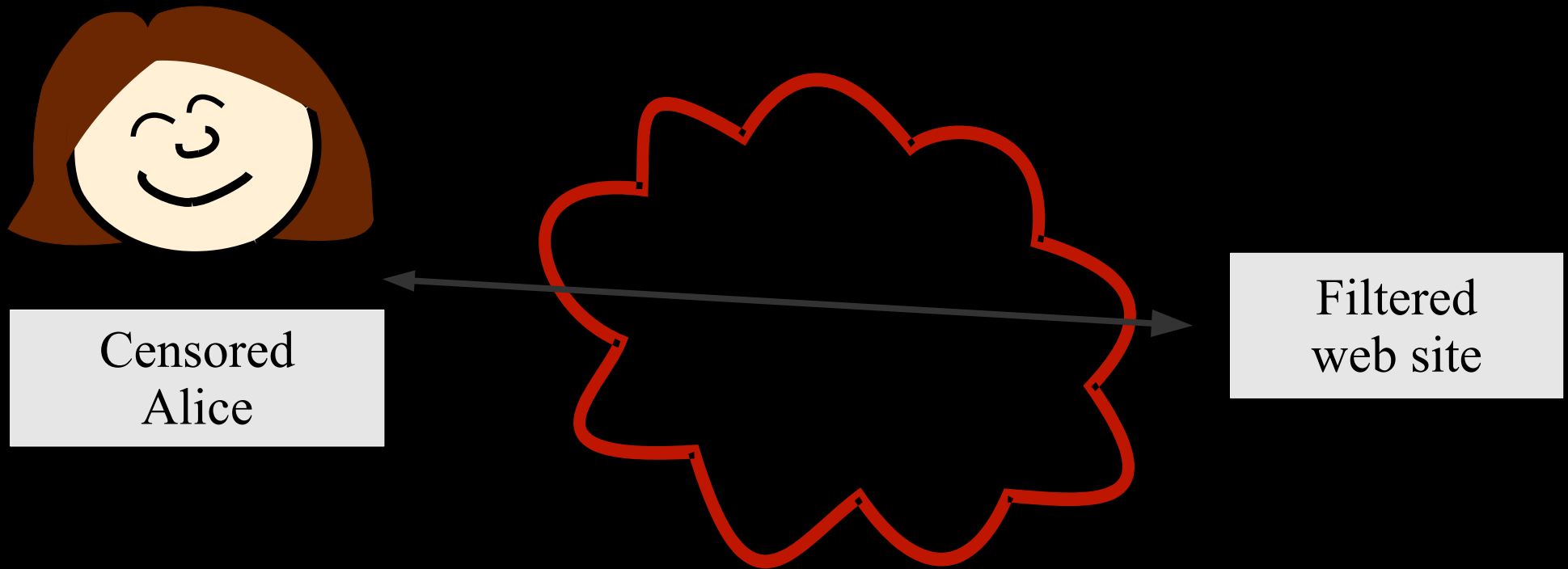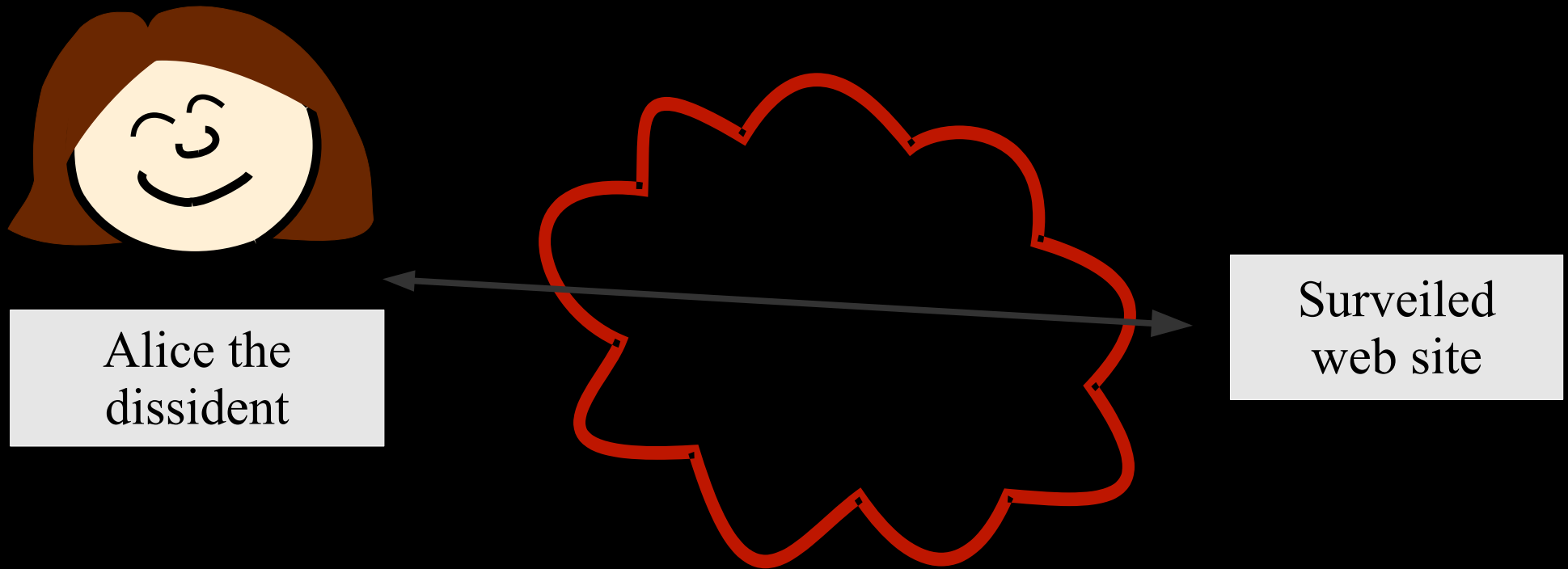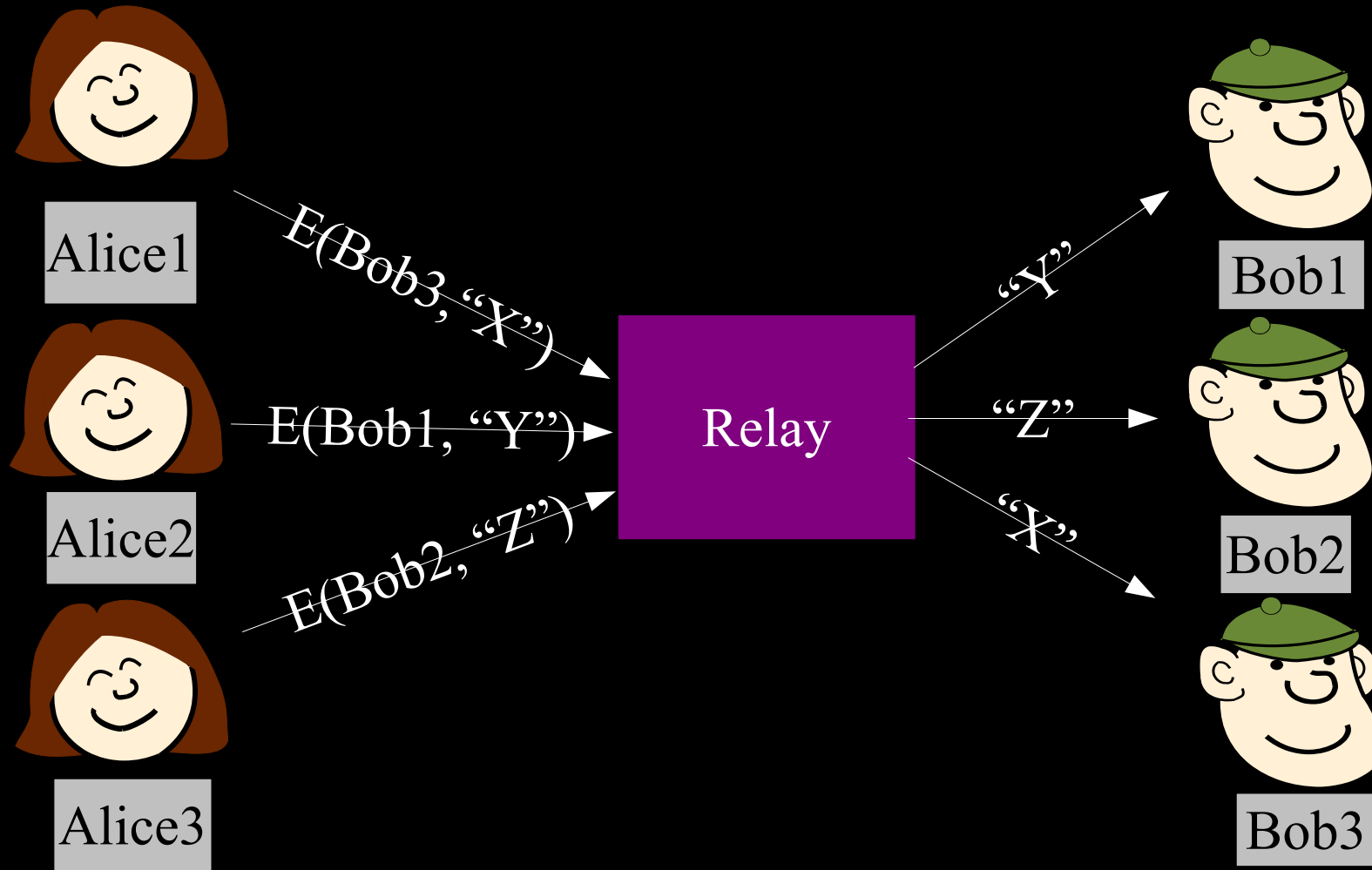
Alice the journalisten

Suspicious company

Journalists and their sources need Tor for their personal safety

Journalists and their sources need Tor for their personal safety

Alice the dissident

Surveiled web site
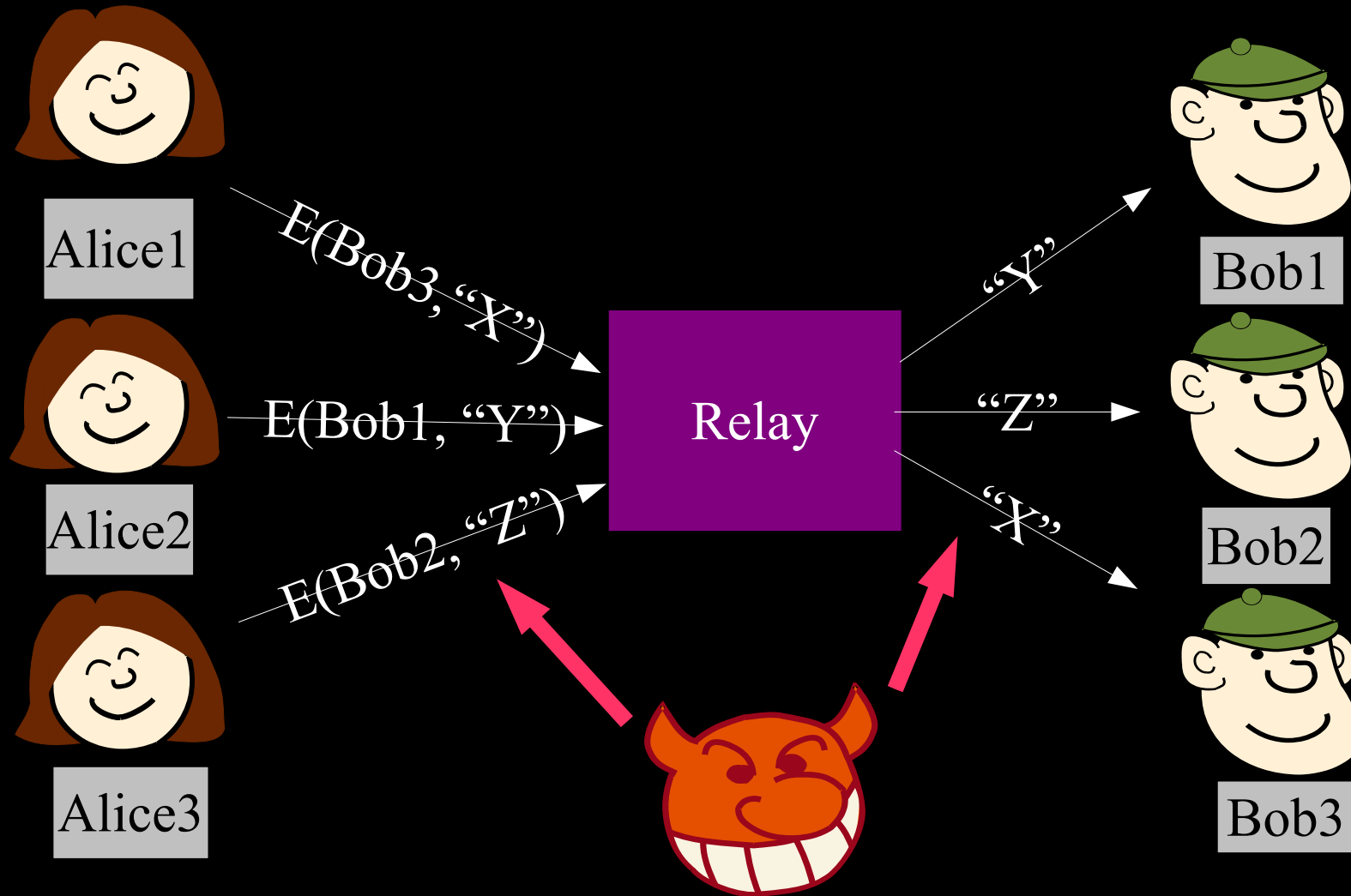
The simpler systems use only one relay

Alice1

Alice2

Alice3

E(Bob3, "X")

E(Bob1, "Y")

E(Bob2, "Z")

Relay

"Y"

"Z"

"X"

Bob1

Bob2

Bob3

(For example relax.se, dold.se and ipredator.se)

The simpler systems put all the eggs in the same basket

Alice1 — E(Bob3, "X") →

Alice2 — E(Bob1, "Y") →

Alice3 — E(Bob2, "Z") →

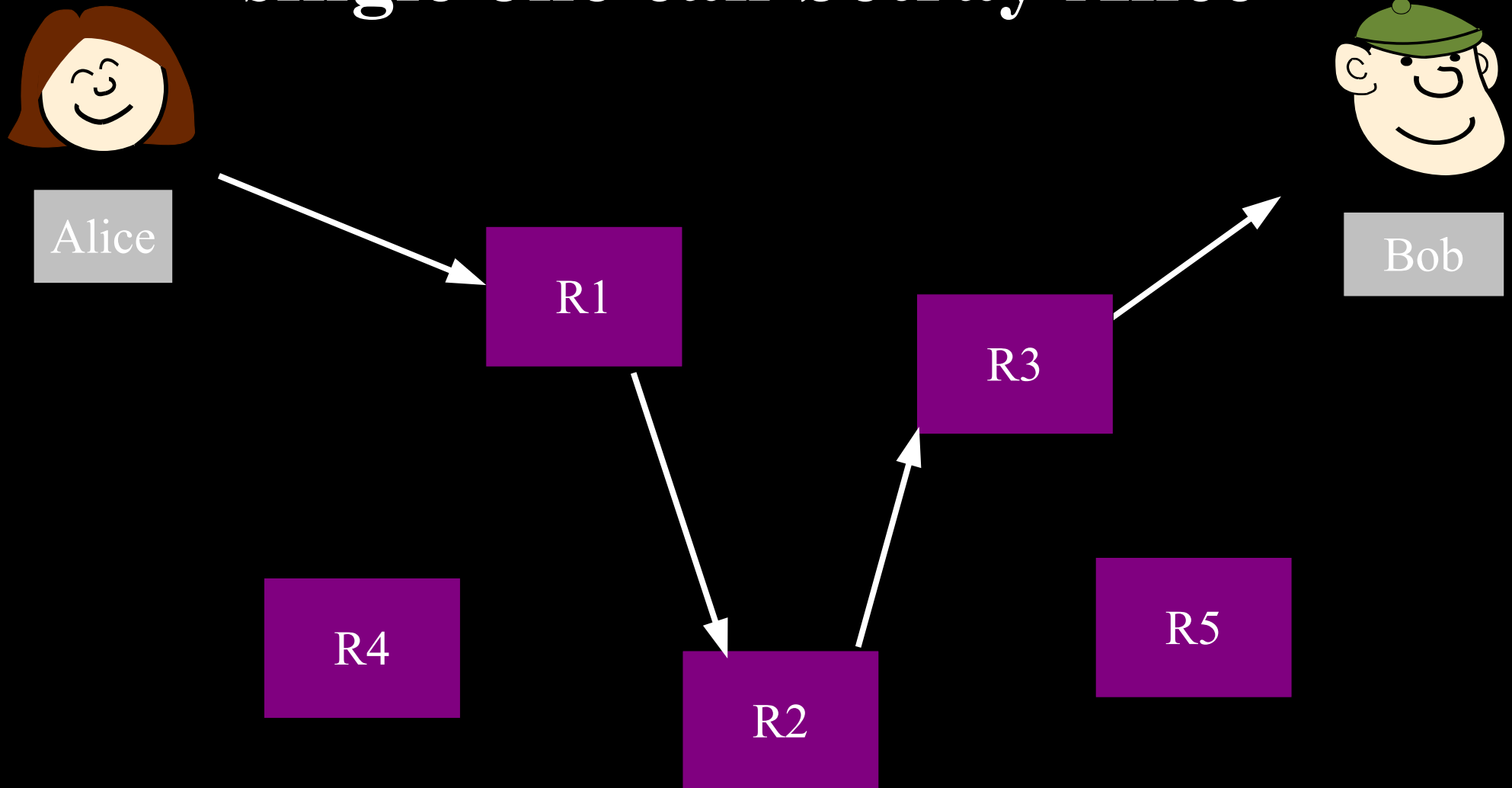"Y" → Bob1

"Z" → Bob2

"X" → Bob3

A single relay is also an attractive target
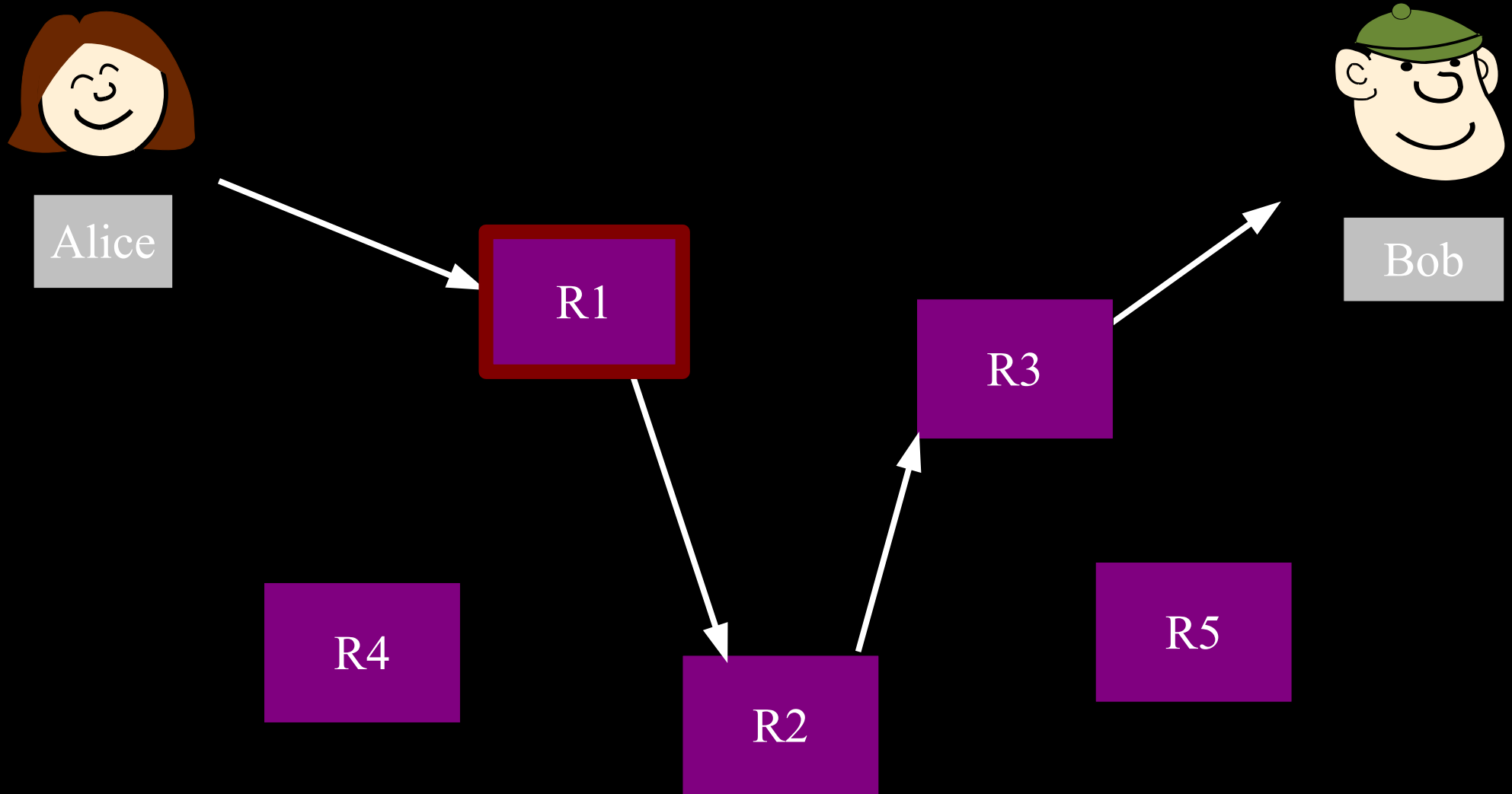

Trafic and timing analysis will reveal which Alice is talking to which Bob.
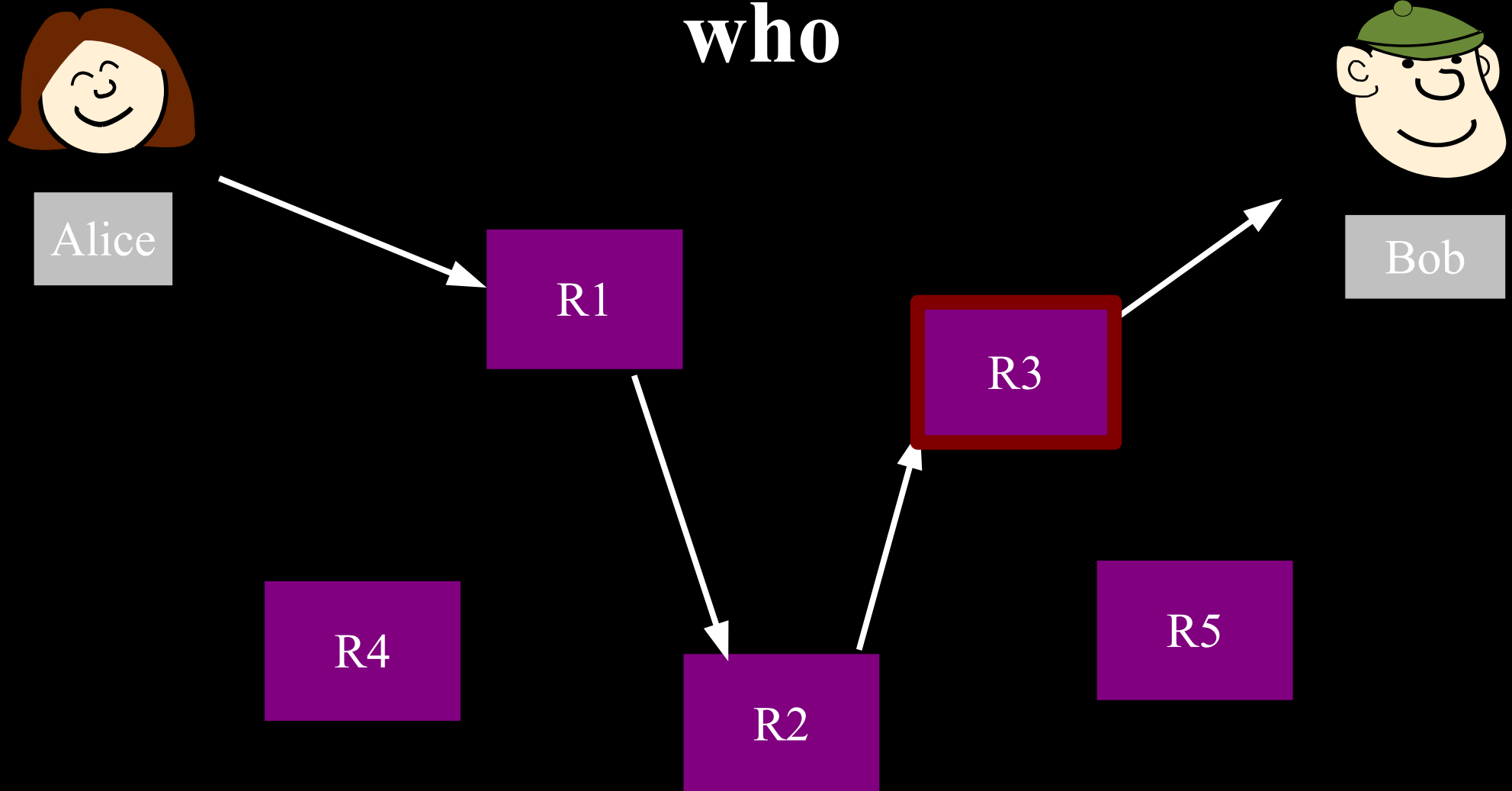
So, add multiple relays so that no single one can betray Alice
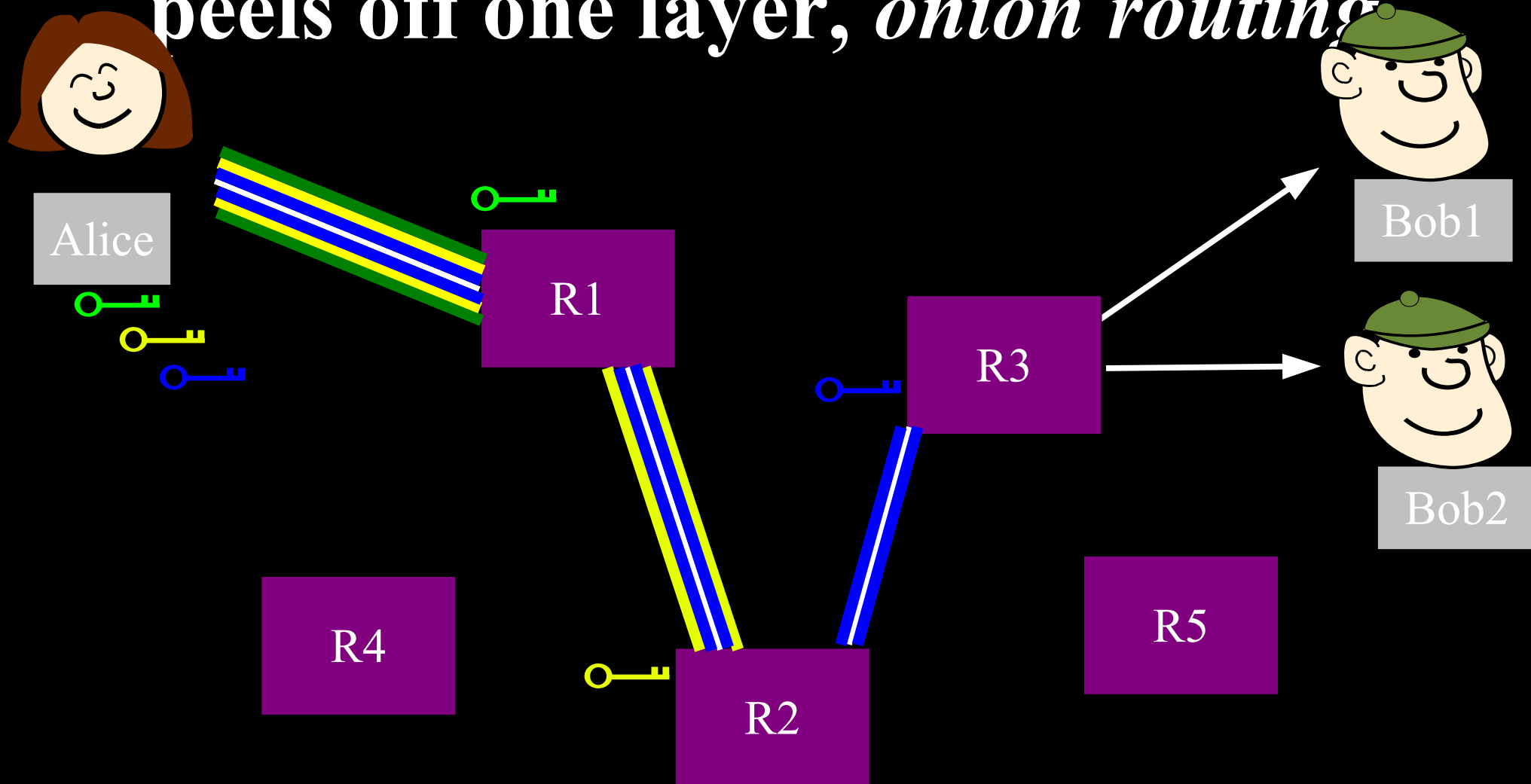

31

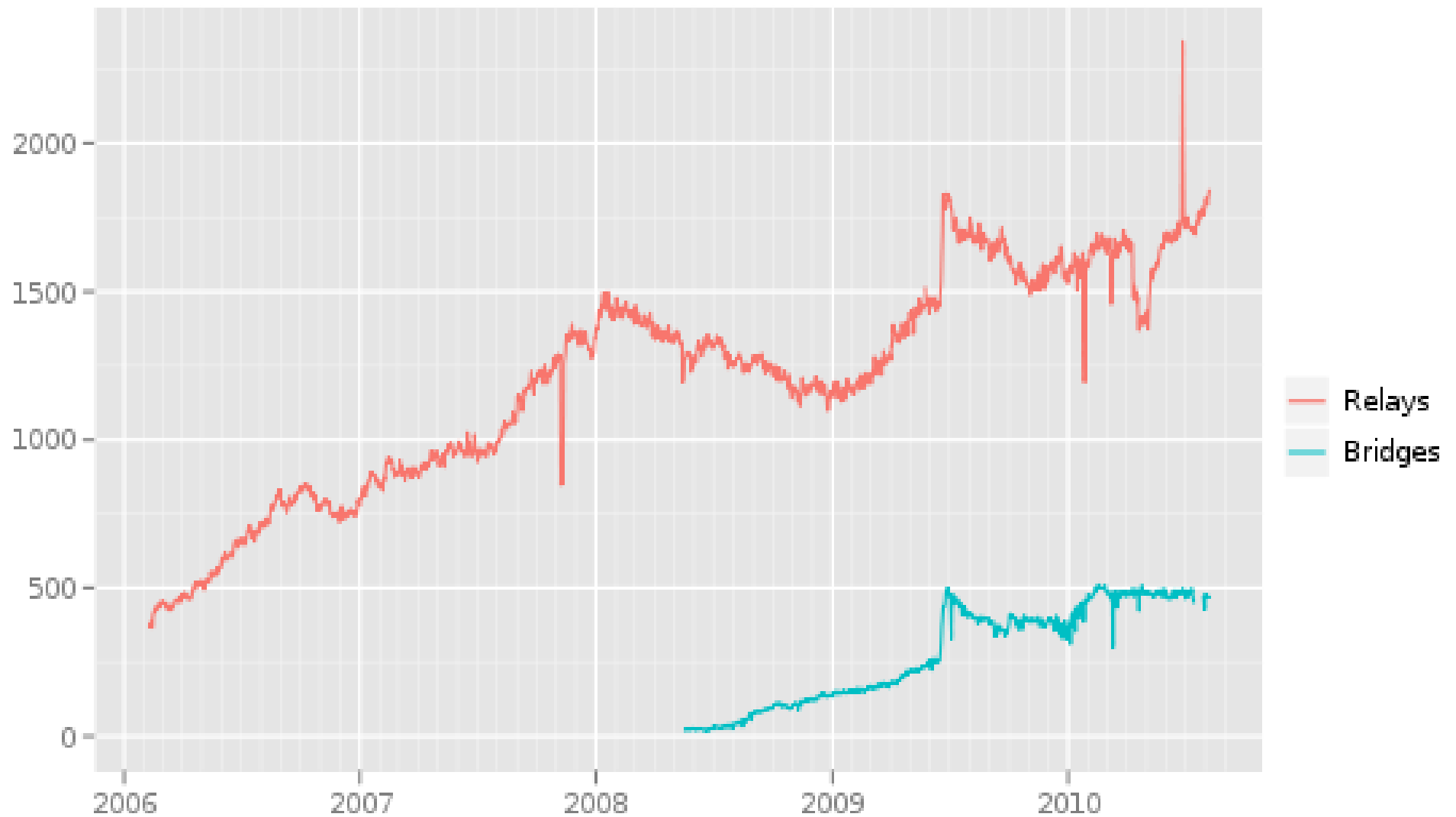# A corrupt first hop can tell that Alice is talking, but not to whom

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

The first hop is protected by three layers of encryption, then each hop peels off one layer, *onion routing*
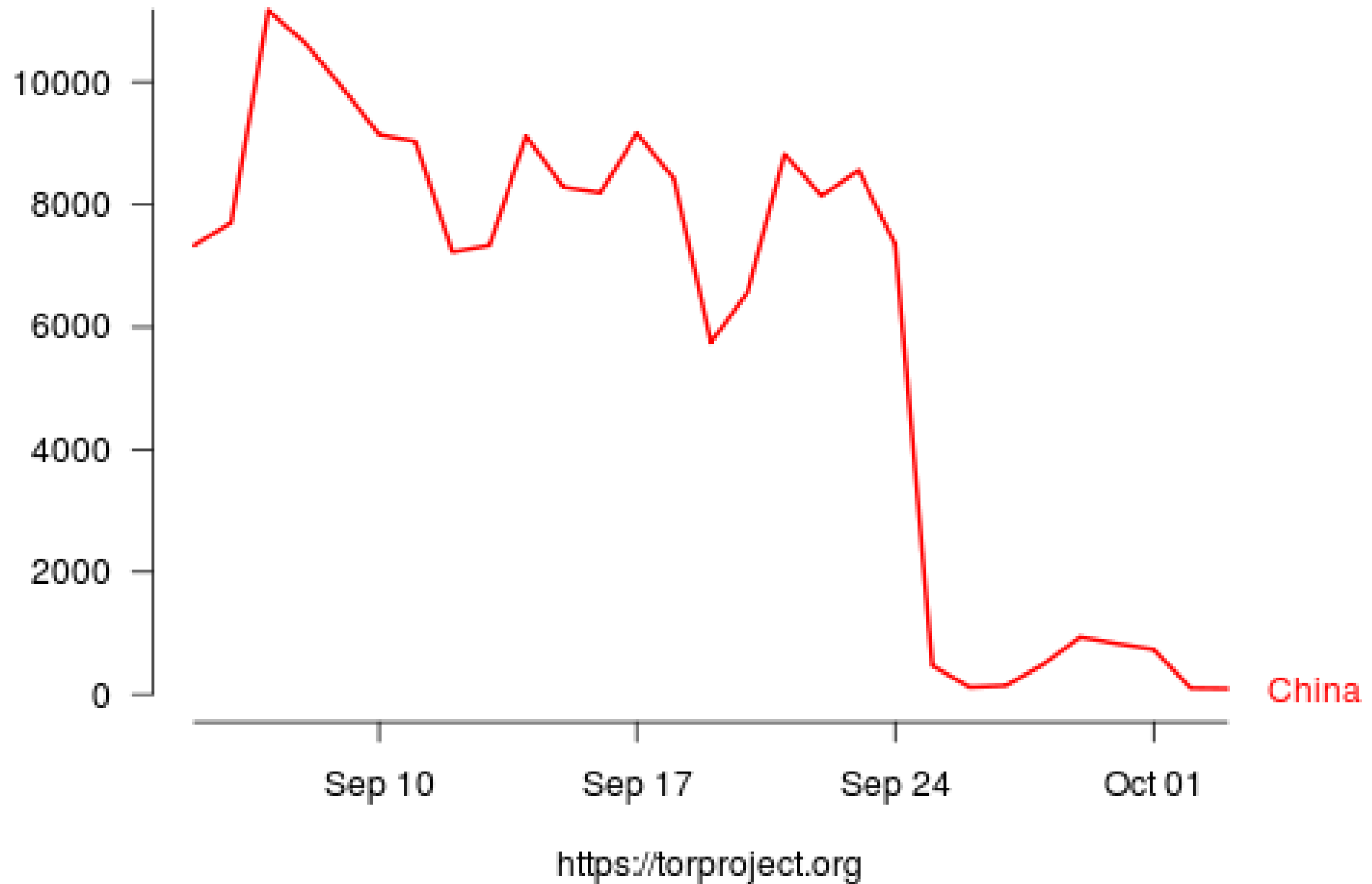

34

Number of relays and bridges (all data)

The Tor Project - https://metrics.torproject.org/

Number of directory requests to directory mirror trusted

https://torproject.org

36

Chinese Tor users via bridges

37