



Learn how to browse the internet privately

Lead Dev: Sean McGregor @seanmcgregor
Community Manager: Jen Davidson @jewifer

@privly 

Thanks to Flux!

Feminist Hackerspace

<http://fluxlab.io>

Code of Conduct

How to get on the wifi

TorProject for Putting Slides Online

What is TA3M?

- Techno-Activism Third Mondays (TA3M) is an informal meetup designed to connect software creators and activists who are interested in censorship, surveillance, and open technology. Currently, TA3M are held in 16 cities throughout the world, with many more launching in the near the future.

10 Minutes of Announcements and Current Events

Do you have a current event related to privacy, security, surveillance, censorship that they'd like to share (2 minutes or less)?

- Start with your name (or not)
- What happened?
- What do you think about it?



Quick Poll

- What is your background?
 - Developer?
 - Journalist?
 - Security?
 - Human Being?

What does it mean to “browse the internet privately”?

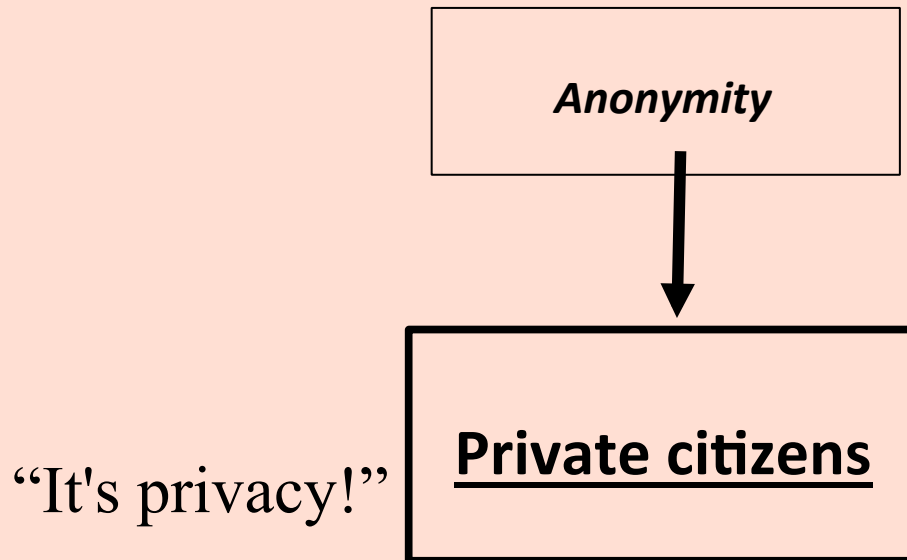
- Your identity will not be tied to the sites you access.
- Anonymous Browsing is NOT encryption!

panopticklick.eff.org

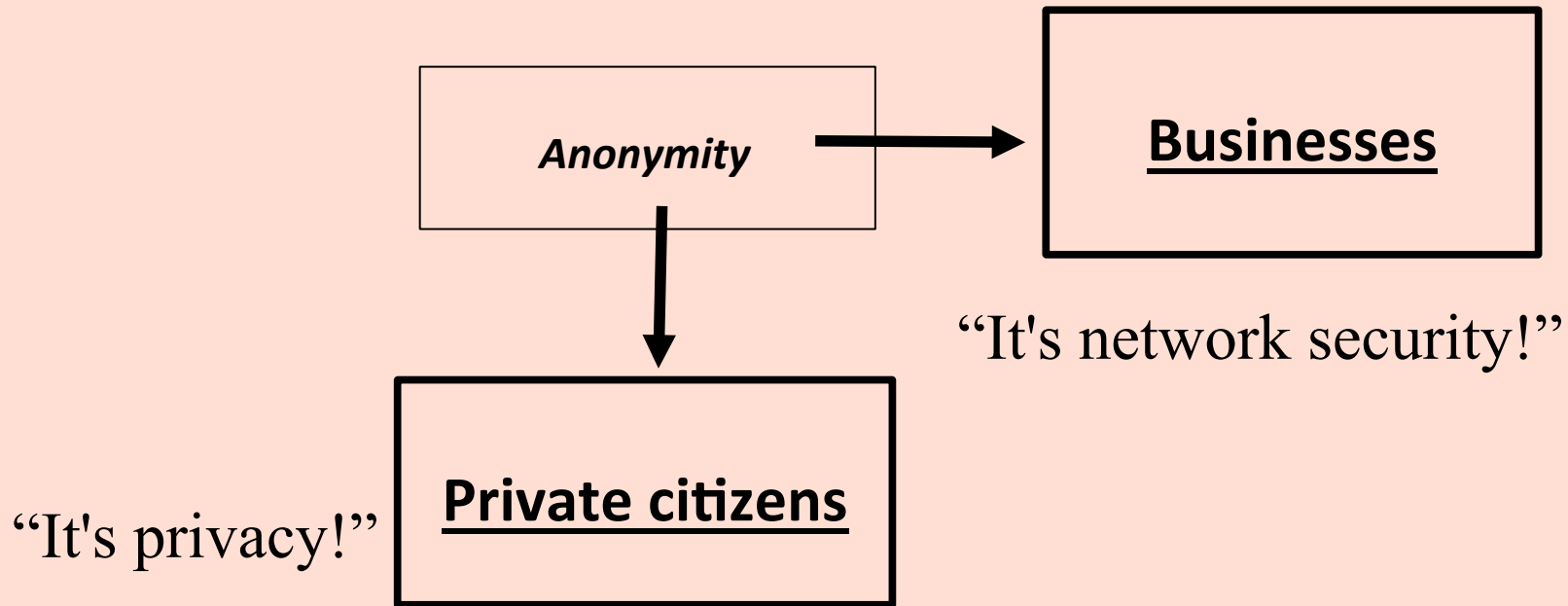
Why would I want to browse the internet privately?

- This depends on who you are.

Anonymity serves different interests for different user groups.

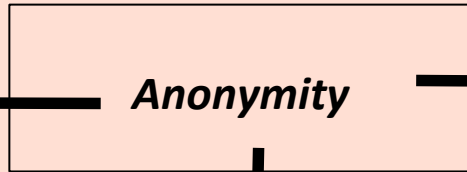
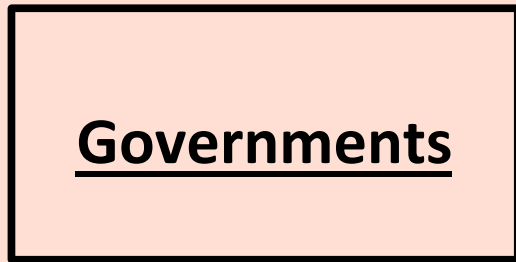


Anonymity serves different interests for different user groups.



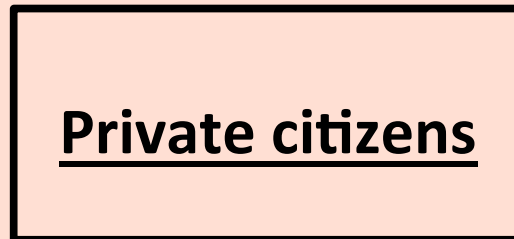
Anonymity serves different interests for different user groups.

“It's traffic-analysis resistance!”

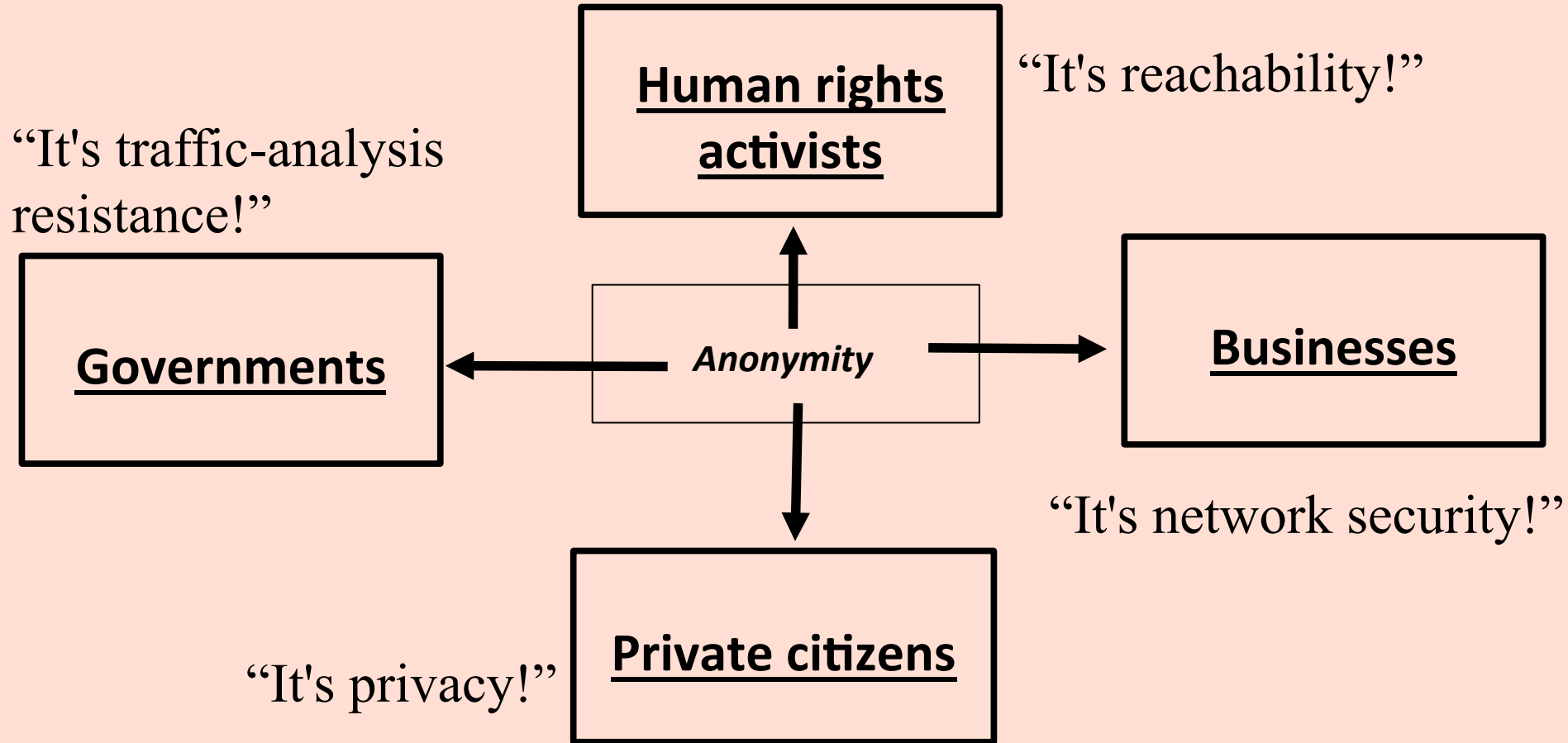


“It's network security!”

“It's privacy!”

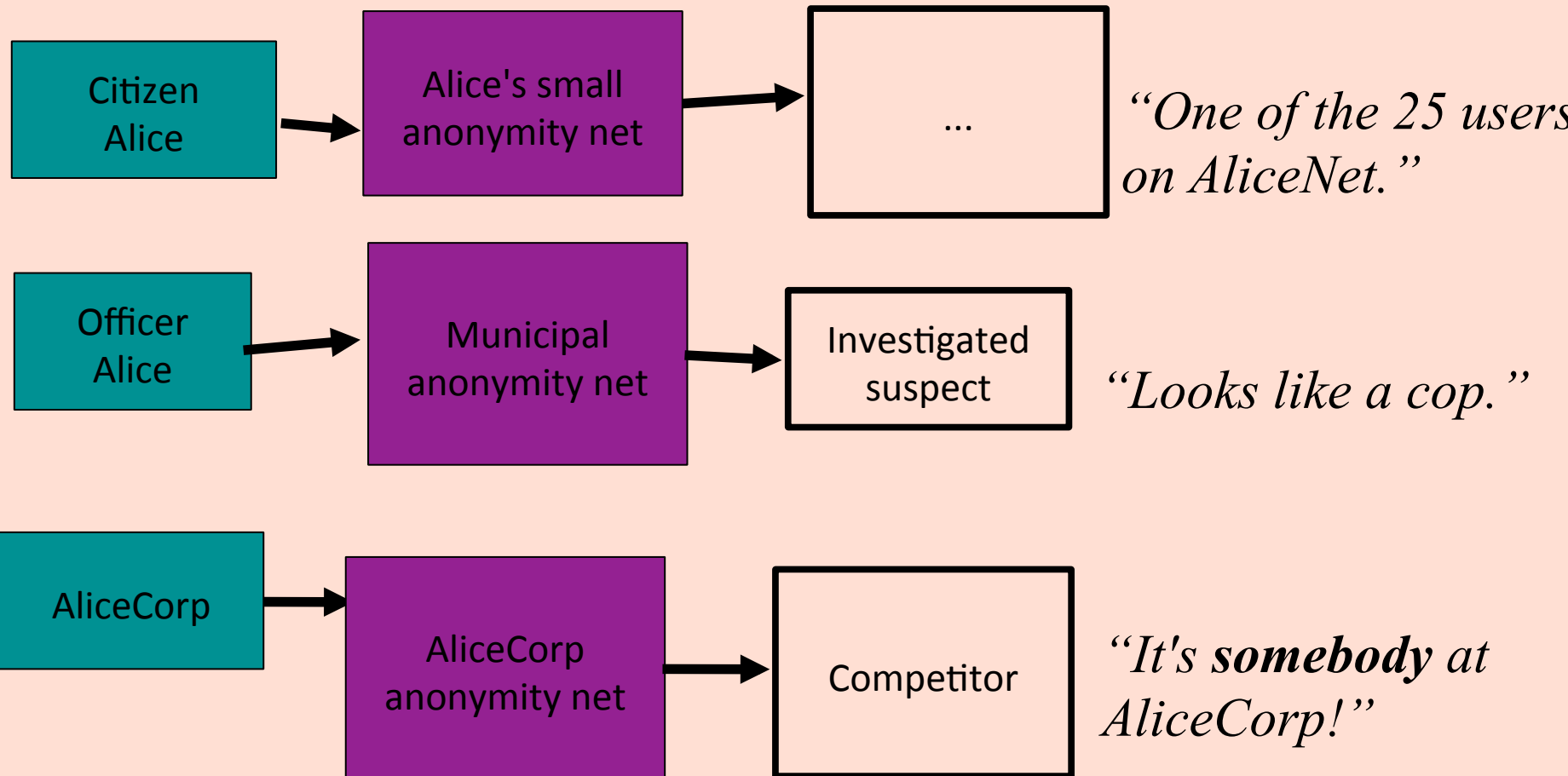


Anonymity serves different interests for different user groups.

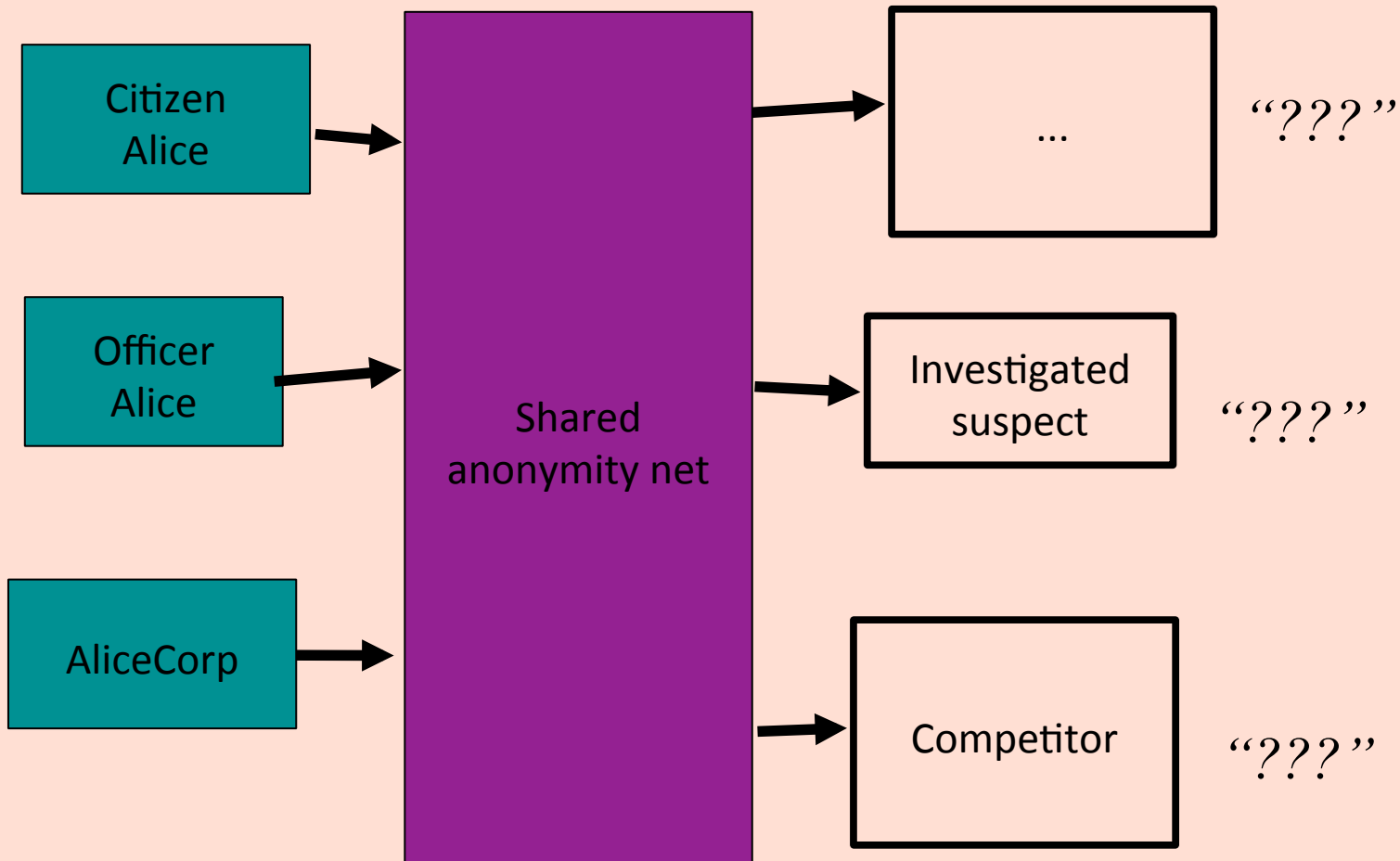


How Do We Get Anonymity?

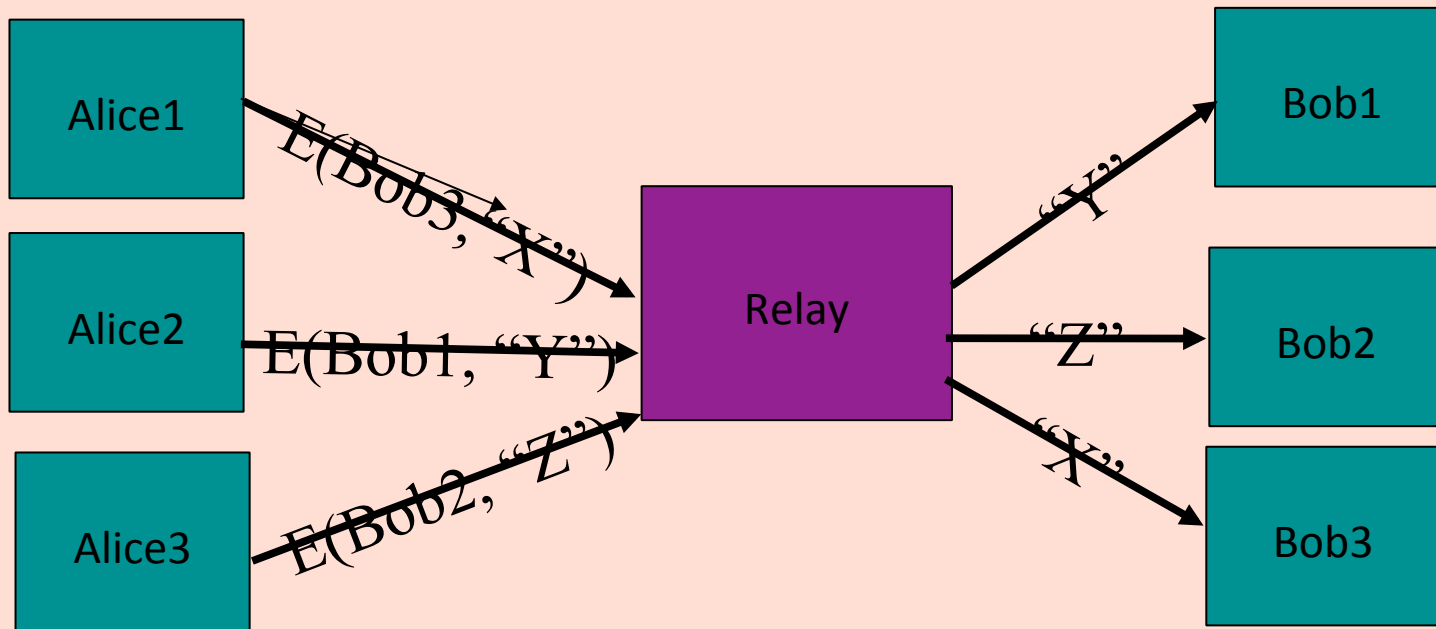
You can't get anonymity on your own: private solutions are ineffective...



... so, anonymity loves company!

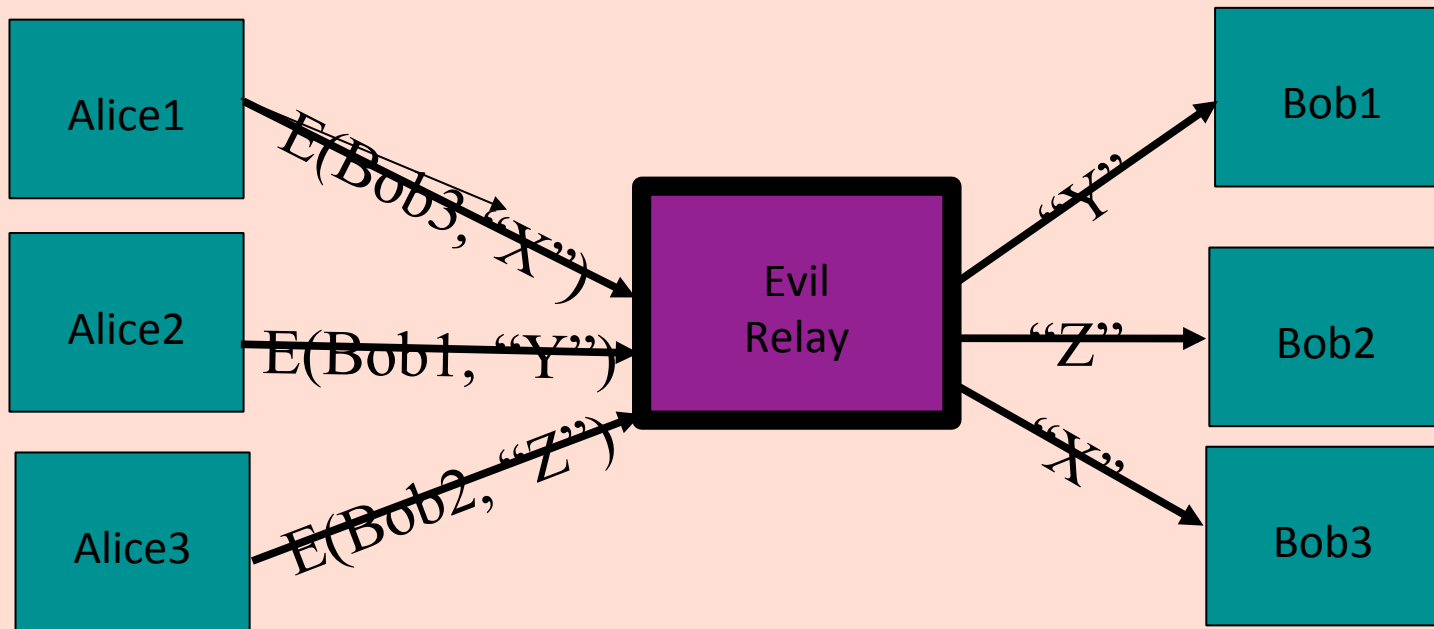


The simplest designs use a single relay to hide connections.

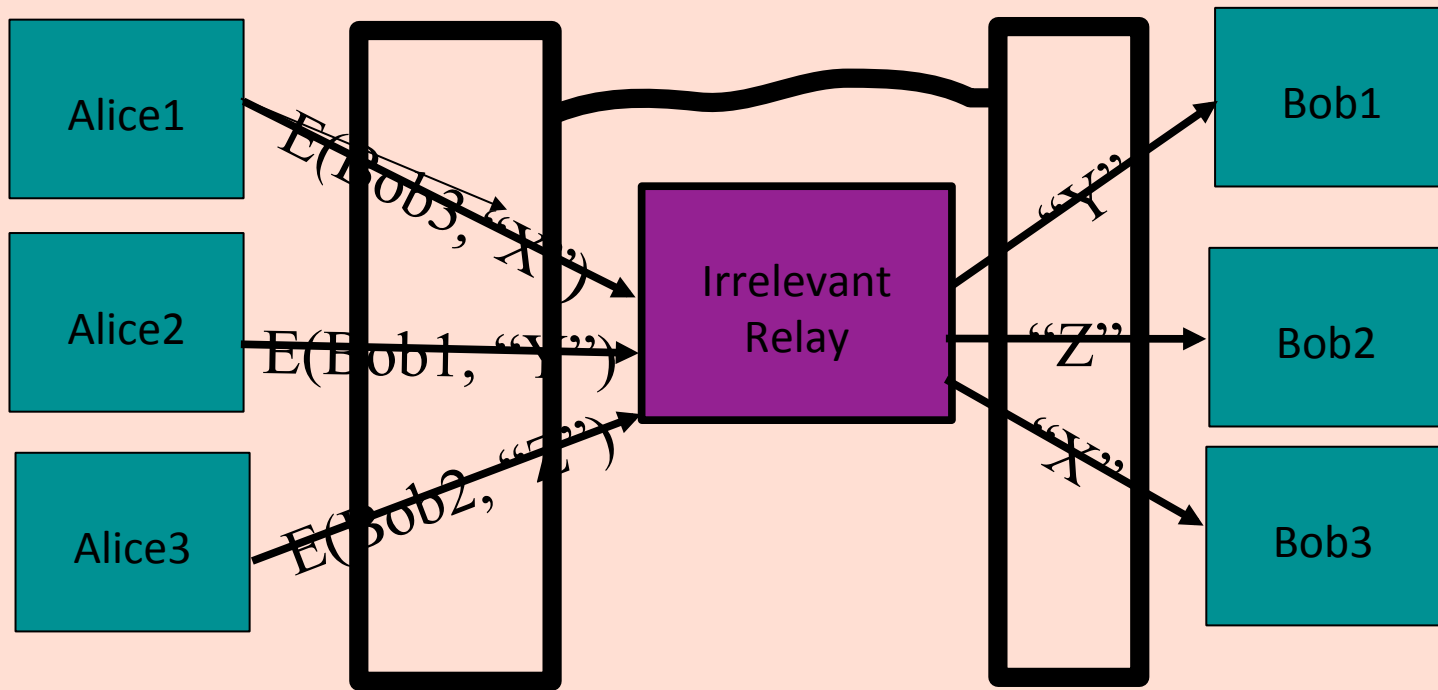


(example: some commercial proxy providers)

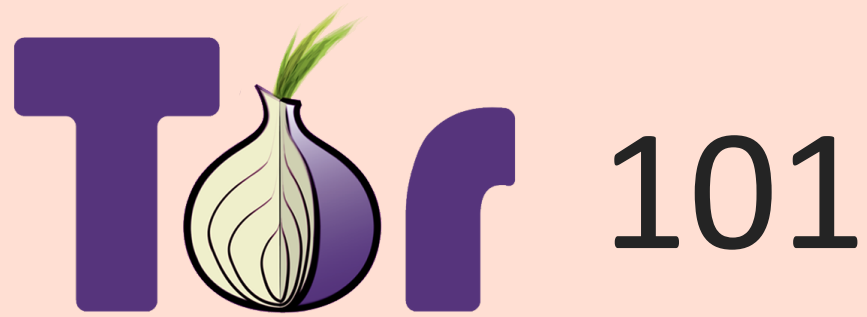
**But a single relay (or eavesdropper!)
is a single point of failure.**



... or a single point of bypass.



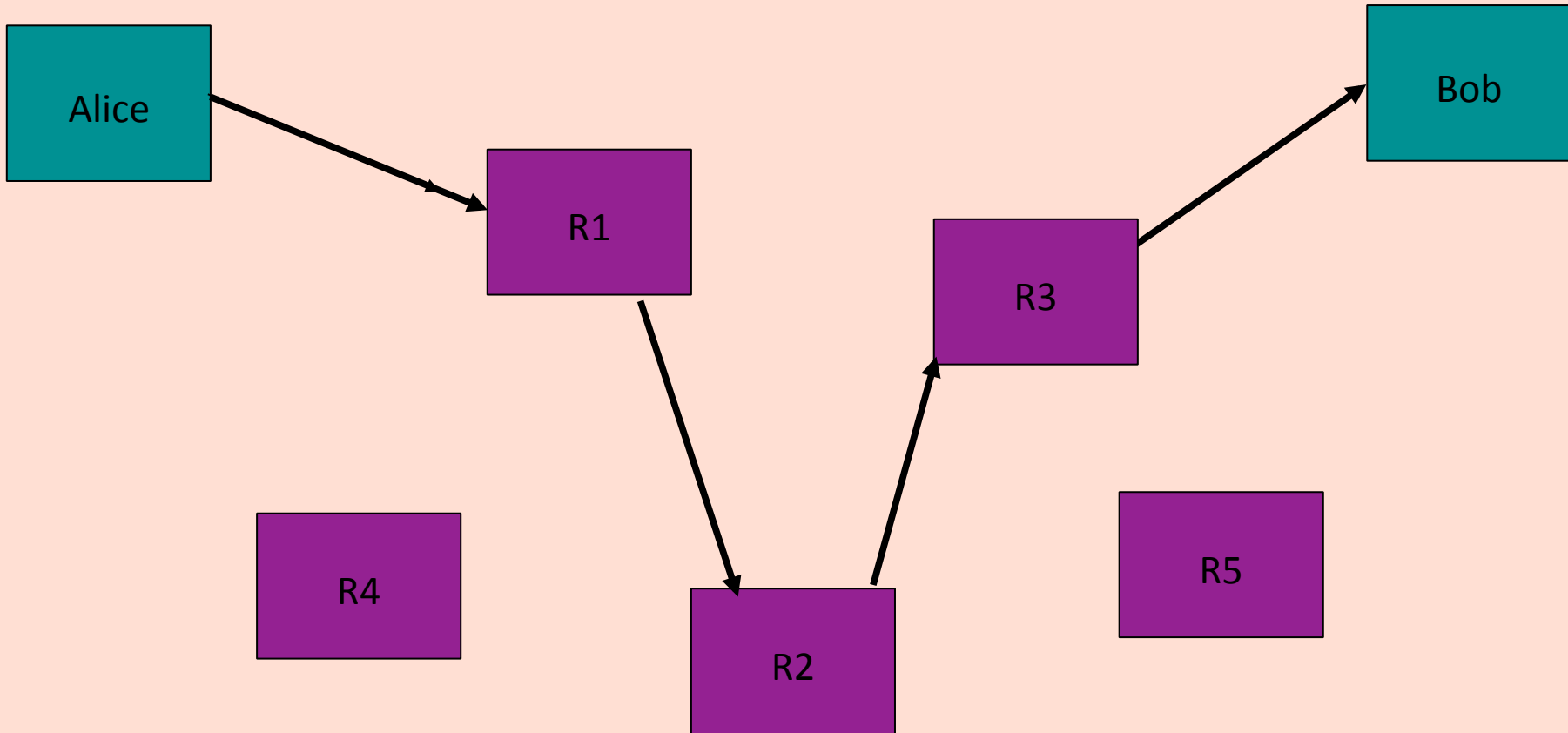
Timing analysis bridges all connections through relay \Rightarrow An attractive fat target



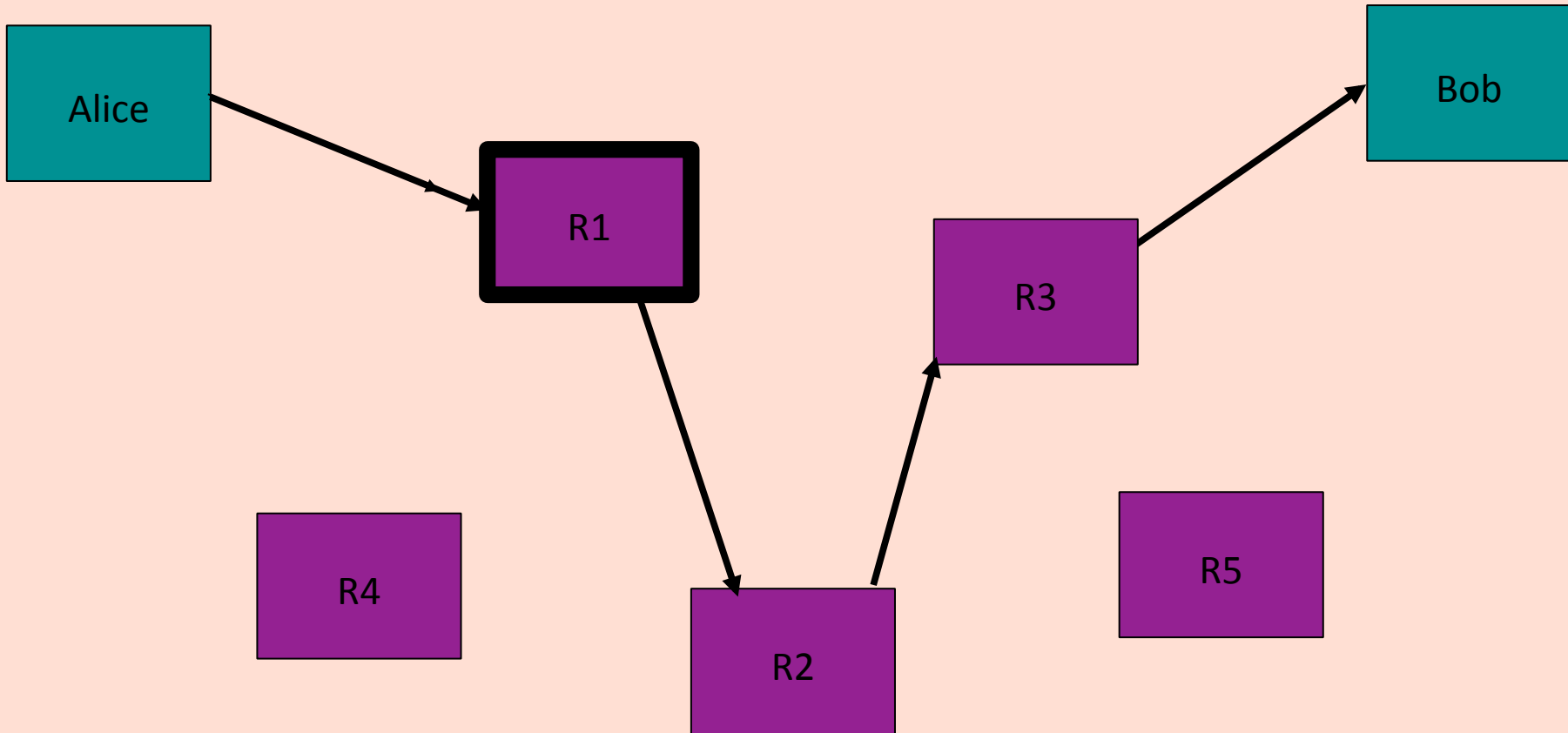
“Hack the Planet!”

<http://youtu.be/XIDxDMwwlsw>

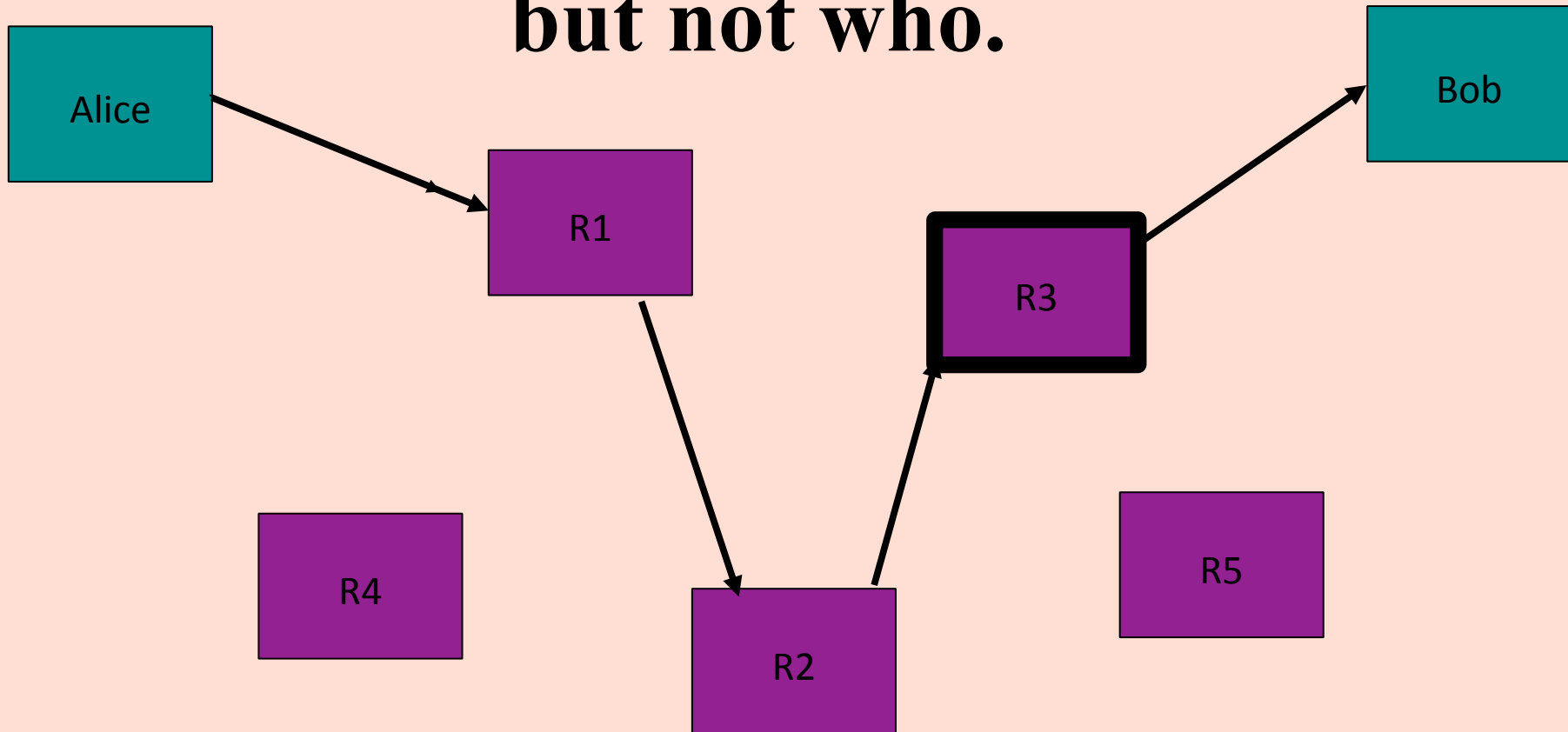
So, add multiple relays so that no single one can betray Alice.



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.



Let's use

- USBs to get the Tor Browser Bundle on your computer
 - This is NOT a great way to get Tor, but wifi is limited
- Install and run!
- It's really that easy*

*Privacy is subject to not making stupid mistakes

Tor Hecklefest

- Break into groups of 3-4
- 2 mins – introduce yourselves
- 20 mins – look up news articles about Tor
 - Is it a positive, negative, or neutral article?
 - Does it mention something that Tor is awesome at?
 - Does it mention something that Tor fails at?
- 10 mins – come back together as a big group and gather a list of “awesomes” and “fails”

Tor Hecklefest

Good

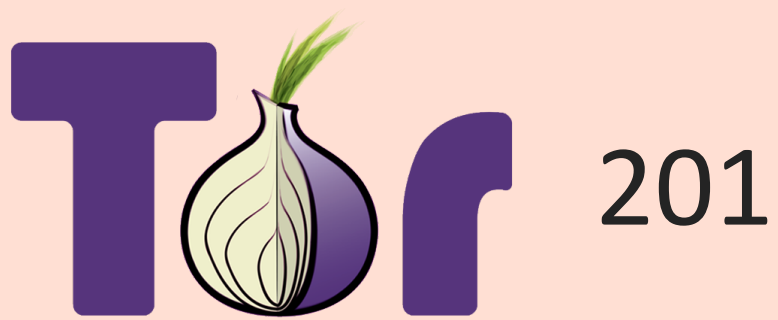
- 501c3
- Distributes with Firefox
- NSA “blessing”
- Used by activists during Arab Spring

Bad

- How Tor encrypted traffic can be hacked
- Botnet used it
- Bad people may use it

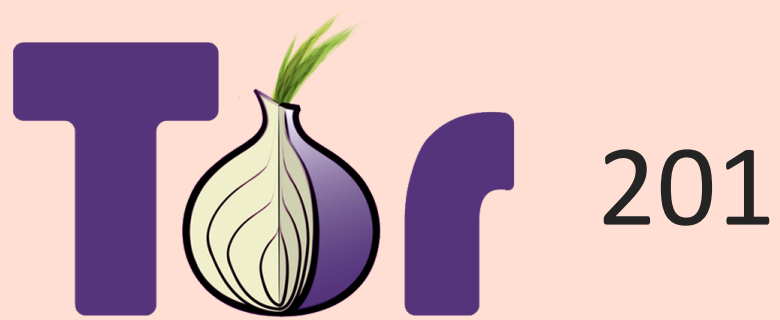
Neutral/Good+Bad

- “Tor Stinks” – NSA
- How to use Tor



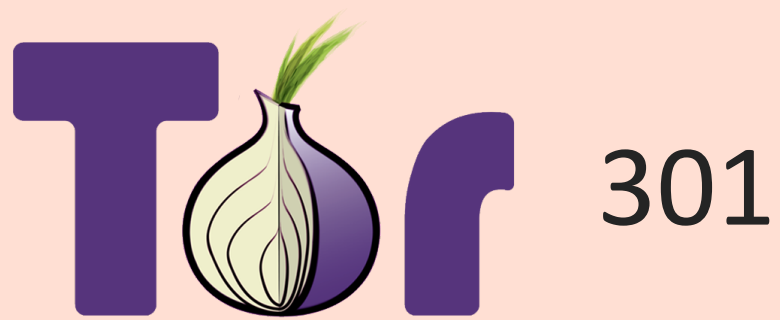
- How is it different?
 - Let's look at what Tor “broadcasts” to the world

panopticklick.eff.org



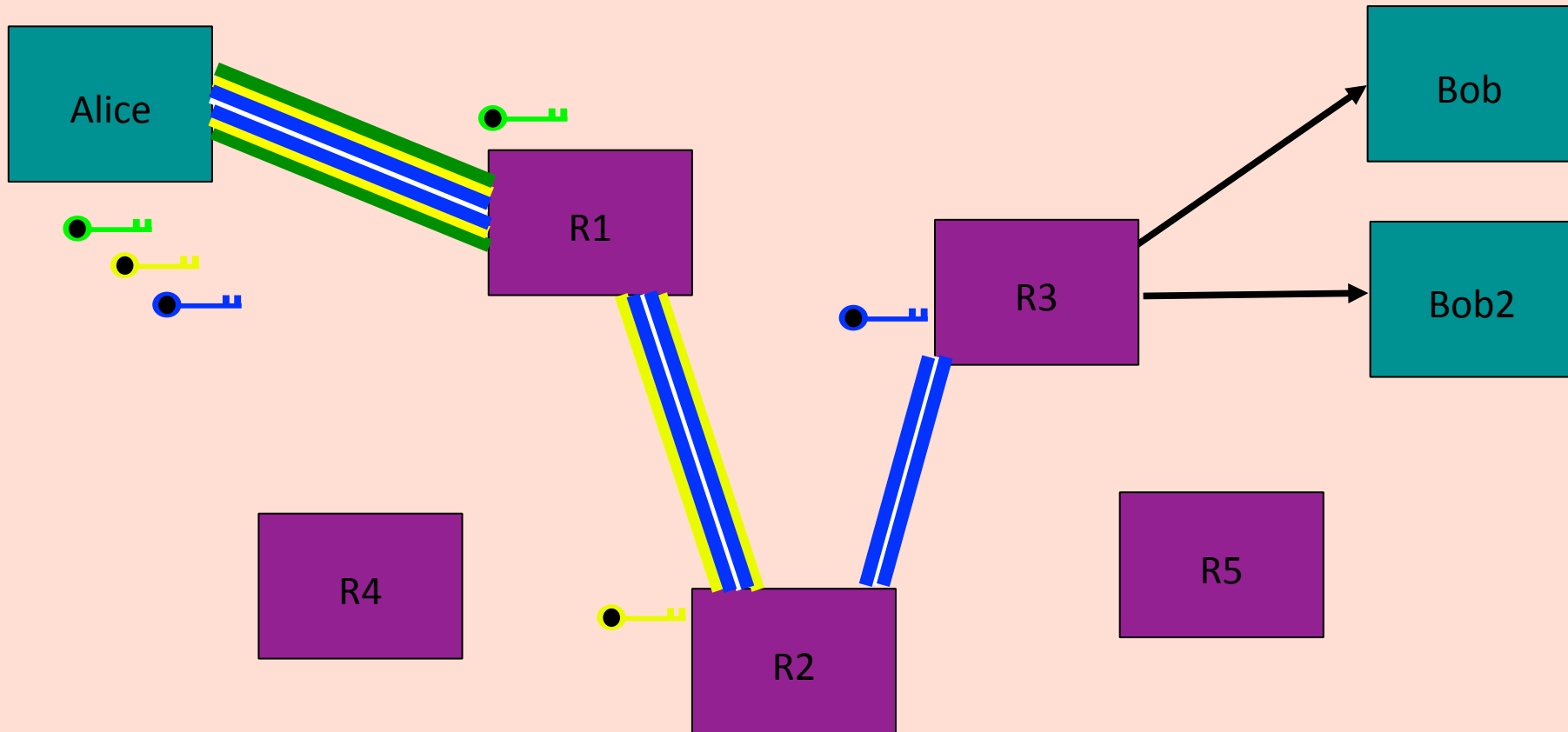
- Now Turn Off Javascript.
 - What is the difference?

panoptick.eff.org

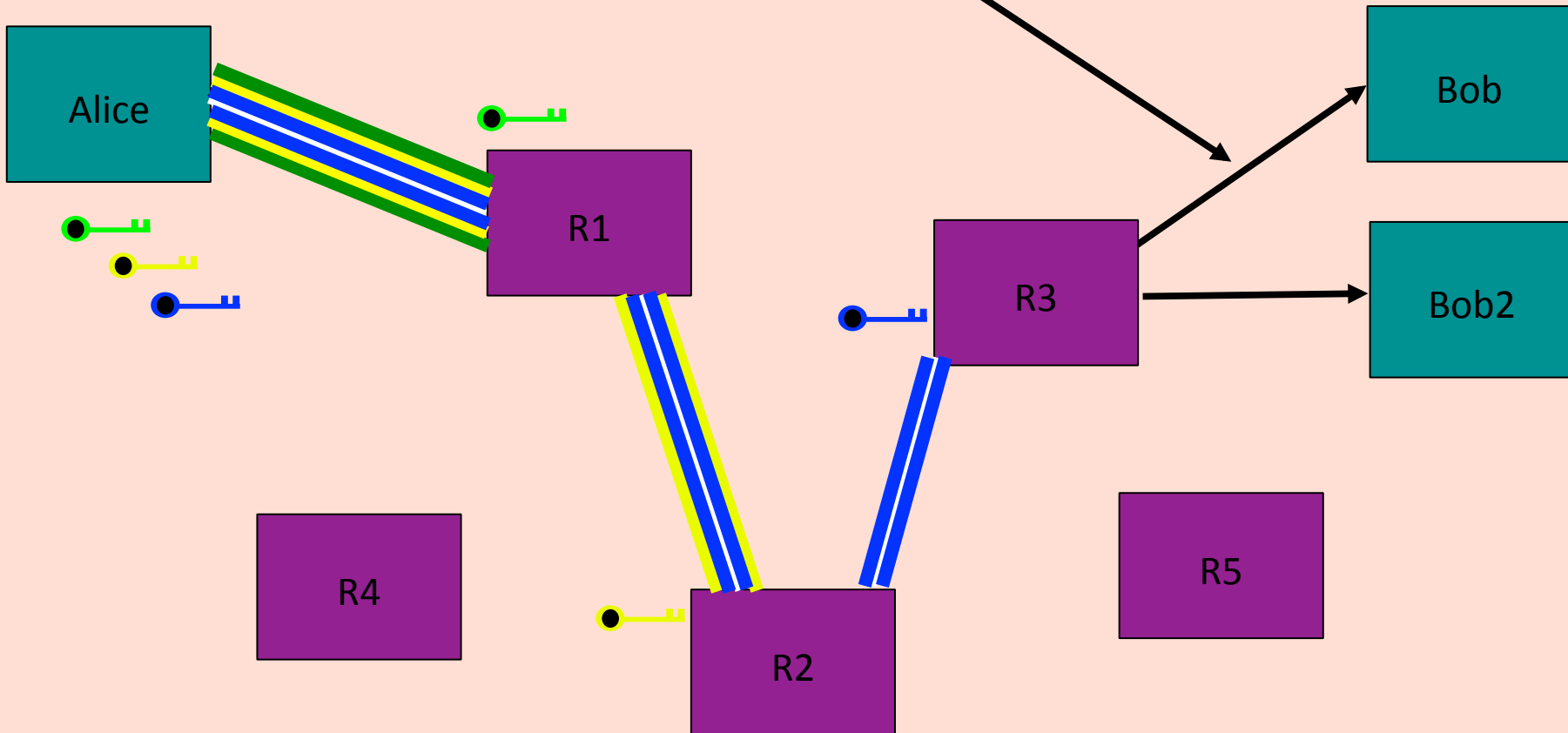


- But how does it really work?

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



What about this step?



Q&A

Thanks!

We'll send a survey out asking for feedback about this event – please watch out for it!

February – PGP?

Lead Dev: Sean McGregor @seanmcgregor
Community Manager: Jen Davidson @jewifer





(Adapted from Slides by)
Roger Dingledine
Jacob Appelbaum