Online Anonymity & Privacy

Andrew Lewman
The Tor Project
https://torproject.org/

Outline

- Why anonymity?
- Crash course on Tor
- Future

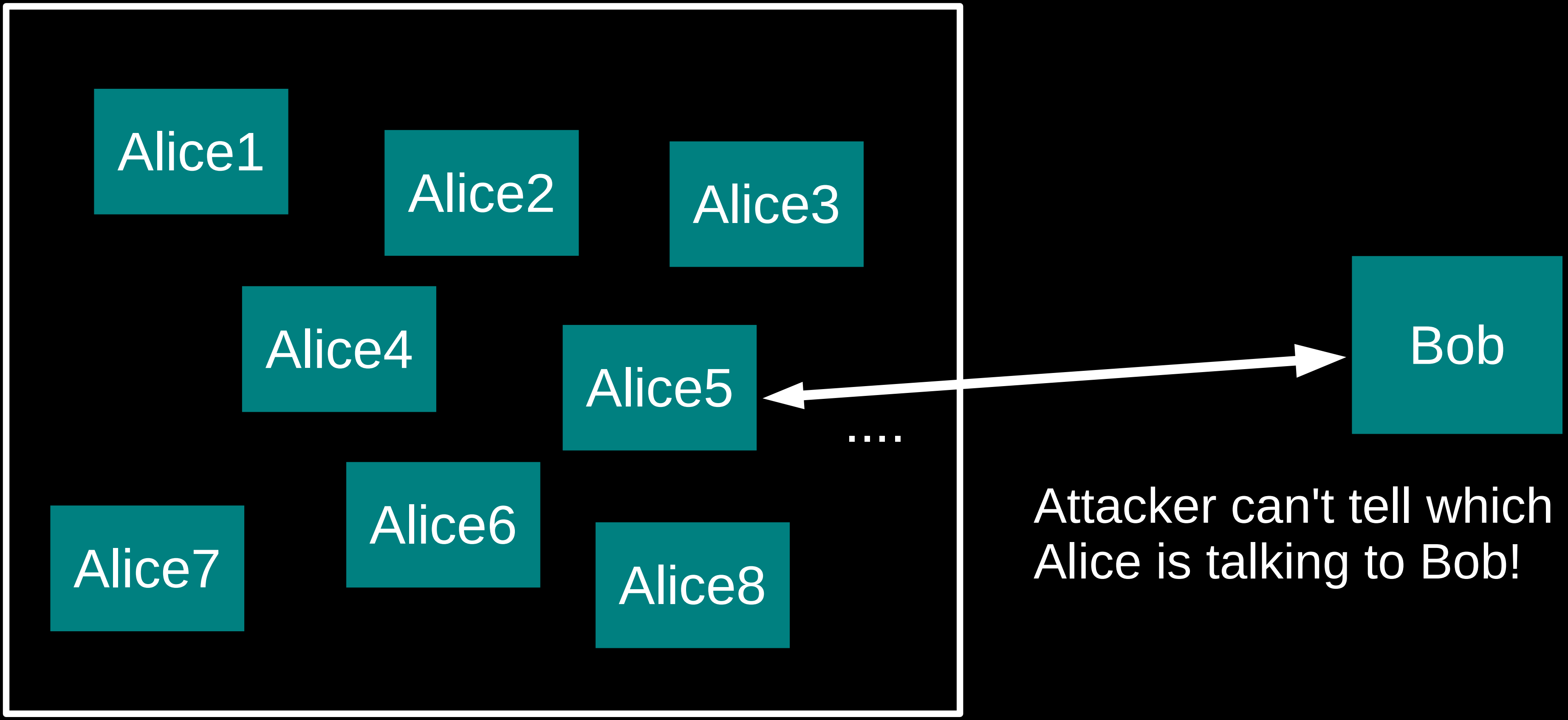
Informally: anonymity means you can't tell who did what

“Who wrote this blog post?”

“Who's been viewing my webpages?”

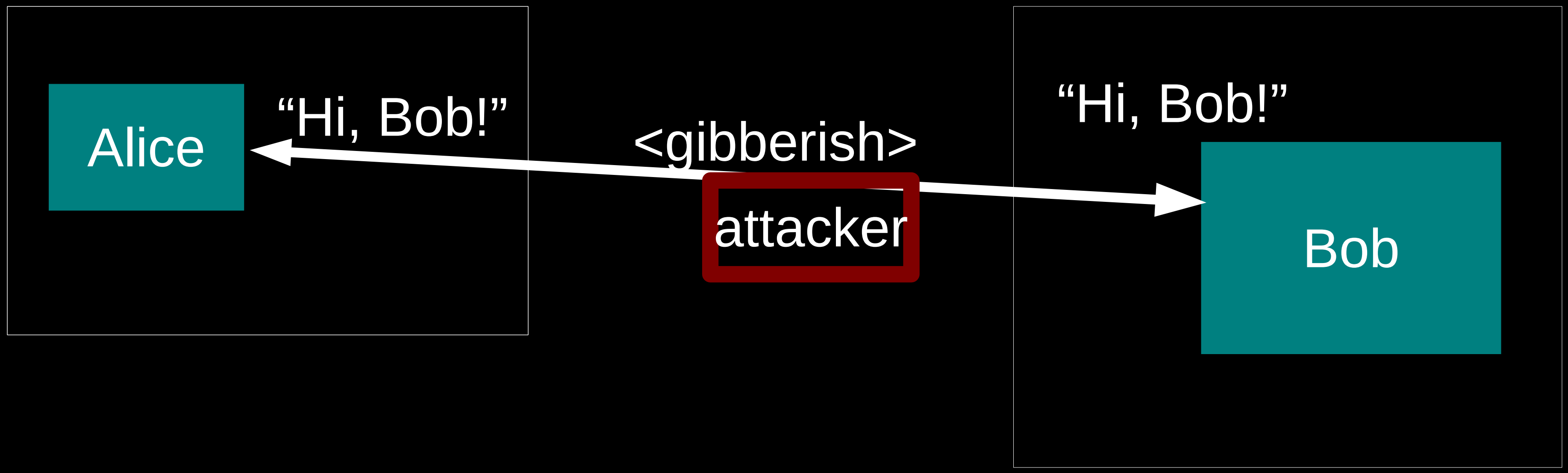
“Who's been emailing patent attorneys?”

Formally: anonymity means indistinguishability within an "anonymity set"



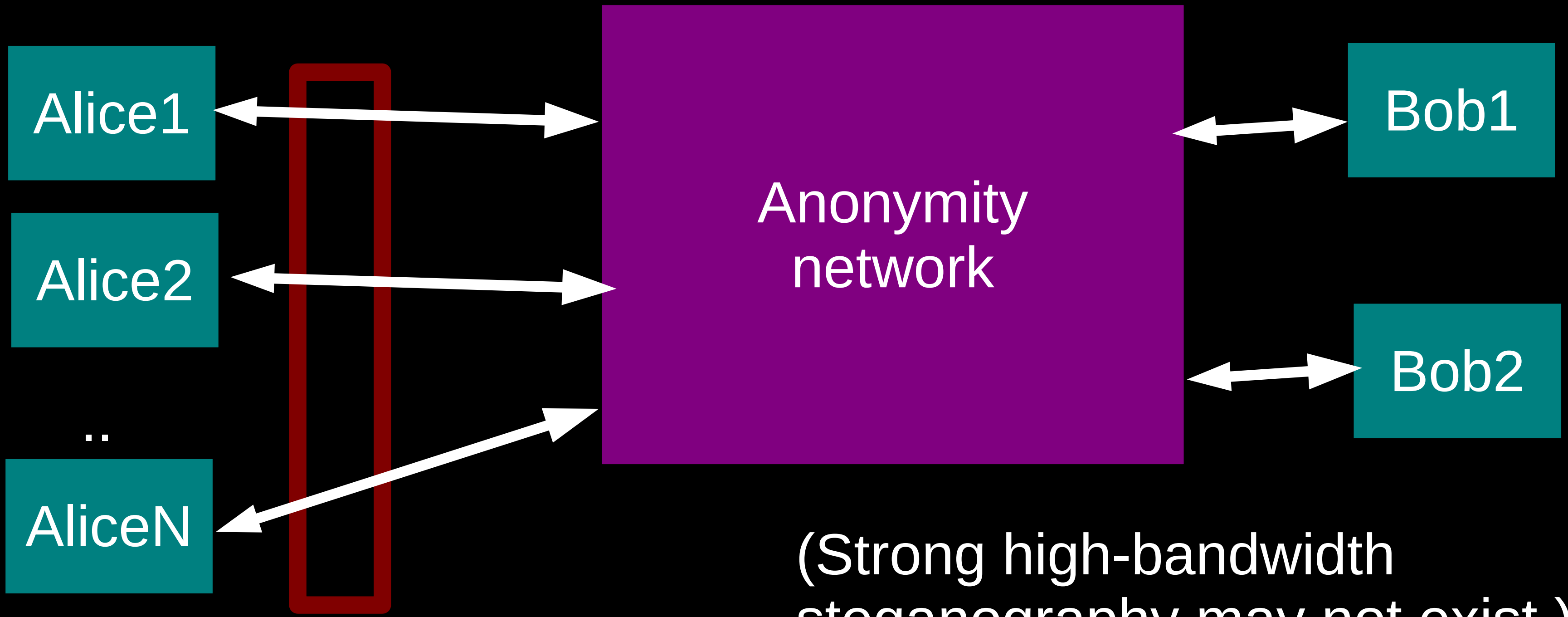
Attacker can't tell which Alice is talking to Bob!

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.

~~Promise you won't look!”~~

~~“Promise you won't remember!”~~

~~“Promise you won't tell!”~~

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

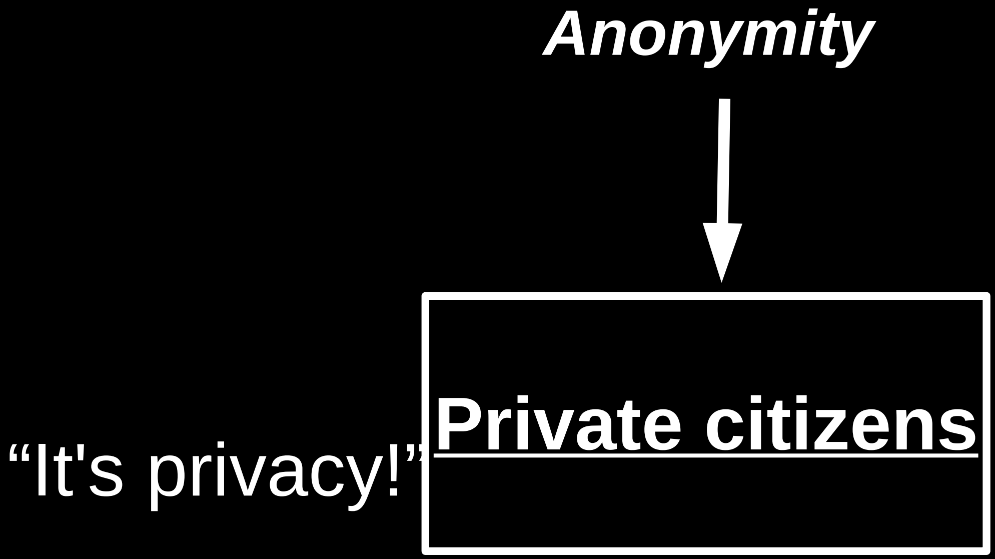
~~“I didn't write my name on it!”~~

Not what we're talking about.

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

Nope!
(More info later.)

Anonymity serves different interests for different user groups.

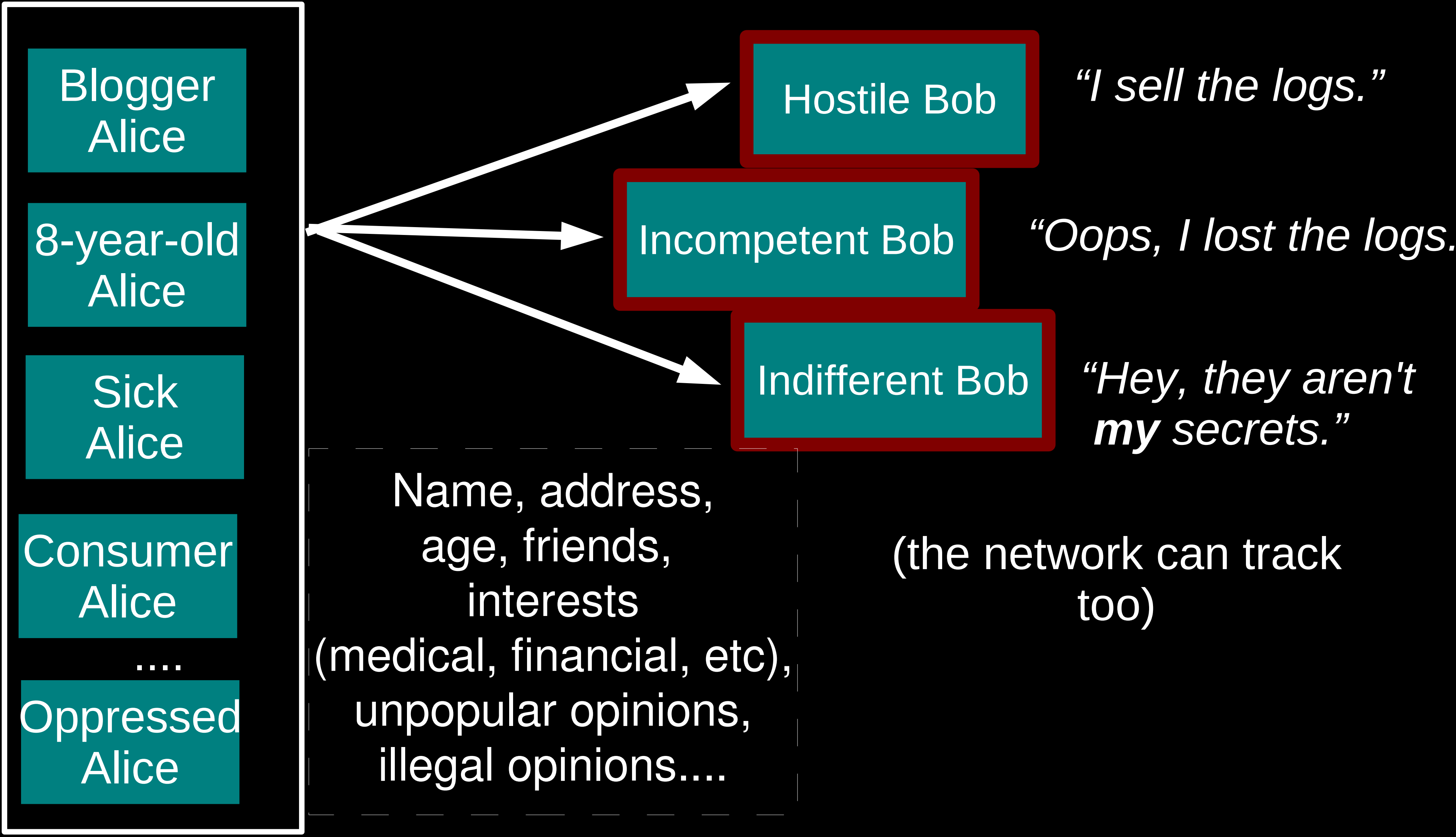


Anonymity

Private citizens

“It's privacy!”

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



Blogger Alice

8-year-old Alice

Sick Alice

Consumer Alice

....

Oppressed Alice

Hostile Bob

“I sell the logs.”

Incompetent Bob

“Oops, I lost the logs.

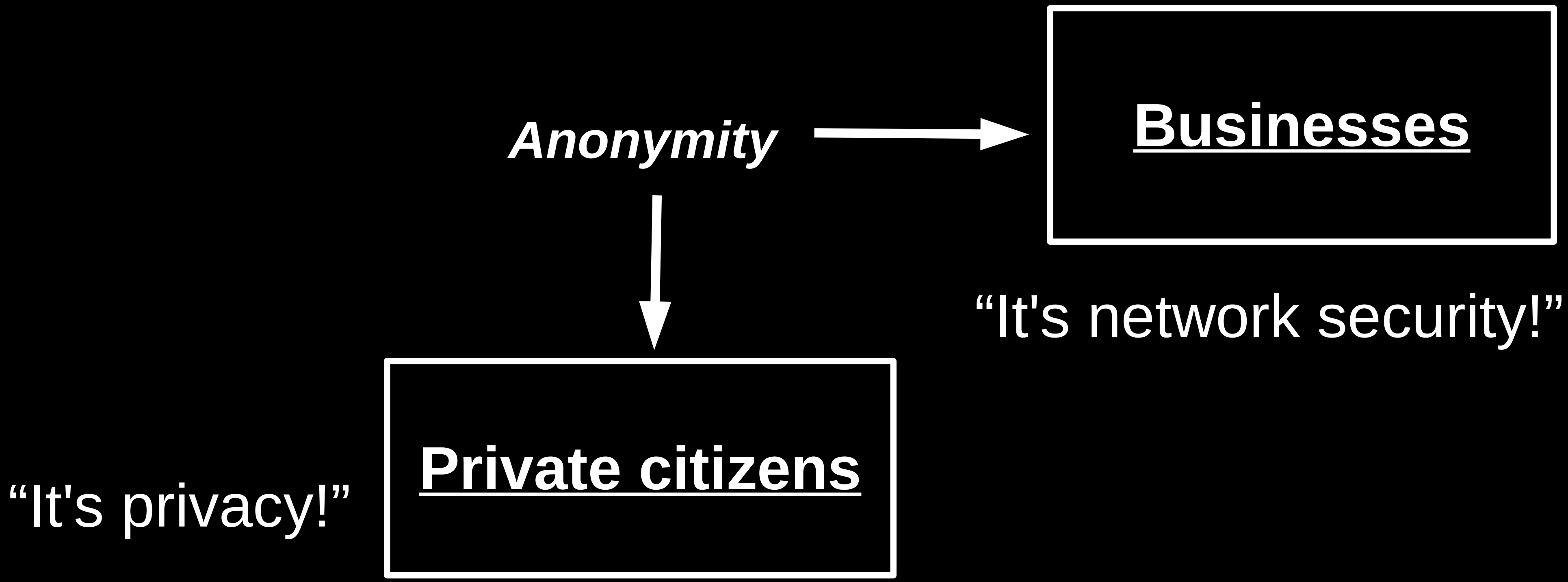
Indifferent Bob

*“Hey, they aren't **my** secrets.”*

Name, address, age, friends, interests (medical, financial, etc), unpopular opinions, illegal opinions....

(the network can track too)

Anonymity serves different interests for different user groups.



Anonymity

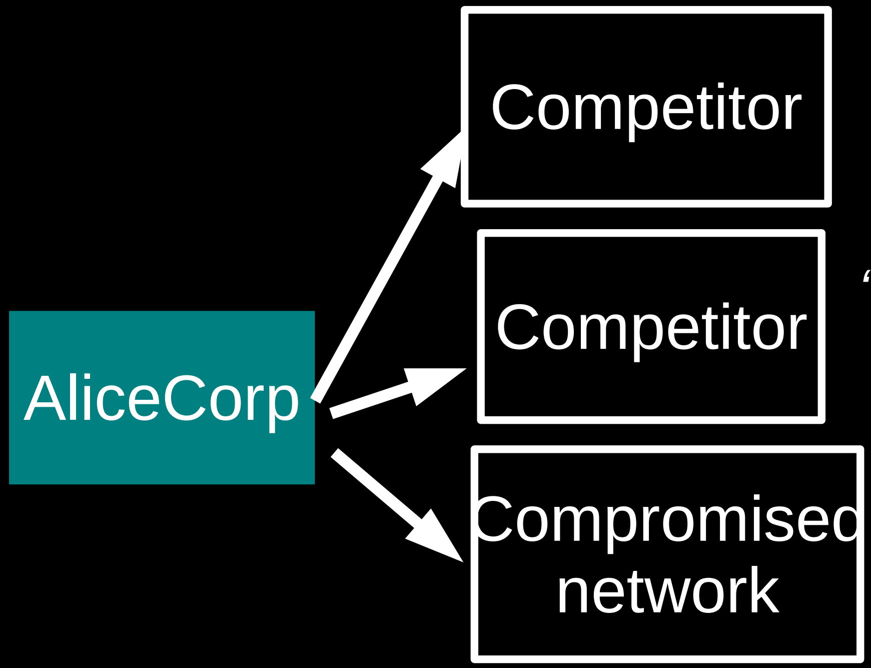
Businesses

“It's network security!”

Private citizens

“It's privacy!”

Businesses need to keep trade secrets.



AliceCorp

Competitor

Competitor

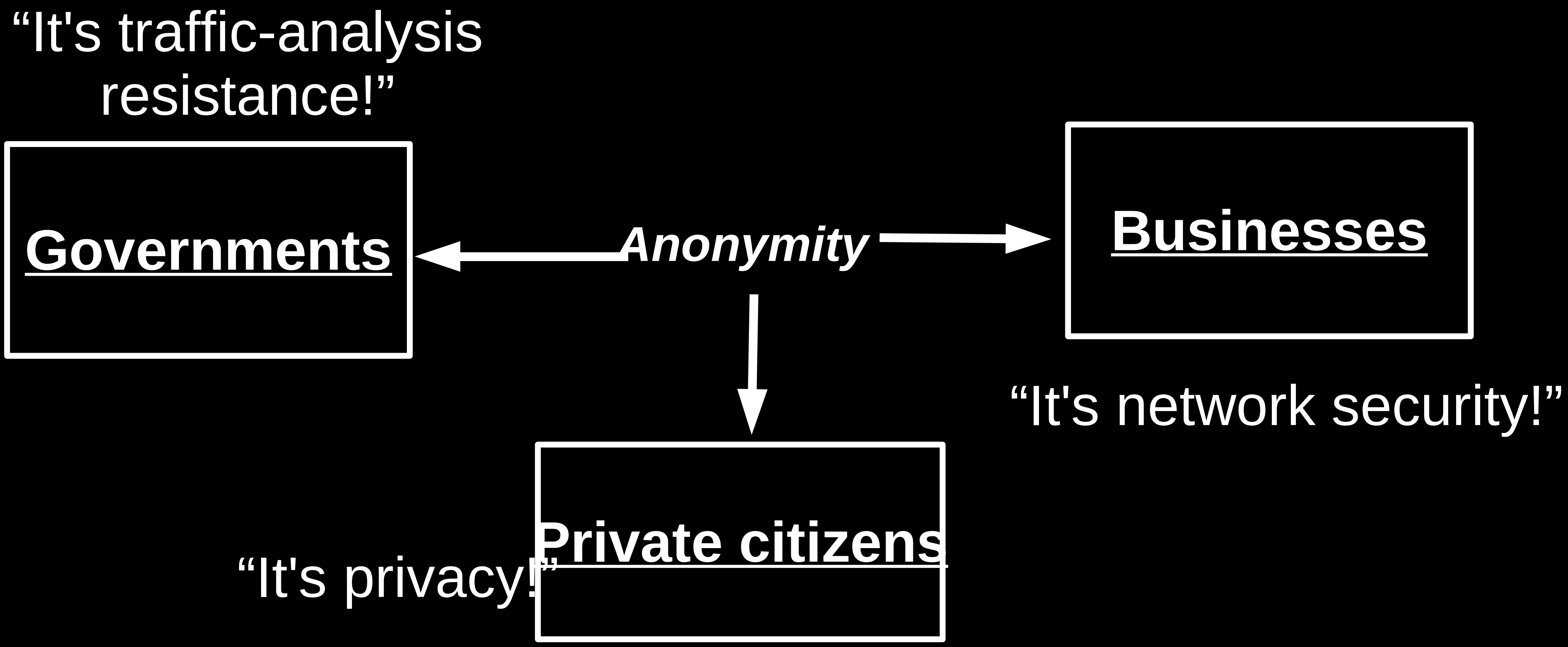
Compromised network

“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.



“It's traffic-analysis resistance!”

Governments

Anonymity

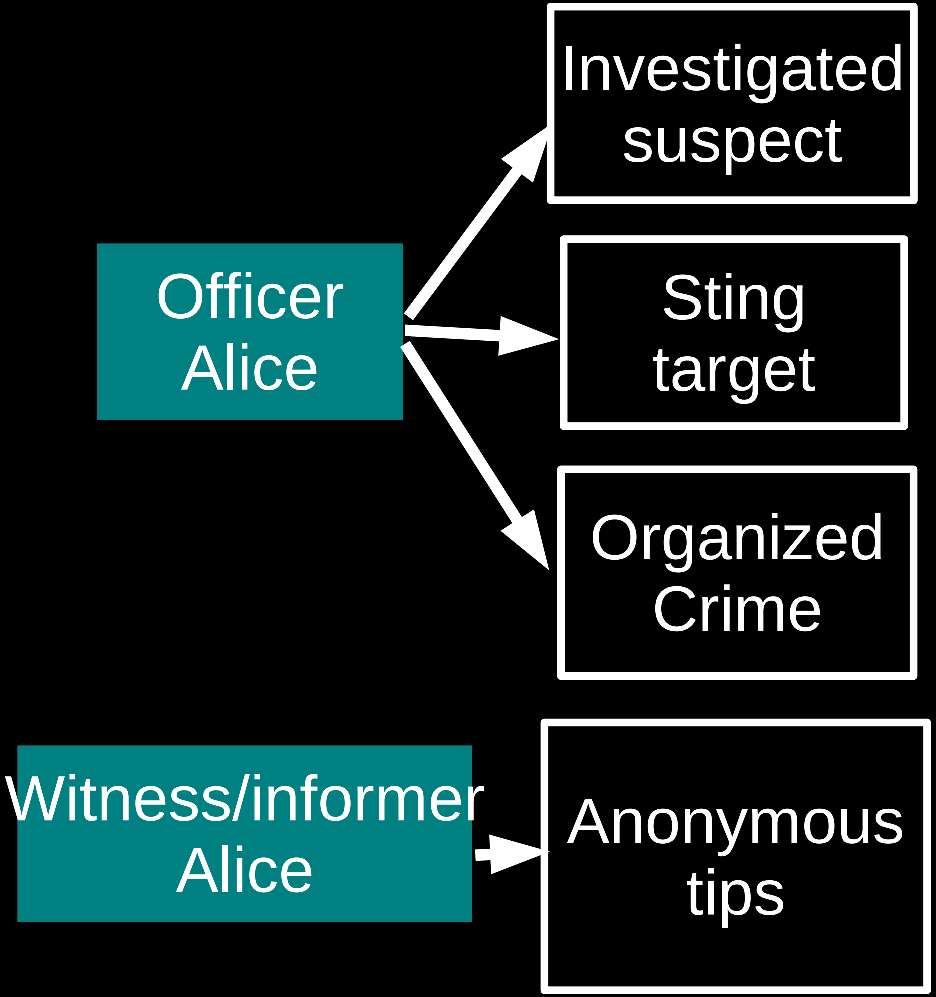
Businesses

“It's network security!”

Private citizens

“It's privacy!”

Law enforcement needs anonymity to get the job done.



Officer Alice

Investigated suspect

“Why is alice.localpolice.gov reading my website?”

Sting target

“Why no, alice.localpolice.gov! I would never sell counterfeits on ebay!”

Organized Crime

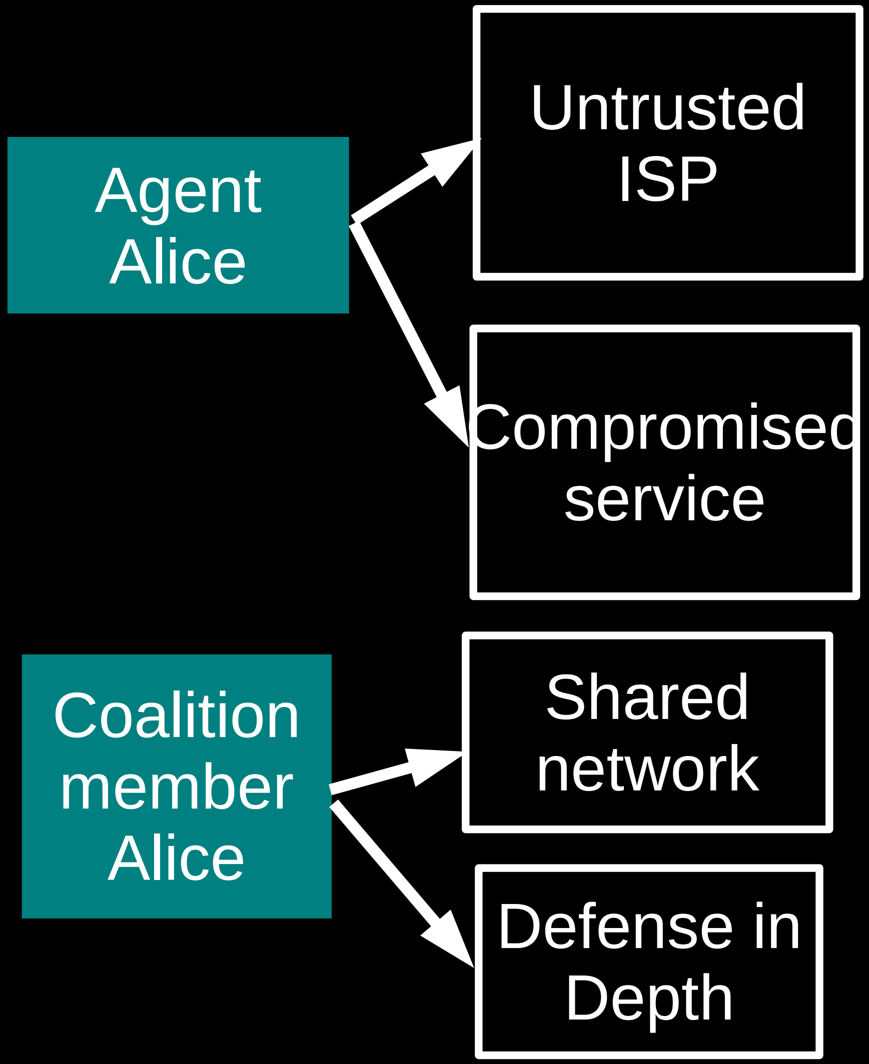
“Is my family safe if I go after these guys?”

Witness/informer Alice

Anonymous tips

“Are they really going to ensure my anonymity?”

Governments need anonymity for their security



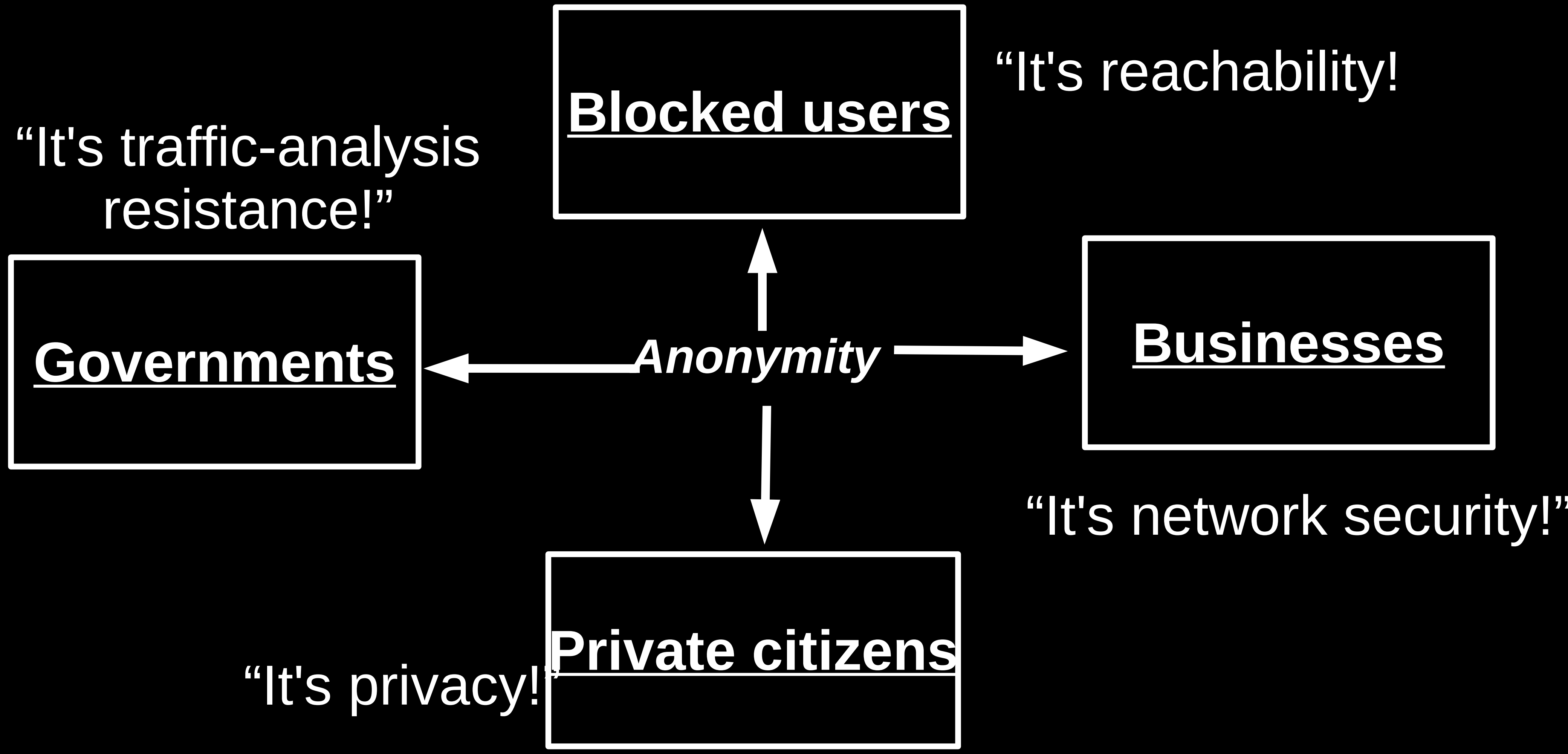
“What will you bid for a list of Baghdad IP addresses that get email from .gov?

“What does the CIA Google for?”

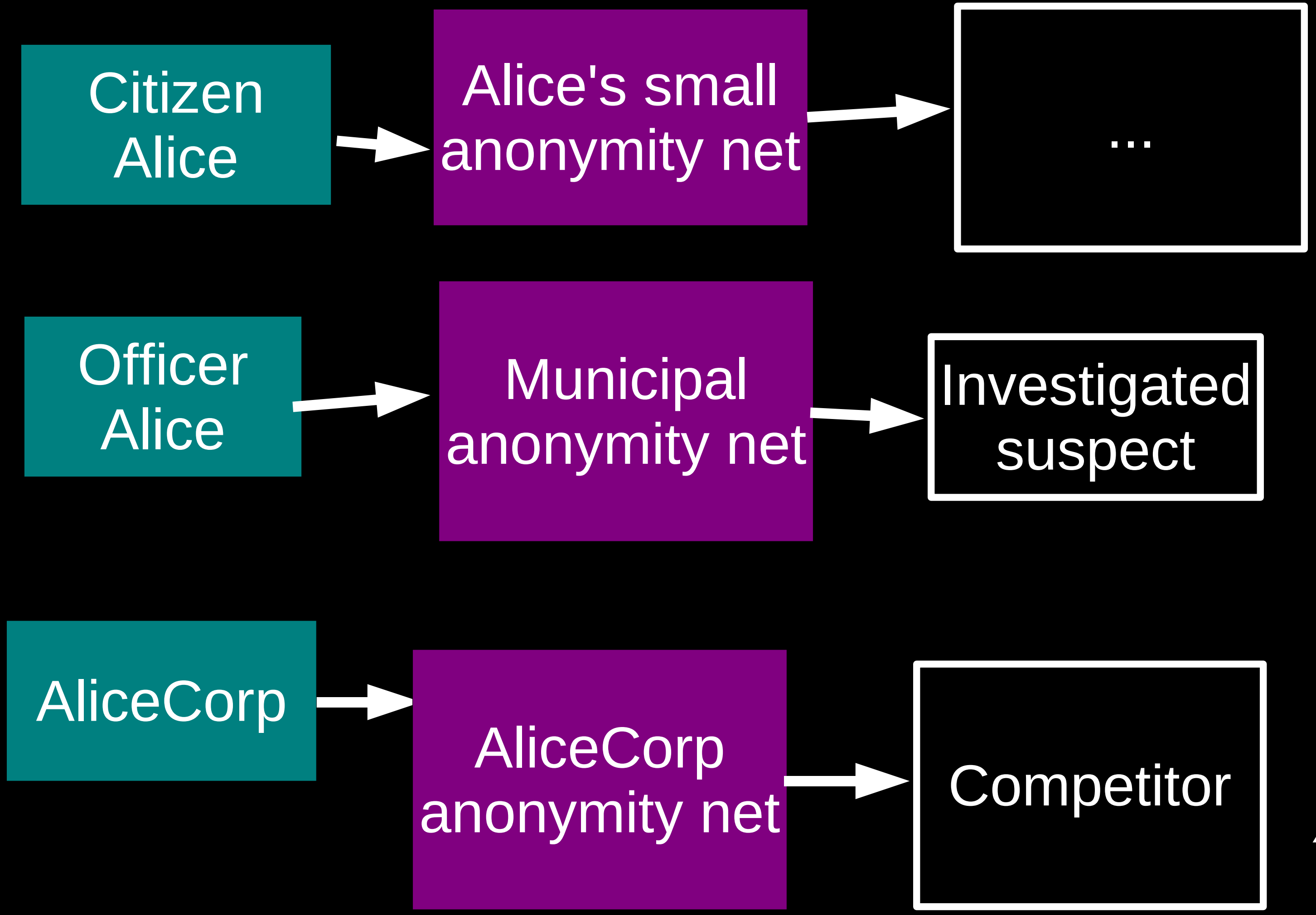
“Do I really want to reveal my internal network topology?”

“What about insiders?”

Anonymity serves different interests for different user groups.



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



Citizen Alice → Alice's small anonymity net → ...

"One of the 25 users on AliceNet."

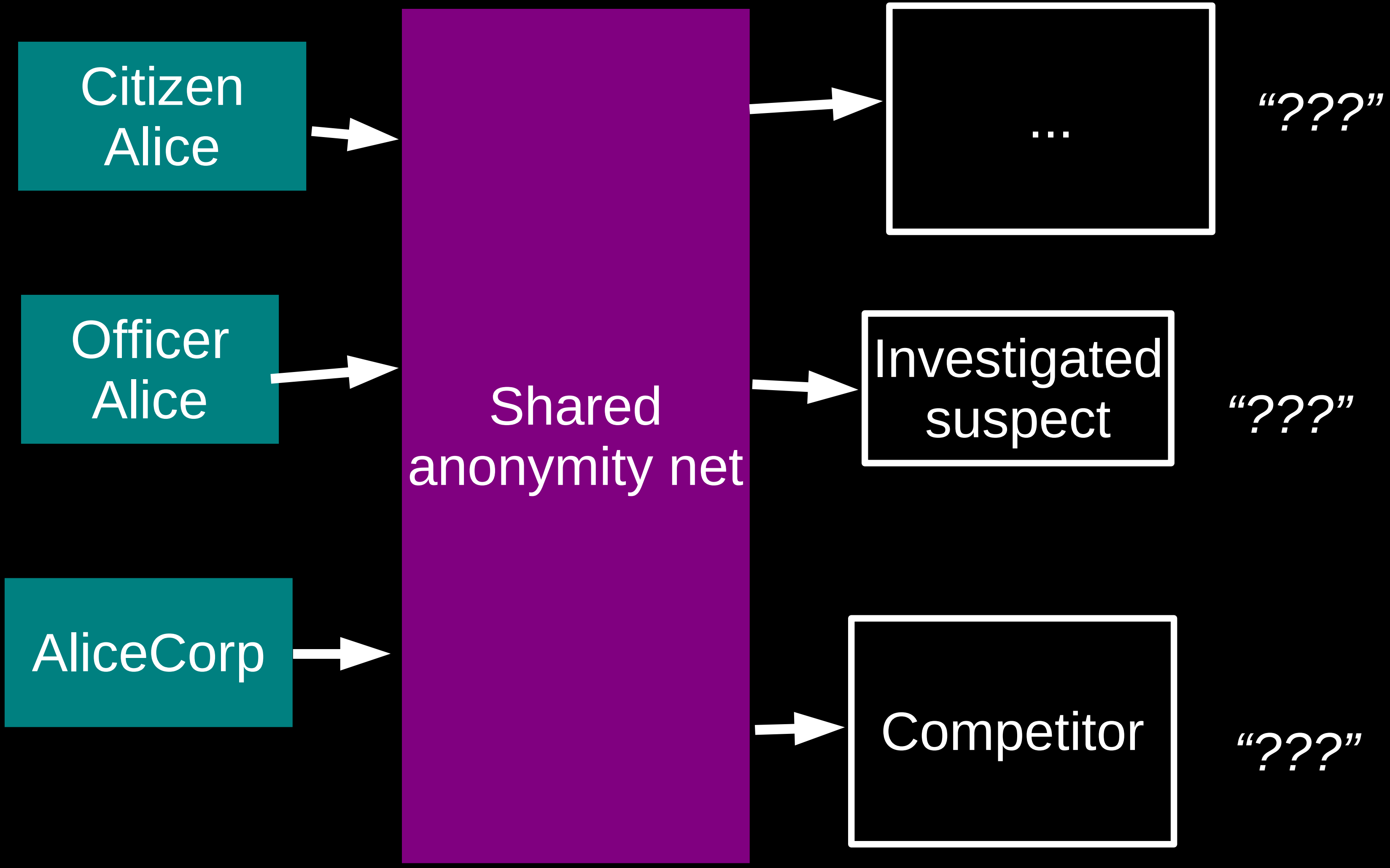
Officer Alice → Municipal anonymity net → Investigated suspect

"Looks like a cop."

AliceCorp → AliceCorp anonymity net → Competitor

*"It's **somebody** at AliceCorp!"*

... so, anonymity loves company!



Citizen Alice

Officer Alice

AliceCorp

Shared anonymity net

...

"???"

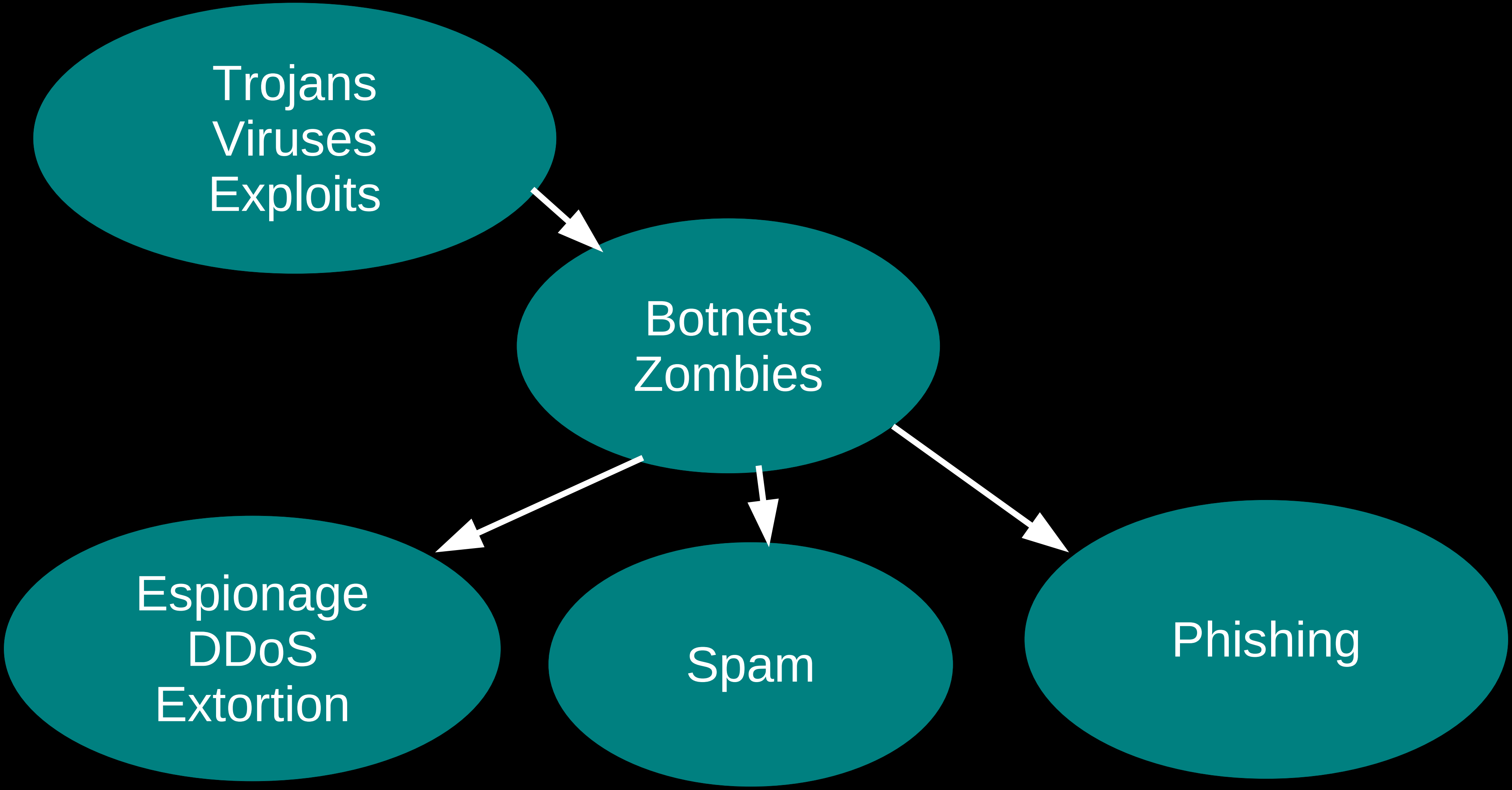
Investigated suspect

"???"

Competitor

"???"

Current situation: Bad people on the Internet are doing fine



Trojans
Viruses
Exploits

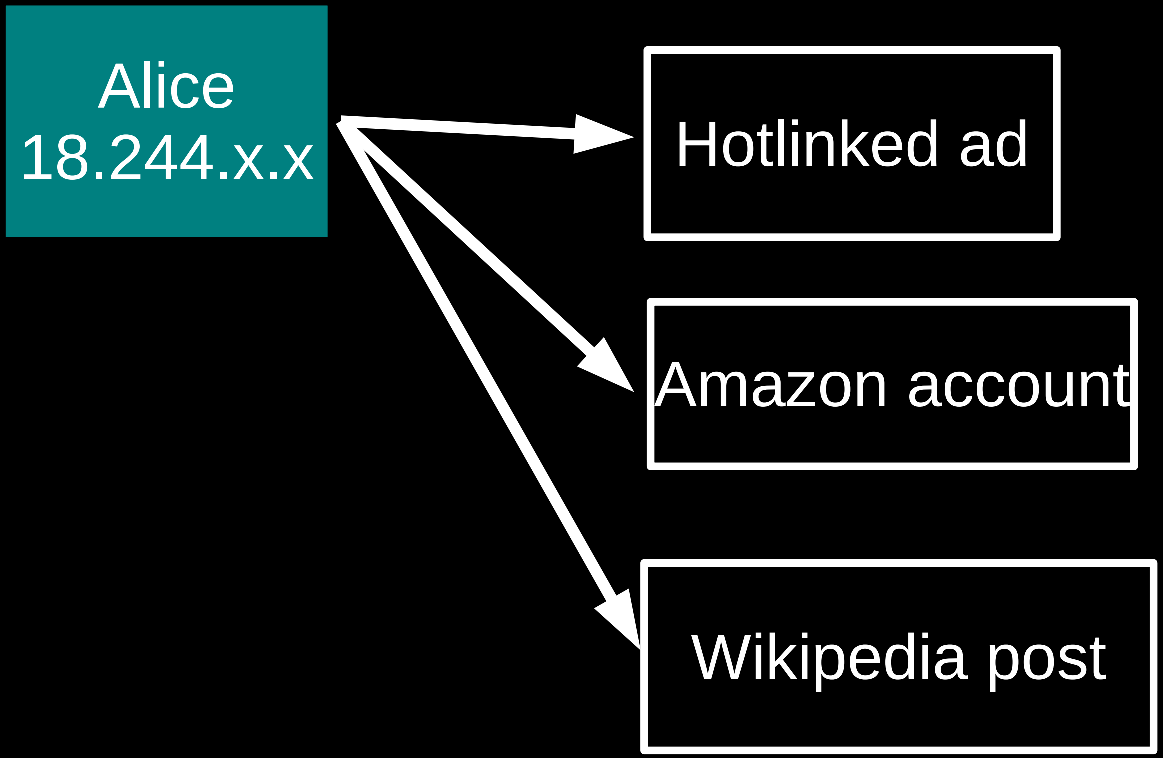
Botnets
Zombies

Espionage
DDoS
Extortion

Spam

Phishing

IP addresses can be enough to bootstrap knowledge of identity.



Alice
18.244.x.x

Hotlinked ad

Amazon account

Wikipedia post

Outline

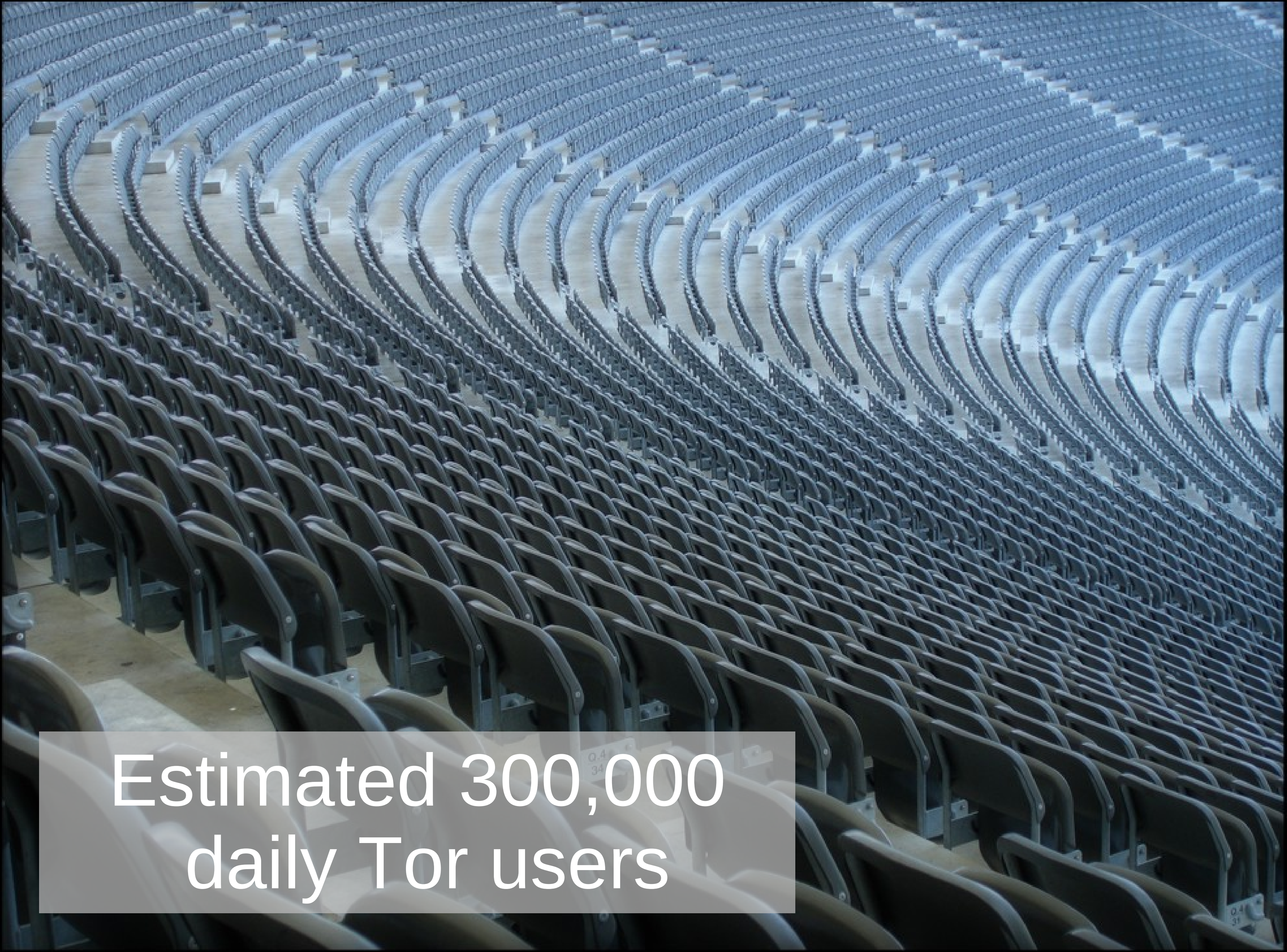
- Why anonymity?
- *Crash course on Tor*
- Future

What is Tor?

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

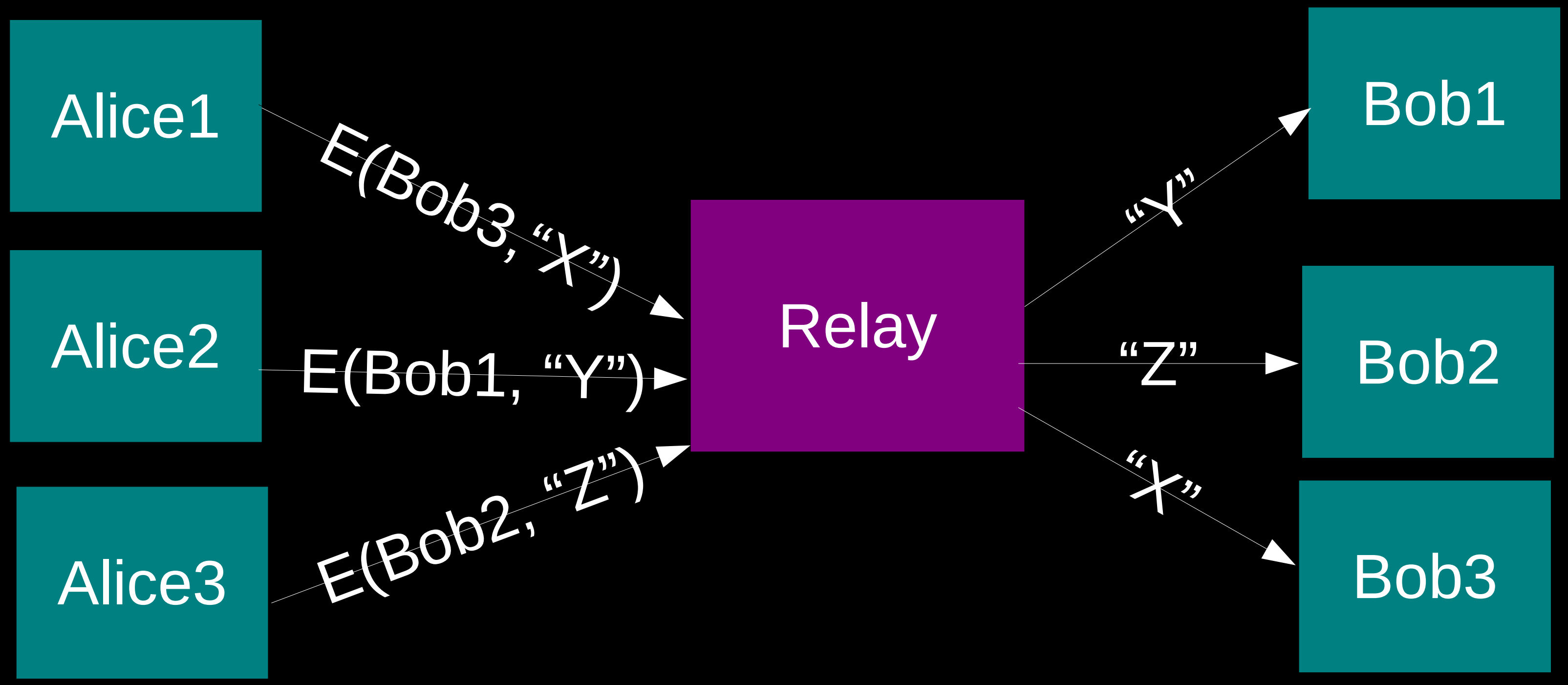
The Tor Project, Inc.

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



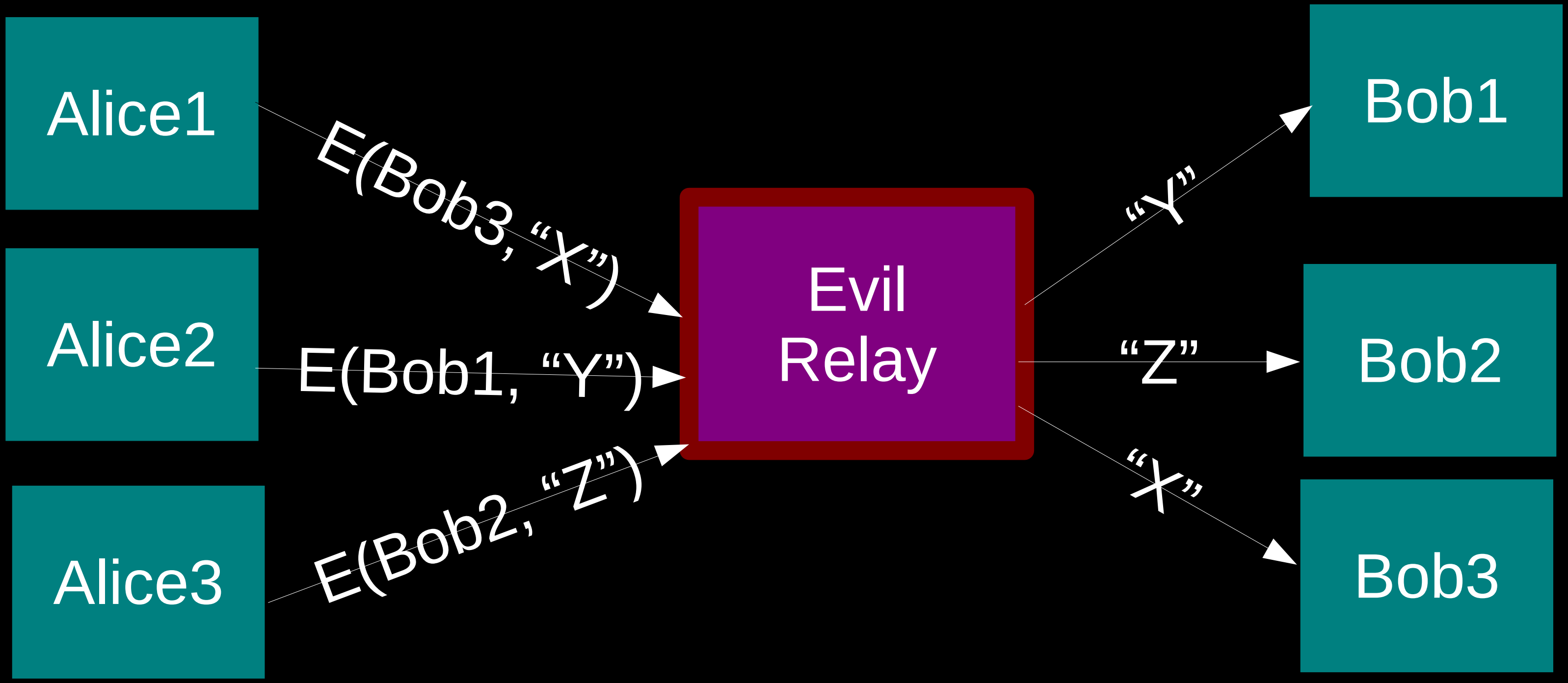
Estimated 300,000 daily Tor users

The simplest designs use a single relay to hide connections.



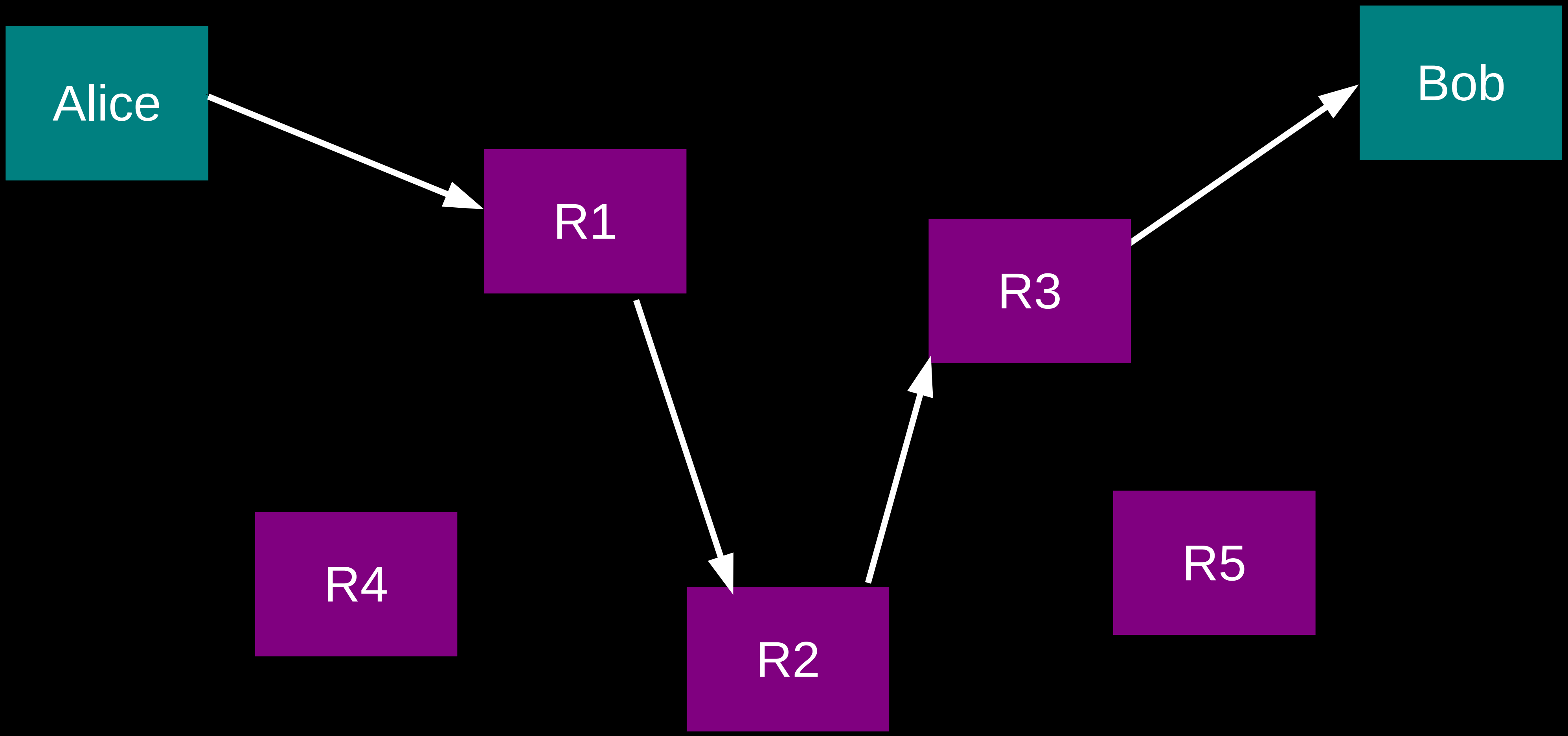
(example: some commercial proxy providers)

But a single relay is a single point of failure.

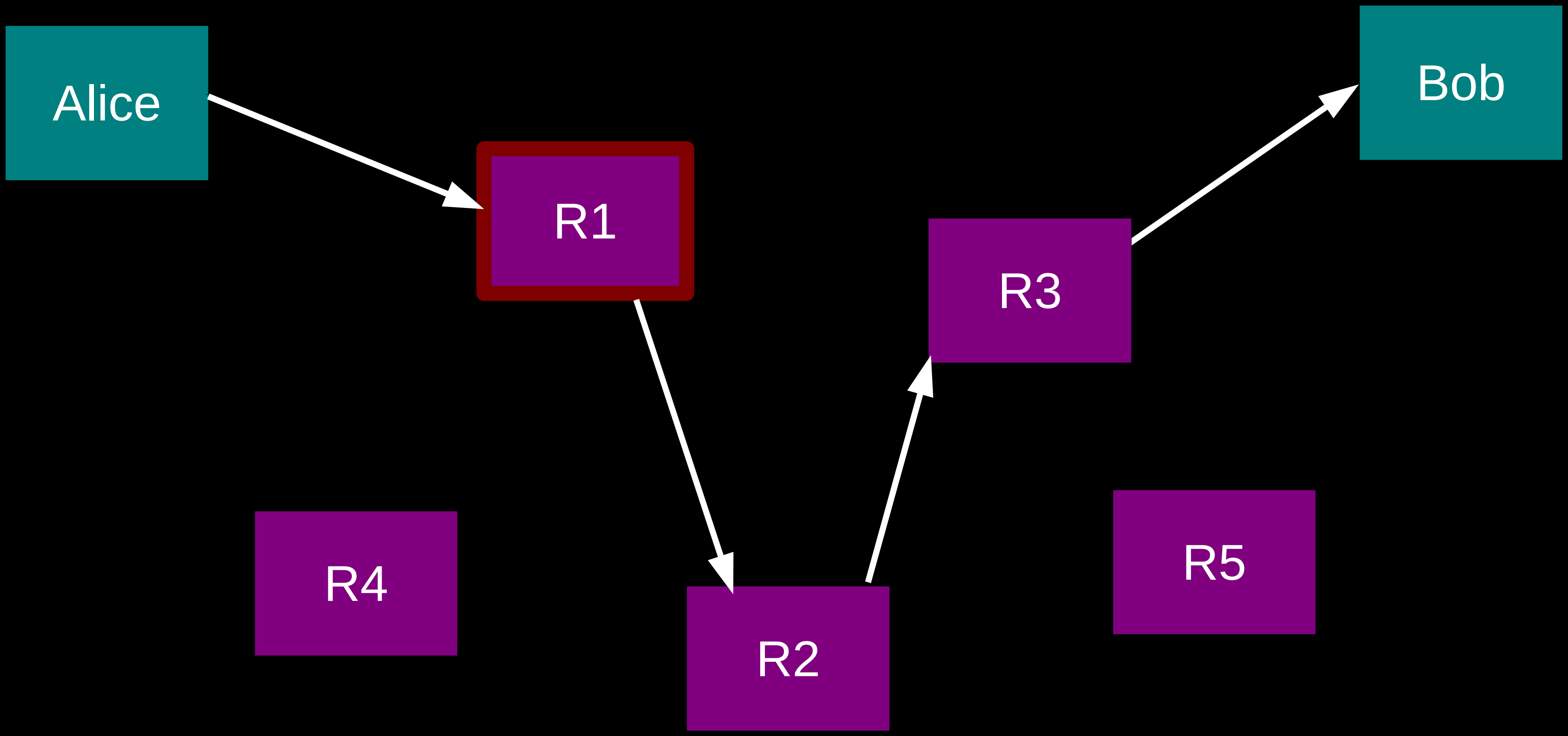


Eavesdropping the relay works too.

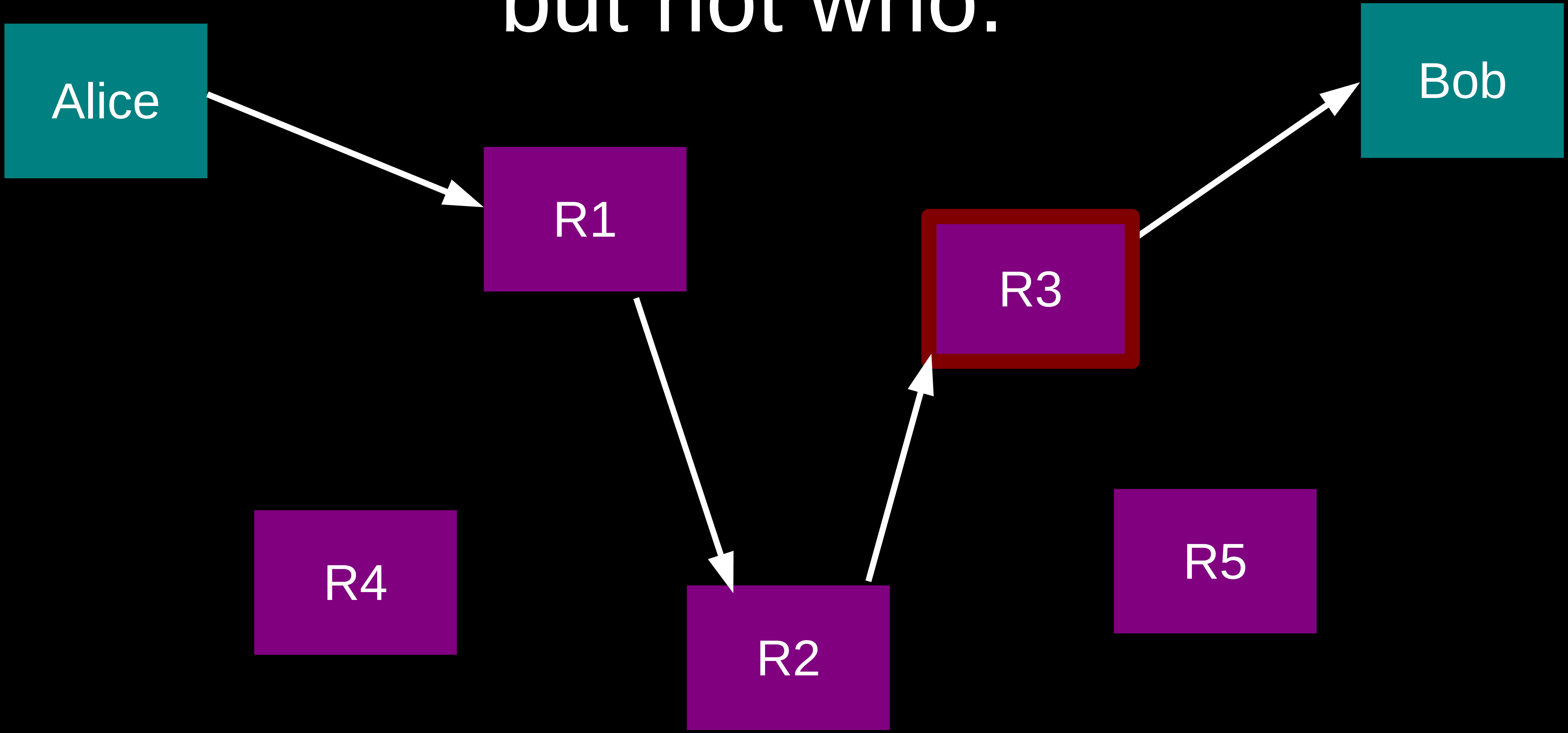
So, add multiple relays so that no single one can betray Alice.



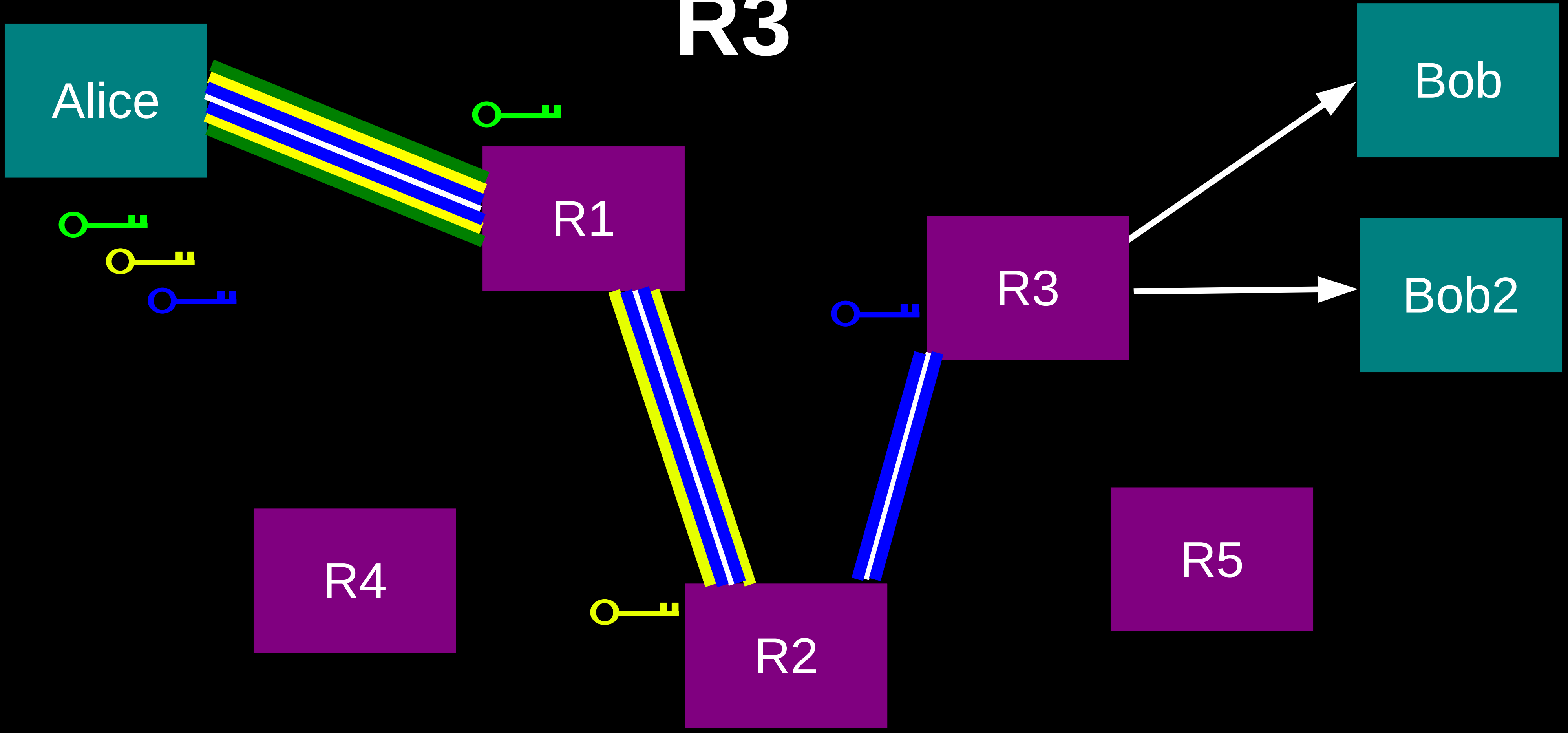
A corrupt first hop can tell that Alice is talking, but not to whom.



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?

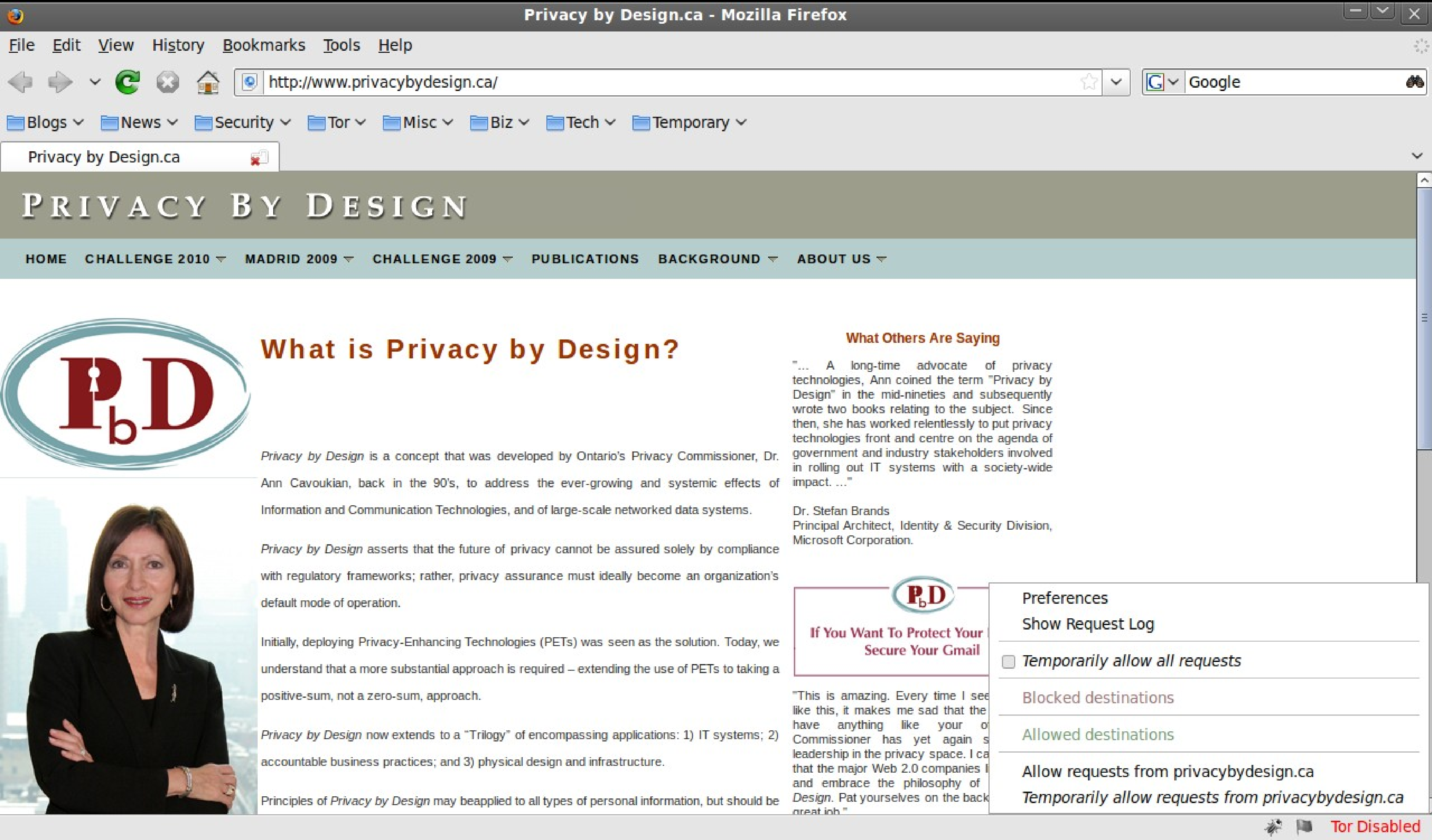
- Normal people
- Law Enforcement
- Human Rights Activists
- Business Execs
- Militaries
- Abuse Victims
- https://torproject.org/torusers

- 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
- *Examples*

Example 1: Pbd.ca



What is Privacy by Design?

Privacy by Design is a concept that was developed by Ontario's Privacy Commissioner, Dr. Ann Cavoukian, back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

Privacy by Design asserts that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we understand that a more substantial approach is required – extending the use of PETs to taking a positive-sum, not a zero-sum, approach.

Privacy by Design now extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and infrastructure.

Principles of *Privacy by Design* may beapplied to all types of personal information, but should be

What Others Are Saying

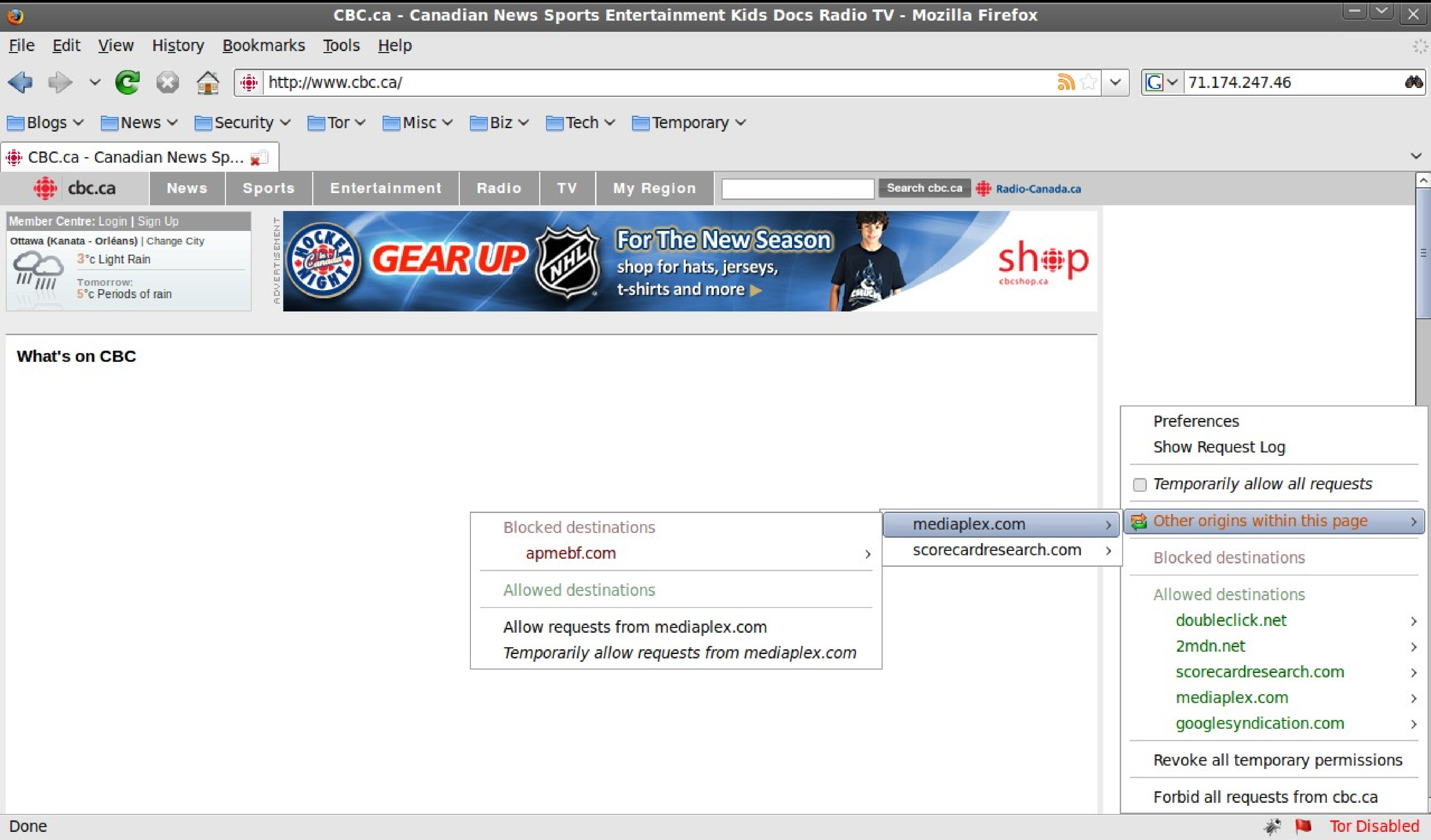
"... A long-time advocate of privacy technologies, Ann coined the term "Privacy by Design" in the mid-nineties and subsequently wrote two books relating to the subject. Since then, she has worked relentlessly to put privacy technologies front and centre on the agenda of government and industry stakeholders involved in rolling out IT systems with a society-wide impact. ..."

Dr. Stefan Brands
Principal Architect, Identity & Security Division,
Microsoft Corporation.

If You Want To Protect Your
Secure Your Gmail

"This is amazing. Every time I see
like this, it makes me sad that the
have anything like your o
Commissioner has yet again s
leadership in the privacy space. I ca
that the major Web 2.0 companies l
and embrace the philosophy of
Design. Pat yourselves on the back
great job."

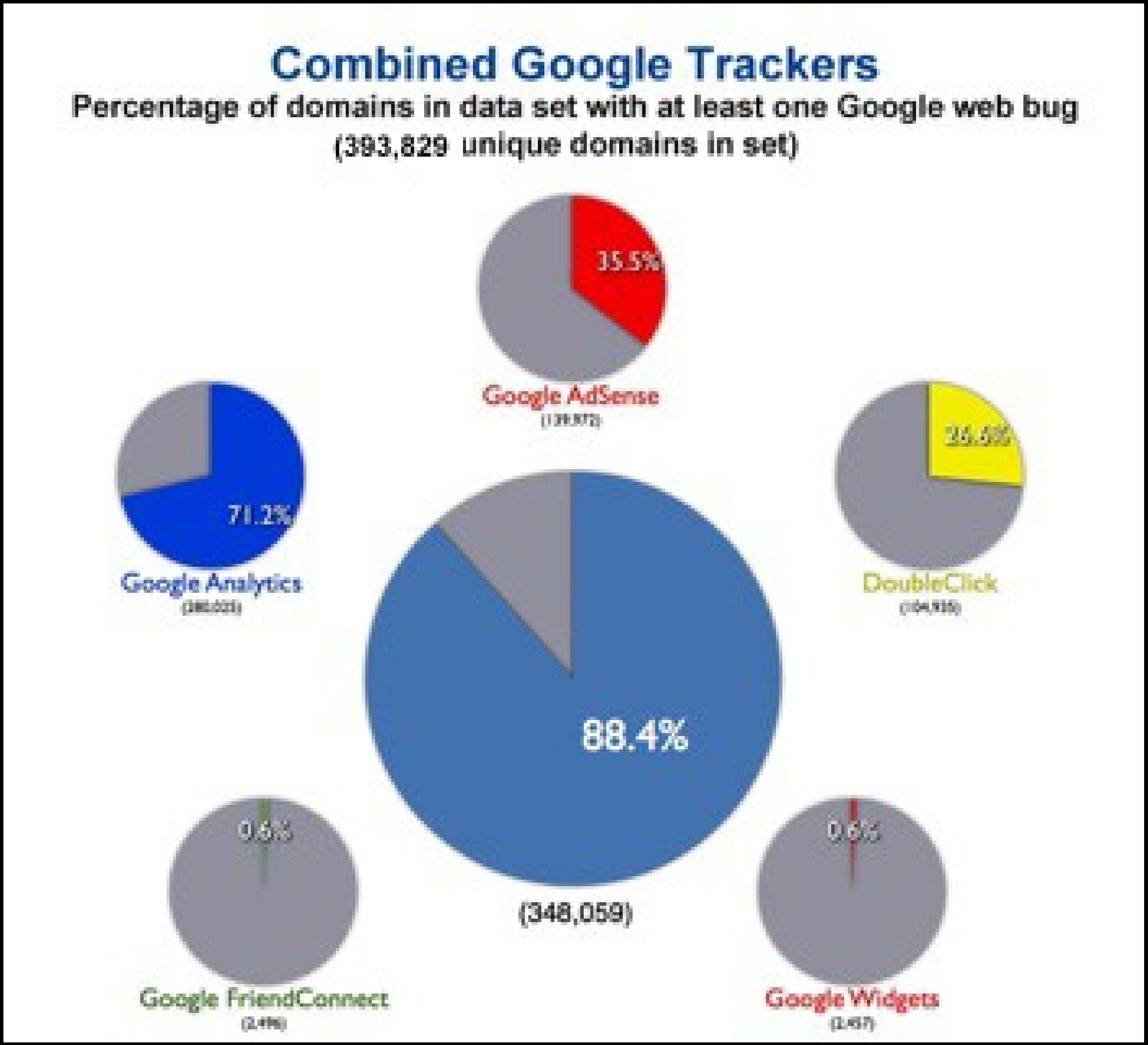
Example 2: cbc.ca



http://www.cbc.ca/

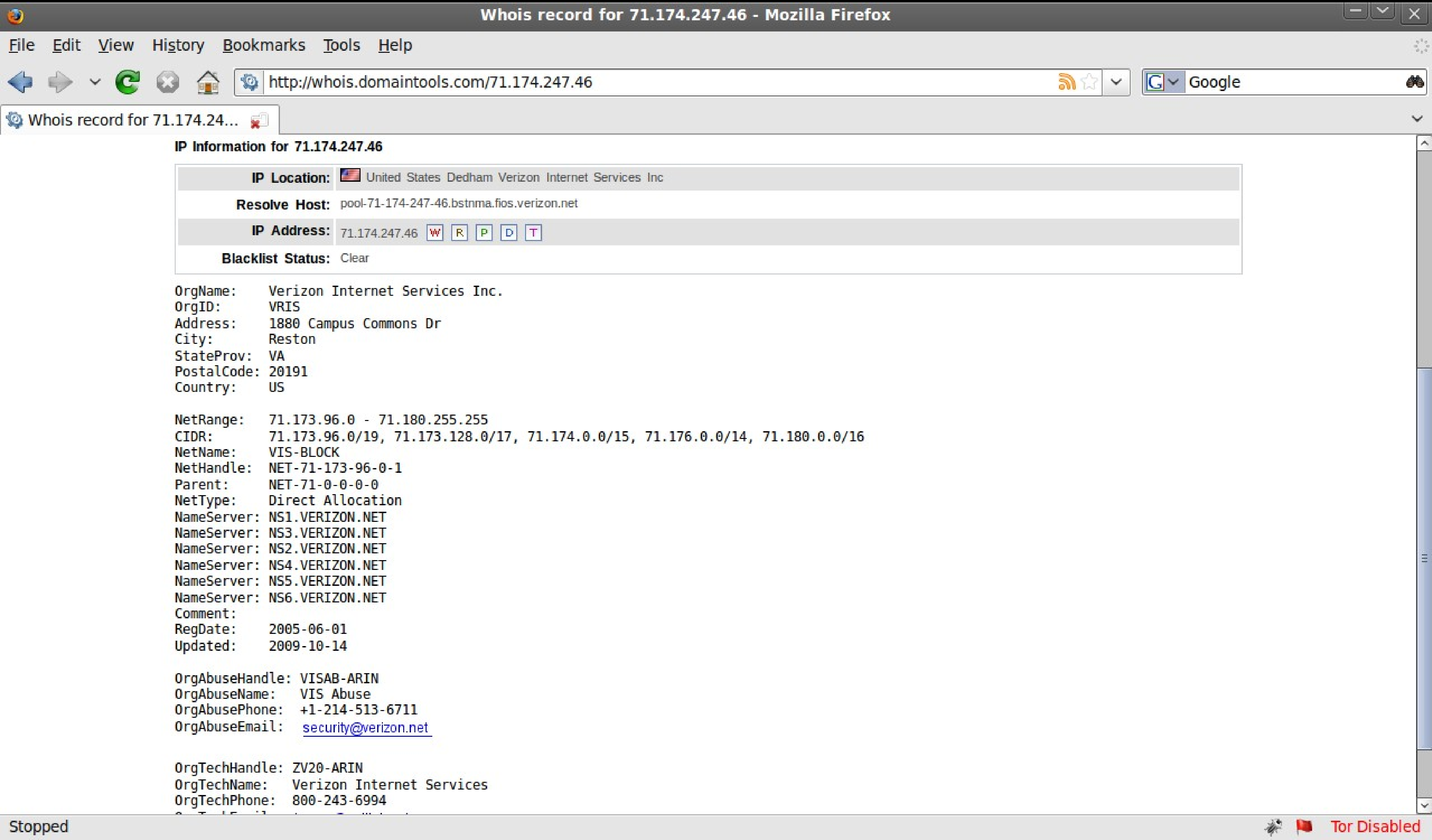
71.174.247.46

Advertising Network Reach



Source: http://www.knowprivacy.org/

IP Address Only?


Whois record for 71.174.247.46 - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
http://whois.domaintools.com/71.174.247.46
Google
Whois record for 71.174.24...
Stopped
Tor Disabled

IP Information for 71.174.247.46

IP Location:	United States Dedham Verizon Internet Services Inc
Resolve Host:	pool-71-174-247-46.bstnma.fios.verizon.net
IP Address:	71.174.247.46 W R P D T
Blacklist Status:	Clear

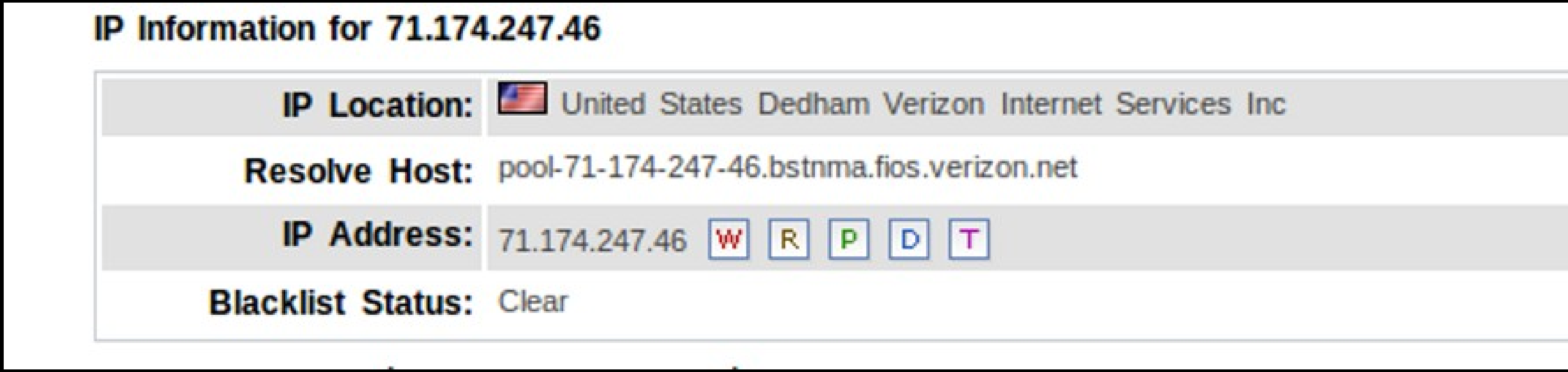
```
OrgName:    Verizon Internet Services Inc.
OrgID:      VRIS
Address:    1880 Campus Commons Dr
City:       Reston
StateProv:  VA
PostalCode: 20191
Country:    US

NetRange:   71.173.96.0 - 71.180.255.255
CIDR:       71.173.96.0/19, 71.173.128.0/17, 71.174.0.0/15, 71.176.0.0/14, 71.180.0.0/16
NetName:    VIS-BLOCK
NetHandle:  NET-71-173-96-0-1
Parent:     NET-71-0-0-0-0
NetType:    Direct Allocation
NameServer: NS1.VERIZON.NET
NameServer: NS3.VERIZON.NET
NameServer: NS2.VERIZON.NET
NameServer: NS4.VERIZON.NET
NameServer: NS5.VERIZON.NET
NameServer: NS6.VERIZON.NET
Comment:
RegDate:    2005-06-01
Updated:    2009-10-14

OrgAbuseHandle: VISAB-ARIN
OrgAbuseName:   VIS Abuse
OrgAbusePhone:  +1-214-513-6711
OrgAbuseEmail:  security@verizon.net

OrgTechHandle: ZV20-ARIN
OrgTechName:   Verizon Internet Services
OrgTechPhone:  800-243-6994
```

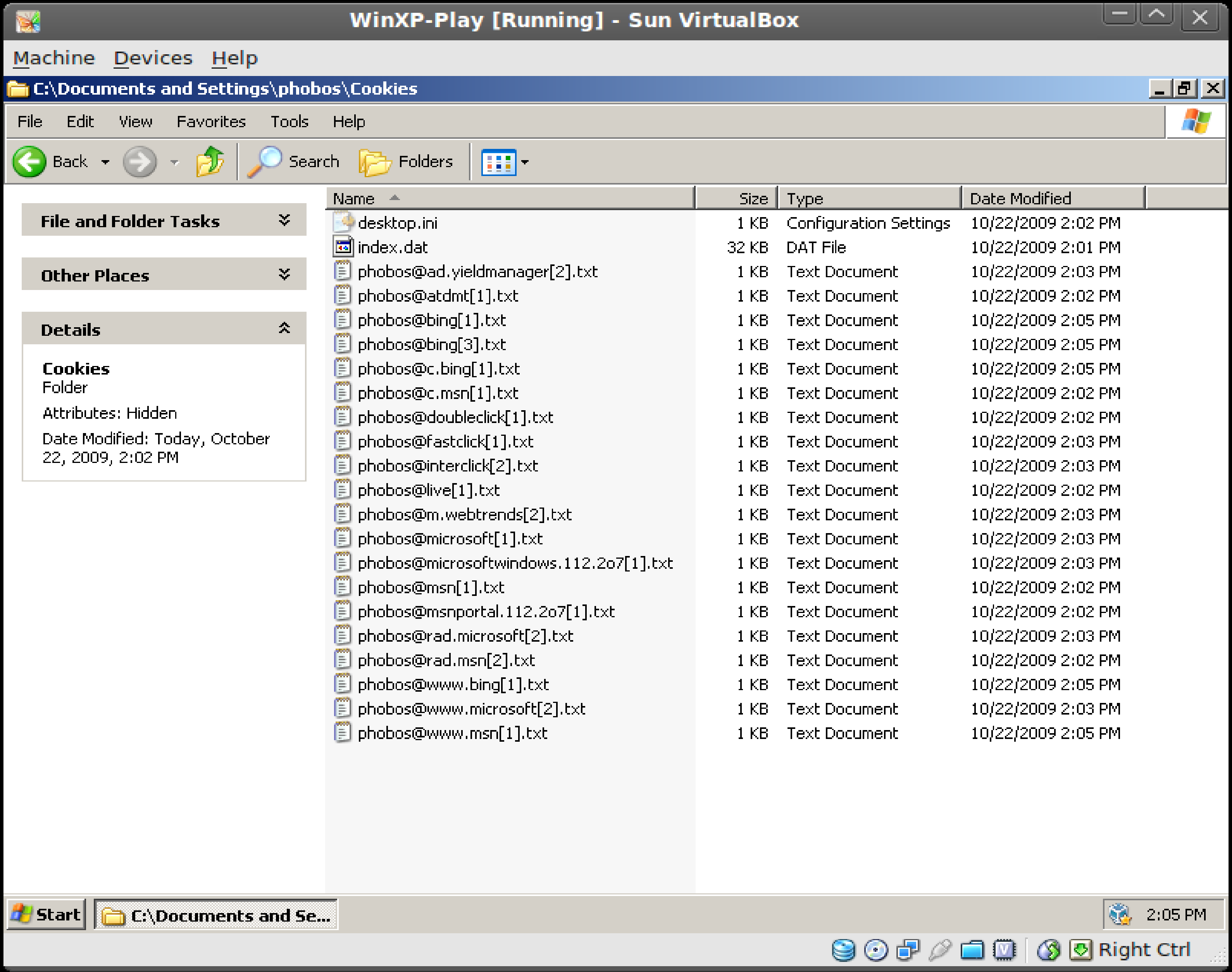
IP Address Detail



IP Information for 71.174.247.46

IP Location:	United States Dedham Verizon Internet Services Inc
Resolve Host:	pool-71-174-247-46.bstnma.fios.verizon.net
IP Address:	71.174.247.46 W R P D T
Blacklist Status:	Clear

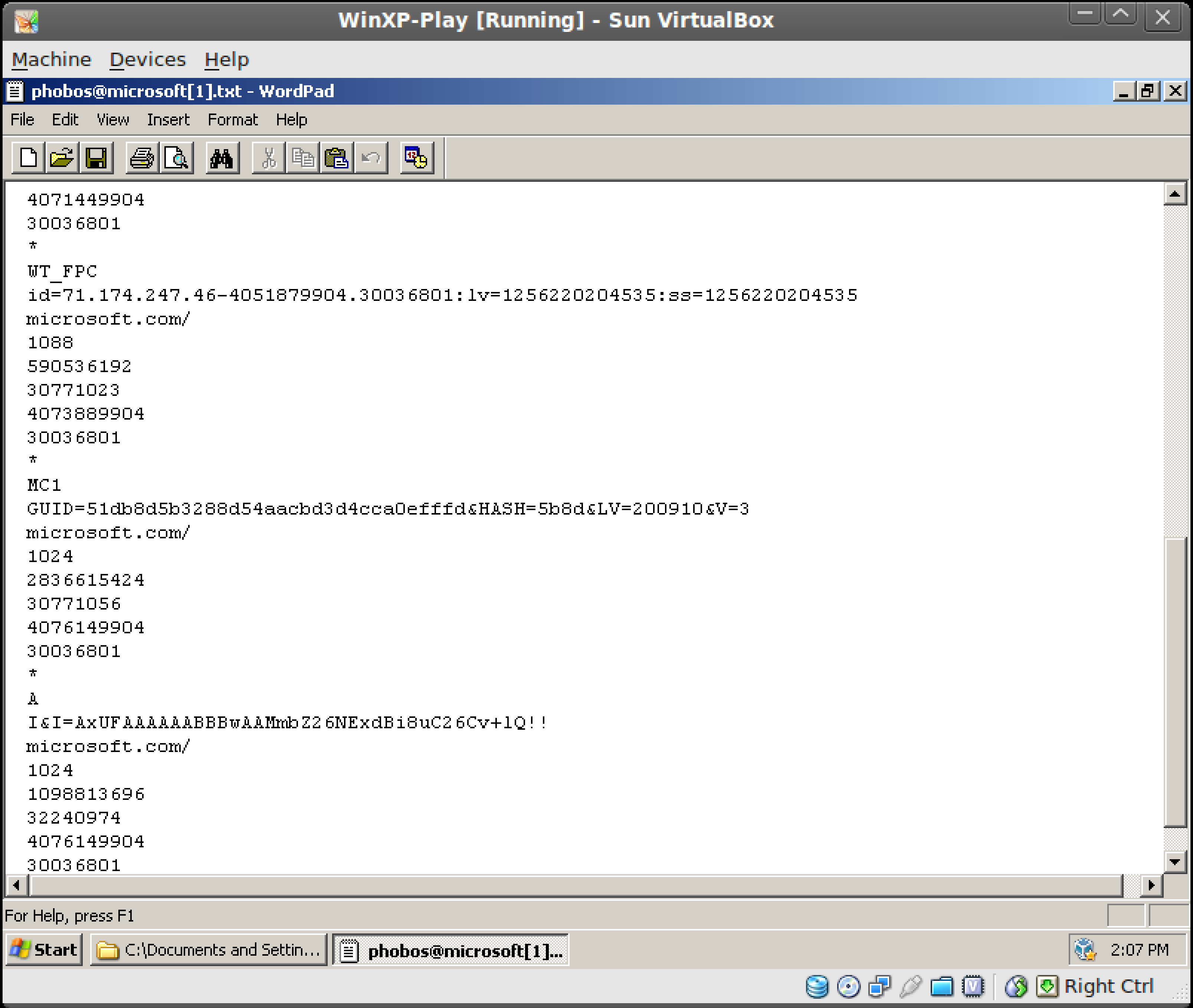
Cookies



Cookies
Folder
Attributes: Hidden
Date Modified: Today, October 22, 2009, 2:02 PM

Name	Size	Type	Date Modified
desktop.ini	1 KB	Configuration Settings	10/22/2009 2:02 PM
index.dat	32 KB	DAT File	10/22/2009 2:01 PM
phobos@ad.yieldmanager[2].txt	1 KB	Text Document	10/22/2009 2:03 PM
phobos@atdmt[1].txt	1 KB	Text Document	10/22/2009 2:02 PM
phobos@bing[1].txt	1 KB	Text Document	10/22/2009 2:05 PM
phobos@bing[3].txt	1 KB	Text Document	10/22/2009 2:05 PM
phobos@c.bing[1].txt	1 KB	Text Document	10/22/2009 2:05 PM
phobos@c.msn[1].txt	1 KB	Text Document	10/22/2009 2:02 PM
phobos@doubleclick[1].txt	1 KB	Text Document	10/22/2009 2:02 PM
phobos@fastclick[1].txt	1 KB	Text Document	10/22/2009 2:03 PM
phobos@interclick[2].txt	1 KB	Text Document	10/22/2009 2:03 PM
phobos@live[1].txt	1 KB	Text Document	10/22/2009 2:02 PM
phobos@m.webtrends[2].txt	1 KB	Text Document	10/22/2009 2:03 PM
phobos@microsoft[1].txt	1 KB	Text Document	10/22/2009 2:03 PM
phobos@microsoftwindows.112.2o7[1].txt	1 KB	Text Document	10/22/2009 2:03 PM
phobos@msn[1].txt	1 KB	Text Document	10/22/2009 2:02 PM
phobos@msnportal.112.2o7[1].txt	1 KB	Text Document	10/22/2009 2:02 PM
phobos@rad.microsoft[2].txt	1 KB	Text Document	10/22/2009 2:03 PM
phobos@rad.msn[2].txt	1 KB	Text Document	10/22/2009 2:02 PM
phobos@www.bing[1].txt	1 KB	Text Document	10/22/2009 2:05 PM
phobos@www.microsoft[2].txt	1 KB	Text Document	10/22/2009 2:03 PM
phobos@www.msn[1].txt	1 KB	Text Document	10/22/2009 2:05 PM

Cookie Details



WinXP-Play [Running] - Sun VirtualBox
Machine Devices Help
phobos@microsoft[1].txt - WordPad
File Edit View Insert Format Help

```
4071449904
30036801
*
WT_FPC
id=71.174.247.46-4051879904.30036801:lv=1256220204535:ss=1256220204535
microsoft.com/
1088
590536192
30771023
4073889904
30036801
*
MC1
GUID=51db8d5b3288d54aacbd3d4cca0efffd&HASH=5b8d&LV=200910&V=3
microsoft.com/
1024
2836615424
30771056
4076149904
30036801
*
A
I&I=AxUFAAAAAABBBwAAMmbZ26NExdBi8uC26Cv+1Q!!
microsoft.com/
1024
1098813696
32240974
4076149904
30036801
```

Summary

- Privacy policies are prone to mistakes and equivalent to promises
- Not having the data, nor being able to get it, is privacy by design
- You are your data trail; increasingly others make decisions about you based upon your data trail.

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