



Privacy, Anonymity, and Censorship Resistance

EECS 388: Intro to Security
University of Michigan

What's Privacy?

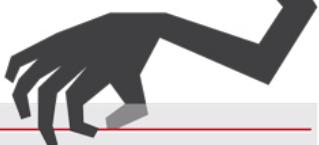
- Privacy is control over your own information
 - What do you have to hide?
 - Leads to the “What do you have to hide?” argument
- Privacy is the “right to be let alone” (Louis Brandeis)
- Privacy means something like what the Founders meant by “liberty”
 - It’s essential for free speech, free association, autonomy, freedom from censorship and constant surveillance
- Privacy-motivating examples in U.S. History
 - MLK “blackmailed” by FBI to get him to kill himself...
 - McCarthyism witch-hunt for communists

SURVEILLANCE UNDER THE PATRIOT ACT

Hastily passed 45 days after 9/11 in the name of national security...

The Patriot Act was the first of many changes to surveillance laws that made it easier for the government to spy on ordinary Americans by expanding the authority to monitor phone and email communications, collect bank and credit

reporting records, and track the activity of innocent Americans on the Internet. While most Americans think it was created to catch terrorists, the Patriot Act actually turns regular citizens into suspects.



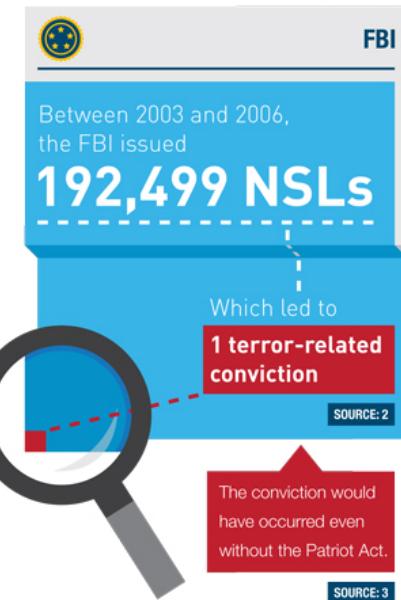
National Security Letters (NSLs) are issued by FBI agents, without a judge's approval, to obtain personal information...



"I want to deliver a warning... when the American people find out how their government has secretly interpreted the Patriot Act, they will be stunned and they will be angry."

Senator Ron Wyden (D-OR),
May 26, 2011

SOURCE: 1



NSL: National Security Letter

Used by the government to demand information about a person from ISPs, phone companies, etc...

No warrant required!

Image credit: ACLU

Surveillance under the PATRIOT Act

Abuse of Privacy:

The Patriot Act does not require information obtained by NSLs to be destroyed – even if the information is determined to concern innocent Americans.

At least **34,000** law enforcement and intelligence agents have access to phone records collected through NSLs.

YOUR INFO:
SAVED FOREVER

In response to 9 NSLs,
11,100 Americans' telephone account records were turned over to the FBI.

SOURCE: 4

The Patriot Act prohibits Americans who receive NSLs from telling anyone. These "gag order" provisions have been held unconstitutional in several legal cases.

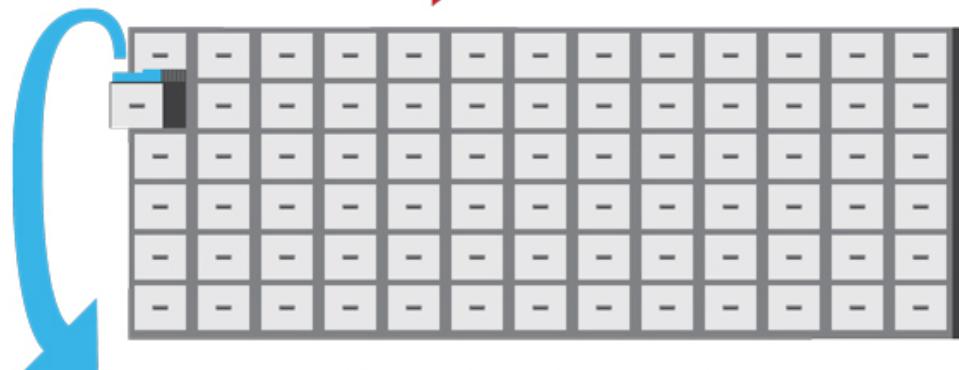


Image credit: ACLU

Surveillance under the PATRIOT Act

Between 2003 and 2005, the FBI made **53 reported criminal referrals to prosecutors** as a result of **143,074 NSLs**.

143,074 NSLs



53 REPORTED CRIMINAL REFERRALS:



17
were for
MONEY LAUNDERING



17
related to
IMMIGRATION



19
involved
FRAUD



0
were for
TERRORISM

SOURCE: 5

Image credit: ACLU

Google Transparency Report

Content requests (more significant than NSLs)

Reporting Period	Number of requests	Users/Accounts
January to June 2014	Data subject to six month reporting delay	
July to December 2013	0–999	15000–15999
January to June 2013	0–999	9000–9999
July to December 2012	0–999	12000–12999
January to June 2012	0–999	8000–8999
July to December 2011	0–999	9000–9999
January to June 2011	0–999	7000–7999
July to December 2010	0–999	5000–5999
January to June 2010	0–999	3000–3999
July to December 2009	0–999	3000–3999
January to June 2009	0–999	2000–2999

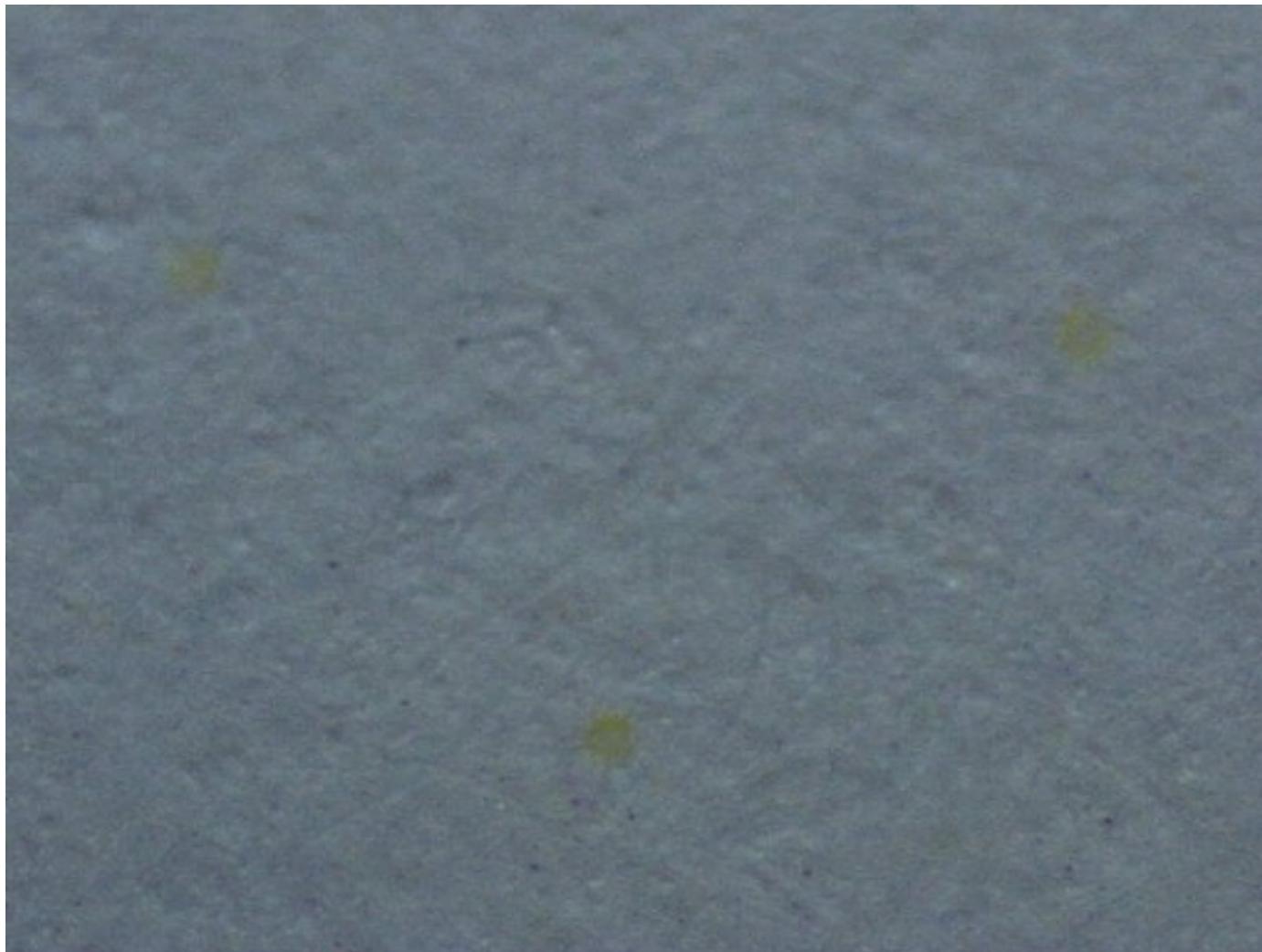
Typewriters & Privacy



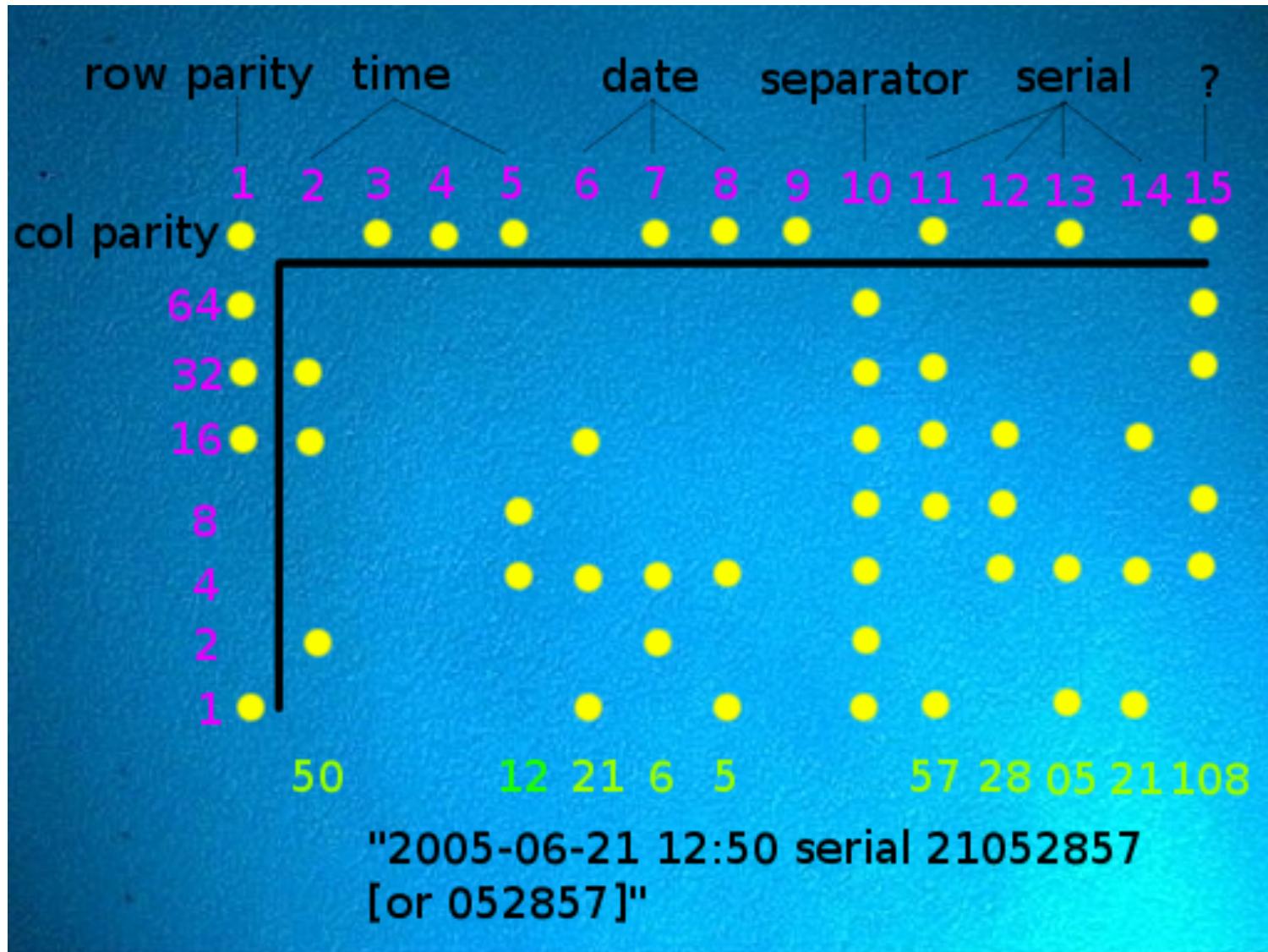
Modern day



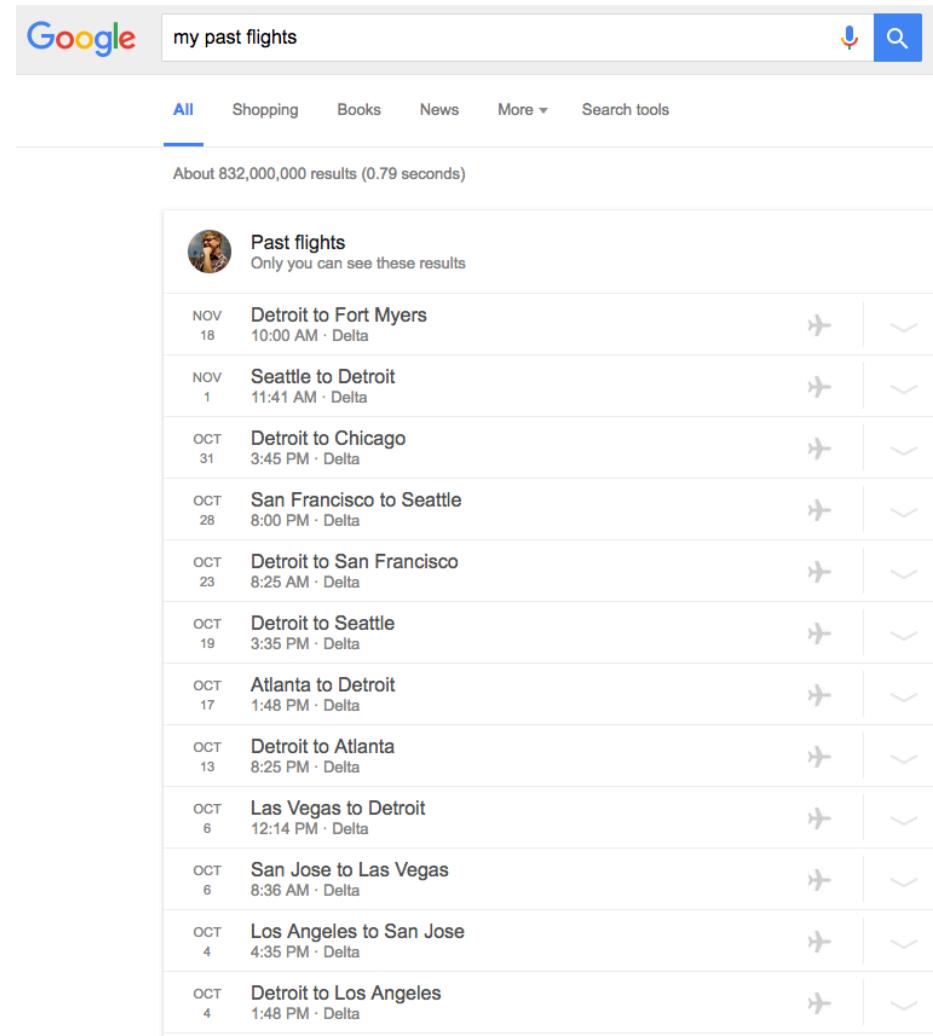
Printer Paper



What your printer reveals about you



Privacy Risks: “Direct” sharing



Google my past flights

All Shopping Books News More Search tools

About 832,000,000 results (0.79 seconds)

Past flights		Only you can see these results	
NOV 18	Detroit to Fort Myers 10:00 AM · Delta		
NOV 1	Seattle to Detroit 11:41 AM · Delta		
OCT 31	Detroit to Chicago 3:45 PM · Delta		
OCT 28	San Francisco to Seattle 8:00 PM · Delta		
OCT 23	Detroit to San Francisco 8:25 AM · Delta		
OCT 19	Detroit to Seattle 3:35 PM · Delta		
OCT 17	Atlanta to Detroit 1:48 PM · Delta		
OCT 13	Detroit to Atlanta 8:25 PM · Delta		
OCT 6	Las Vegas to Detroit 12:14 PM · Delta		
OCT 6	San Jose to Las Vegas 8:36 AM · Delta		
OCT 4	Los Angeles to San Jose 4:35 PM · Delta		
OCT 4	Detroit to Los Angeles 1:48 PM · Delta		

Privacy Risks: “Direct” sharing

BUSINESS
INSIDER

The Incredible Story Of How Target Exposed A Teen Girl's Pregnancy



GUS LUBIN

FEB. 16, 2012, 10:27 AM

Target broke through to a new level of customer tracking with the help of statistical genius Andrew Pole, according to a New York Times Magazine cover story by Charles Duhigg.

Pole identified 25 products that when purchased together indicate a woman is likely pregnant. The value of this information was that Target could send coupons to the pregnant woman at an expensive and habit-forming period of her life.

Plugged into Target's customer tracking technology, Pole's formula was a beast. Once it even exposed a teen girl's pregnancy:

[A] man walked into a Target outside Minneapolis and demanded to see the manager. He



You might also like...



Roll over image to zoom in

First Response Early Result Pregnancy Test, 3 tests, Packaging May Vary

by First Response

4.5 out of 5 stars 486 customer reviews | 17 answered questions

#1 Best Seller in Pregnancy Tests

47 Amazon Students rated this highly



List Price: \$49.57

Price: \$12.98 & Free Returns. [Details](#)

You Save: \$6.59 (34%)

Note: Available at a lower price from [other sellers](#), potentially without free Prime shipping.

In Stock.

Ships from and sold by Amazon.com. Gift-wrap available.

Want it Tuesday, March 24? Order within 29 hrs 56 mins and choose One-Day Shipping at checkout. [Details](#)

Package Quantity: 1

1
\$12.98

2
\$41.00

3
\$57.99

Customers Who Bought This Item Also Bought

Page 6 of 14 | [Start over](#)



Vitafusion Prenatal DHA and Folic Acid Gummy Vitamins, 180 Count
4.5 out of 5 stars 140
\$20.25



One A Day Women's Prenatal One Pill, 30 Count
4.5 out of 5 stars 18
\$13.48



Mayo Clinic Guide to a Healthy Pregnancy...
the pregnancy experts...
4.5 out of 5 stars 804
#1 Best Seller in Motherhood



Summer's Eve Cleansing Wash, Morning Paradise, 15 Ounce
4.5 out of 5 stars 44
\$3.99



Nexcare 524560 Basal Digital Thermometer
4.5 out of 5 stars 19
\$14.06



Nature Made Prenatal Multi Vitamin Value Size, Tablets, 250-Count
4.5 out of 5 stars 213
\$16.79



Trojan Condom Pleasure Pack Lubricated, 40 Count
4.5 out of 5 stars 126
\$18.12

Privacy Risks: Third-party tracking

≡ COSMOPOLITAN LOVE | CELEBS | BEAUTY & STYLE | FITNESS SEARCH

18 Things You Should Know Before Dating a Cat Lady

She knows the difference between a guy who's allergic to cats and a guy who's "allergic to cats."

By Anna Breslaw

12.3k Shares

f SHARE 12.2K
t TWEET 46
p PIN 6

MOST READ

THE BEDROOM BLOG 

Does Seafood Make Guys Horny?

 Instagram

 f t p

1. First of all, define "cat lady." Does one cat = cat lady? Two cats = cat lady? Does joking about being a cat lady à la sparkling, outgoing multimillionaire Taylor Swift automatically make one a cat lady? It is my personal belief that most female cat owners below the age of 40 fall into the "not a cat girl, not yet a cat lady" category.

2. Cat ladies mostly look like ... normal ladies. You know. Like regular women. Not like the old bag who sits in front of your local Shop Rite with aluminum foil on her head.

Blocking with Tools

The screenshot shows the Ghostery extension interface. At the top, it says "Ghostery found 13 trackers" for the website "www.cnn.com". Below this, there is a list of trackers with their descriptions and blocking controls:

- ClickTale (Analytics, Analytics, Behavior Tracking) - Blocking status: Enabled (red switch)
- DoubleClick (Advertising) - Blocking status: Enabled (red switch)
- Facebook Connect (Widgets, Social) - Blocking status: Enabled (red switch)
- Gravity Insights (Analytics) - Blocking status: Enabled (red switch)
- Krux Digital (Beacons) - Blocking status: Enabled (red switch)
- Livefyre (Widgets, Commenting System) - Blocking status: Enabled (red switch)

At the bottom of the interface are three buttons: "Pause Blocking", "Whitelist Site", and a question mark icon.

The screenshot shows the Privacy Badger extension interface. It features a red badger icon and the text "Privacy Badger is protecting you on this page. These sliders let you control how privacy badger handles each tracker." Below this, there is a list of domains with corresponding sliders:

- api-public.addthis.com (Slider: mostly green)
- ct1.addthis.com (Slider: mostly green)
- m.addthis.com (Slider: mostly green)
- s7.addthis.com (Slider: mostly green)
- googleads.g.doubleclick.net (Slider: mostly red)
- themes.googleusercontent.com (Slider: mostly green)
- www.google.com (Slider: yellow and green)

At the bottom of the interface are three buttons: "Disable Privacy Badger for This Site", "Deactivate Privacy Badger", and "What is Privacy Badger?"

Third-party cookies

- Site A's page requests a third-party resource (image, script, iframe)
 - Normally, browser sends cookie associated with that third-party in that request



Cookie: ID=784c39
Referrer: cnn.com/



Third-party cookies

- Site A's page requests a third-party resource (image, script, iframe)
 - Normally, browser sends cookie associated with that third-party in that request



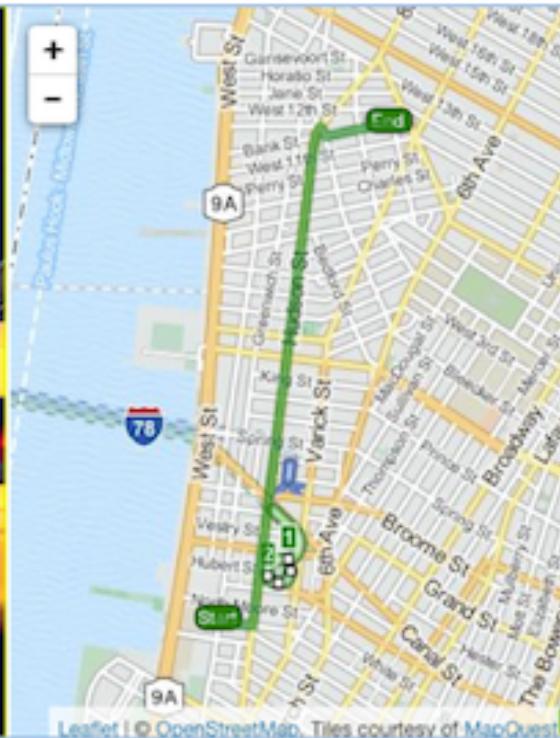
NYC Taxi Data



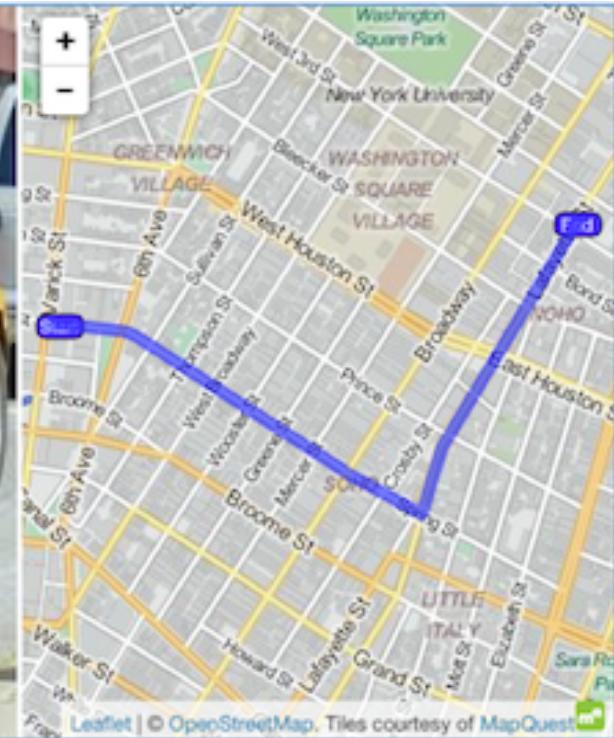
NYC Taxi – Tracking Celebrities



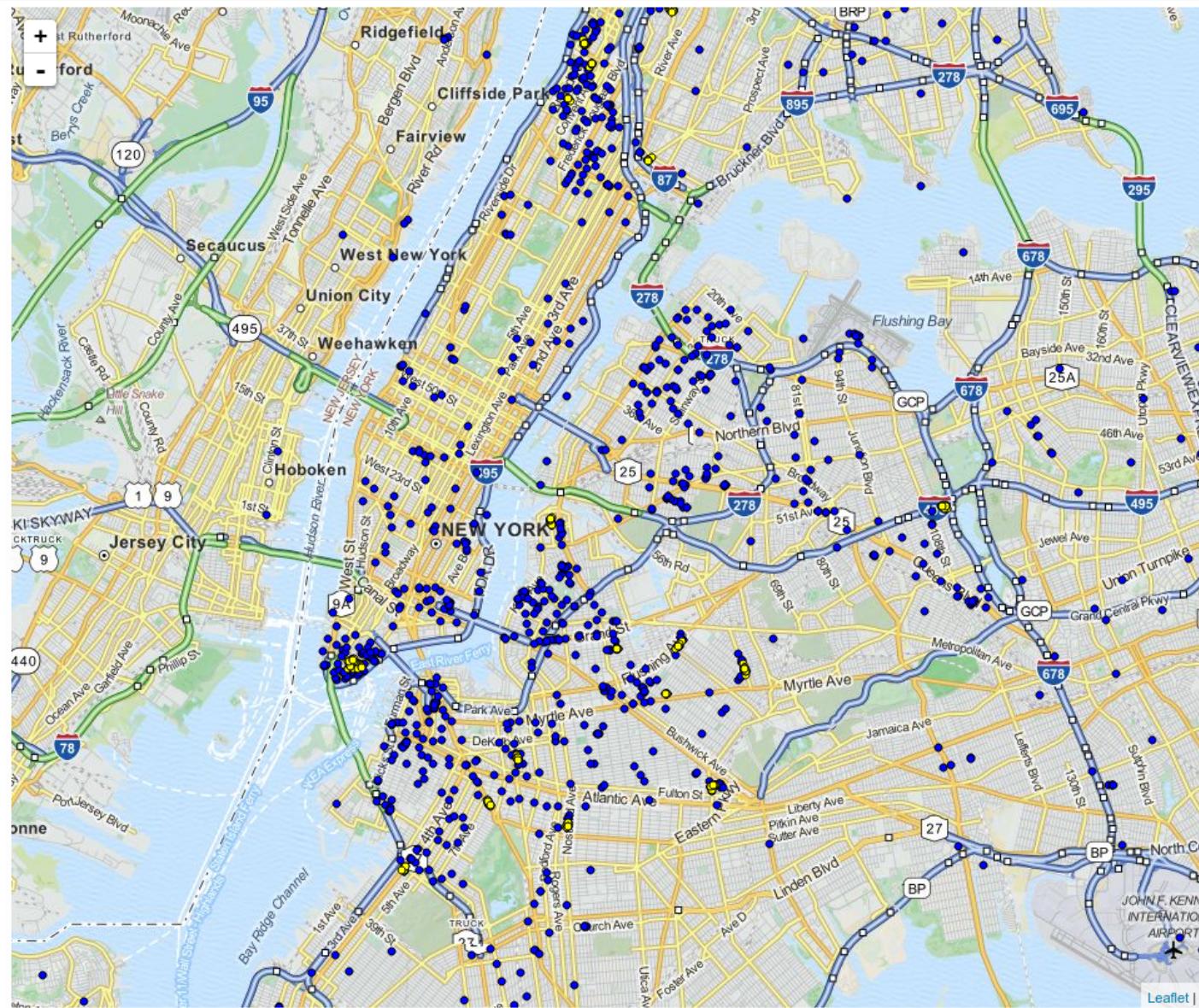
Bradley Cooper



Jessica Alba



NYC Taxi – Strip Club drop-offs



AOL Search Data Publication

98280	prayers to break curses	2006-04-09 5	
98280	prayers for cleansing	2006-04-09 2	
98280	prayers for defeating enemy	2006-04-09 1	
98280	bible scriptures for defeating the enemy	2006-04-09 4	
98280	prayers to plead the blood of jesus against problems	2006-04-09 2	
98280	prayers to plead the blood of jesus against problems	2006-04-09 1	
98280	prayers to plead the blood of jesus against problems	2006-04-09 3	
98280	how does a male's cocaine use affect a fetus	2006-04-10 1	
98280	how does a male's cocaine use affect a fetus	2006-04-10 5	
98280	birth defects caused by father's cocaine use	2006-04-10 1	
98280	birth defects caused by father's cocaine use	2006-04-10 4	
98280	are chainletter scams ever successful	2006-04-10 0	
4417749	clothes for age 60		9062176 13092305 south bend indiana time change ;
4417749	60 single men		9062177 13092305 www.cornholegamer.com 2006-05-10
4417749	best retirement city		9062178 13092305 www.cornholegamer.com 2006-05-10
4417749	jarret arnold		9062179 13092305 www.cornholegamer.com 2006-05-10
4417749	jack t. arnold		9062180 13092305 obtaining a real estate license ;
4417749	jaylene and jarrett arnold		9062181 13092305 obtaining an indiana real estate
4417749	gwinnett county yellow pages		9062182 13092305 evanescence song my immortal 201
4417749	rescue of older dogs		9062183 13092352 ebay.com 2006-03-11 14:22:02 8
4417749	movies for dogs		9062184 13092352 babe 20ruth 2006-03-11 14:30:19
4417749	sinus infection		9062185 13092352 babe 20ruth 2006-03-11 14:32:48
			9062186 13092352 babe 20ruth 2006-03-11 14:32:51
			9062187 13092352 amazon 20.com 2006-03-11 15:13
			9062188 13092352 amazon.com 2006-03-11 15:15:49
			9062189 13092352 priceline.com 2006-03-14 12:23:21
			9062190 13092352 priceline.com 2006-03-18 15:11:1
			9062191 13092352 newark 20airport 2006-05-22 15:
			- 2006-05-22 15:44:32
			9062192 13092352 newark airport 2006-05-22 15:47
			9062193 13092352 newark airport 2006-05-22 15:47
			9062194 13092352 car 20rental 2006-05-22 15:55:0
			9062195 13092352 car rental 2006-05-22 15:56:13
			9062196 13092352 car rental 2006-05-22 15:56:16
			9062197 13092352 car rental 2006-05-22 15:56:16
			9062198 13092352 dollar 20rent 20a 20car 2006-05-
			9062199 13092589 excel rims 2006-03-11 13:50:26 :
			9062200 13092589 google 2006-03-12 02:04:12 1 ht
			9062201 13092589 exciel rims 2006-03-12 02:21:43
			9062202 13092589 excel rims 2006-03-12 02:22:13
			9062203 13092589 excel dirt bike rims 2006-03-12
			9062204 13092589 google 2006-04-09 22:25:39 1 ht
			9062205 13092589 ak474sale 2006-04-09 23:38:29
			9062206 13092589 ak474sale 2006-04-09 23:38:49
			9062207 13092589 guns 2006-04-09 23:39:11

AOL Search Data Leak

A Face Is Exposed for AOL Searcher No. 4417749

By MICHAEL BARBARO and TOM ZELLER Jr.
Published: August 9, 2006

Buried in a list of 20 million Web search queries collected by AOL and recently released on the Internet is user No. 4417749. The number was assigned by the company to protect the searcher's anonymity, but it was not much of a shield.



Erik S. Lesser for The New York Times
Thelma Arnold's identity was betrayed by AOL records of her Web searches, like ones for her dog, Dudley, who clearly has a problem.

No. 4417749 conducted hundreds of searches over a three-month period on topics ranging from "numb fingers" to "60 single men" to "dog that urinates on everything."

And search by search, click by click, the identity of AOL user No. 4417749 became easier to discern. There are queries for "landscapers in Lilburn, Ga., several people with the last name Arnold and "homes sold in shadow lake subdivision gwinnett county georgia."

It did not take much investigating to follow that data trail to Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga., frequently researches her friends' medical ailments and loves her three dogs. "Those are my searches," she said, after a reporter read part of the list to her.

AOL removed the search data from its site over the weekend and apologized for its release, saying it was an unauthorized move by a team that had hoped it would benefit academic researchers.

But the detailed records of searches conducted by Ms. Arnold and 657,000 other Americans, copies of which continue to circulate online, underscore how much people unintentionally reveal about themselves when they use search engines — and how risky it can be for companies like AOL, [Google](#) and [Yahoo](#) to compile such data.

Those risks have long pitted privacy advocates against online marketers and other

SIGN IN TO E-
MAIL THIS

PRINT

REPRINTS



Multimedia

Graphic: What Revealing Search Data Reveals

Data Privacy Defenses

- k-anonymity
 - Ensure that each record is *indistinguishable* from at least $k - 1$ other records.
 - Make use of quasi-identifiers (e.g., ZIP, DOB, etc)
 - Further, reduce granularity (partial zip codes, year of birth)

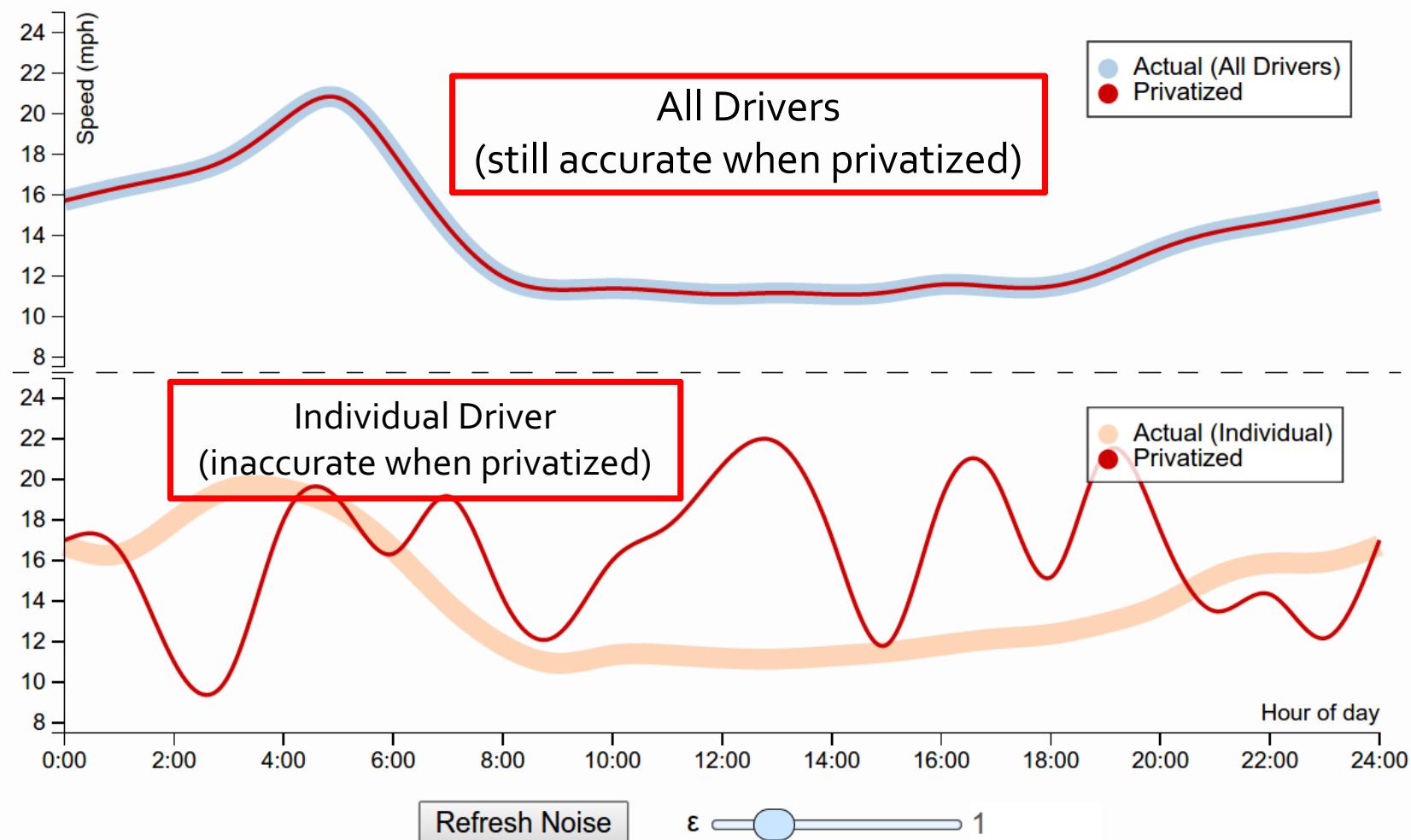
k-anonymity

ZIP	DOD	Disease
902**	1987	Cancer
902**	1987	Cancer
902**	1987	Cancer
902**	1954	Heart Disease
902**	1954	GI Disease
902**	1954	Died of poison apple
904**	1978	Heart Disease
904**	1978	Cancer
904**	1978	Cancer

Another option: Differential Privacy

- Instead of providing whole data set, provide an **algorithm** for answering queries:
 - A differentially private algorithm is insensitive to single-row changes
 - $A(Data[0:n - 1]) \approx A(Data[0:n])$
 - Basically, add (bounded) noise to A()
- Computation of A() happens at dataset
- Noise: tradeoff between usability and privacy
- This is an active area of research.

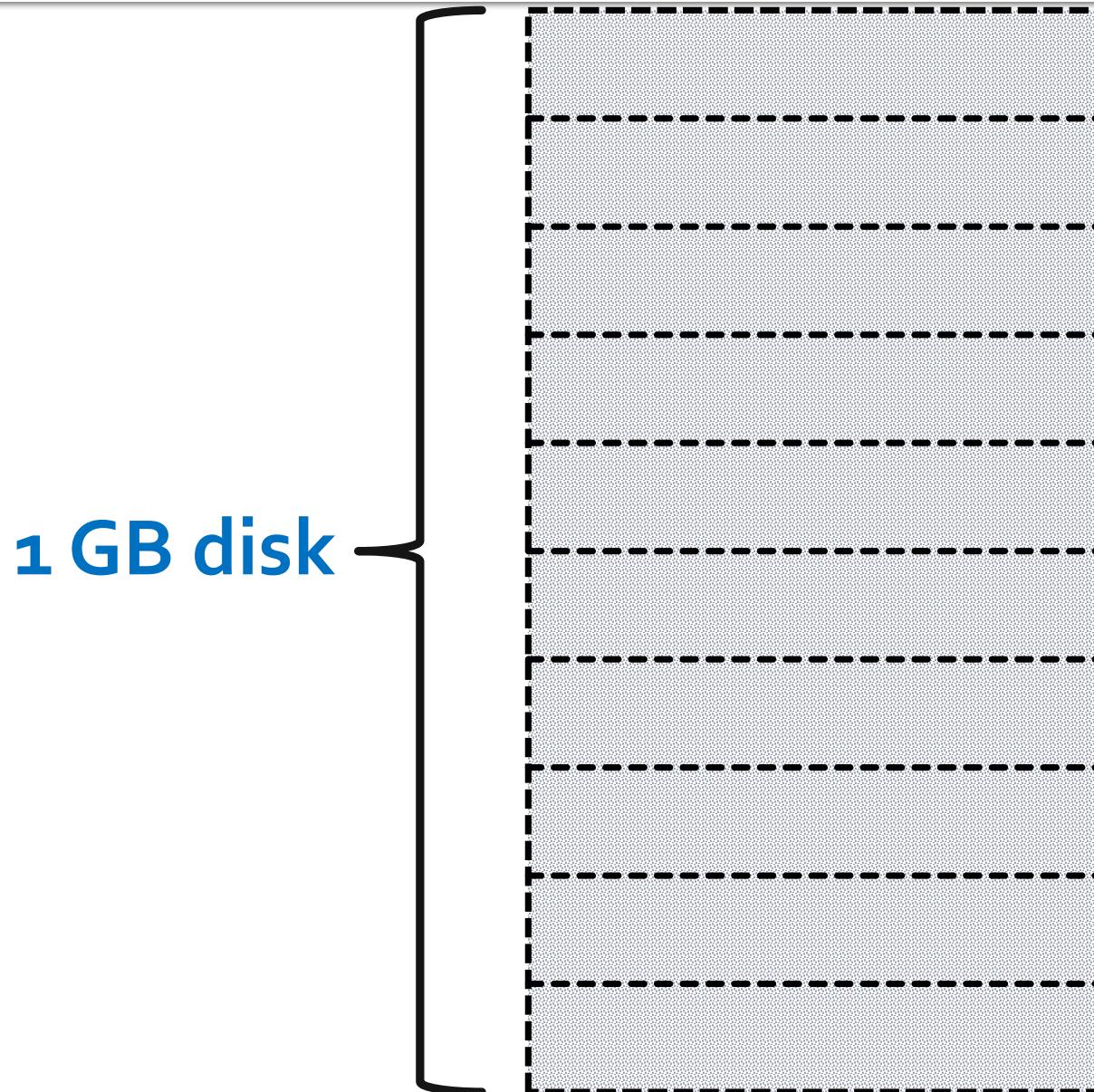
Differential Privacy



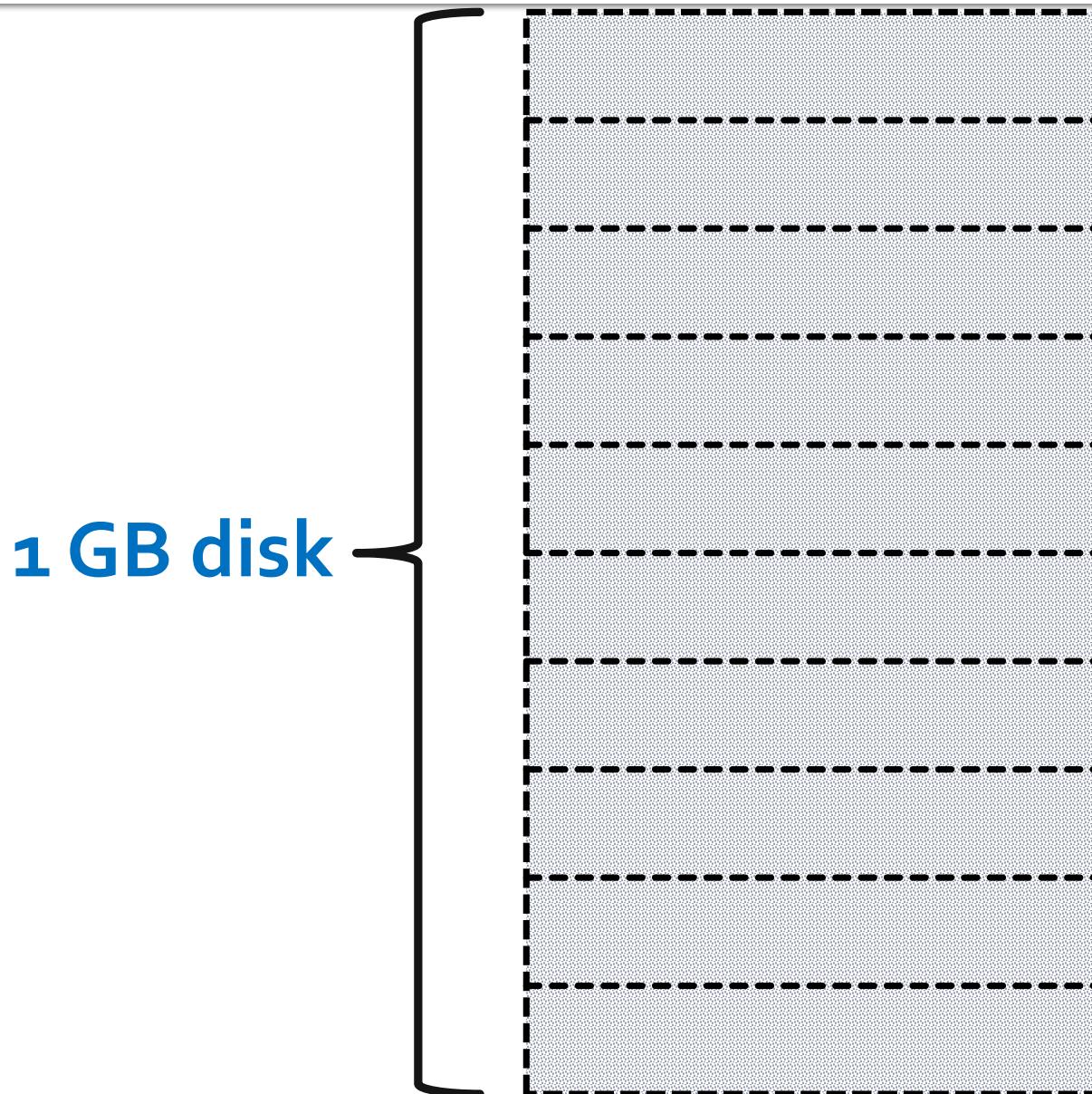
Privacy Defenses: Encrypt your filesystem(s)



Rubberhose File System



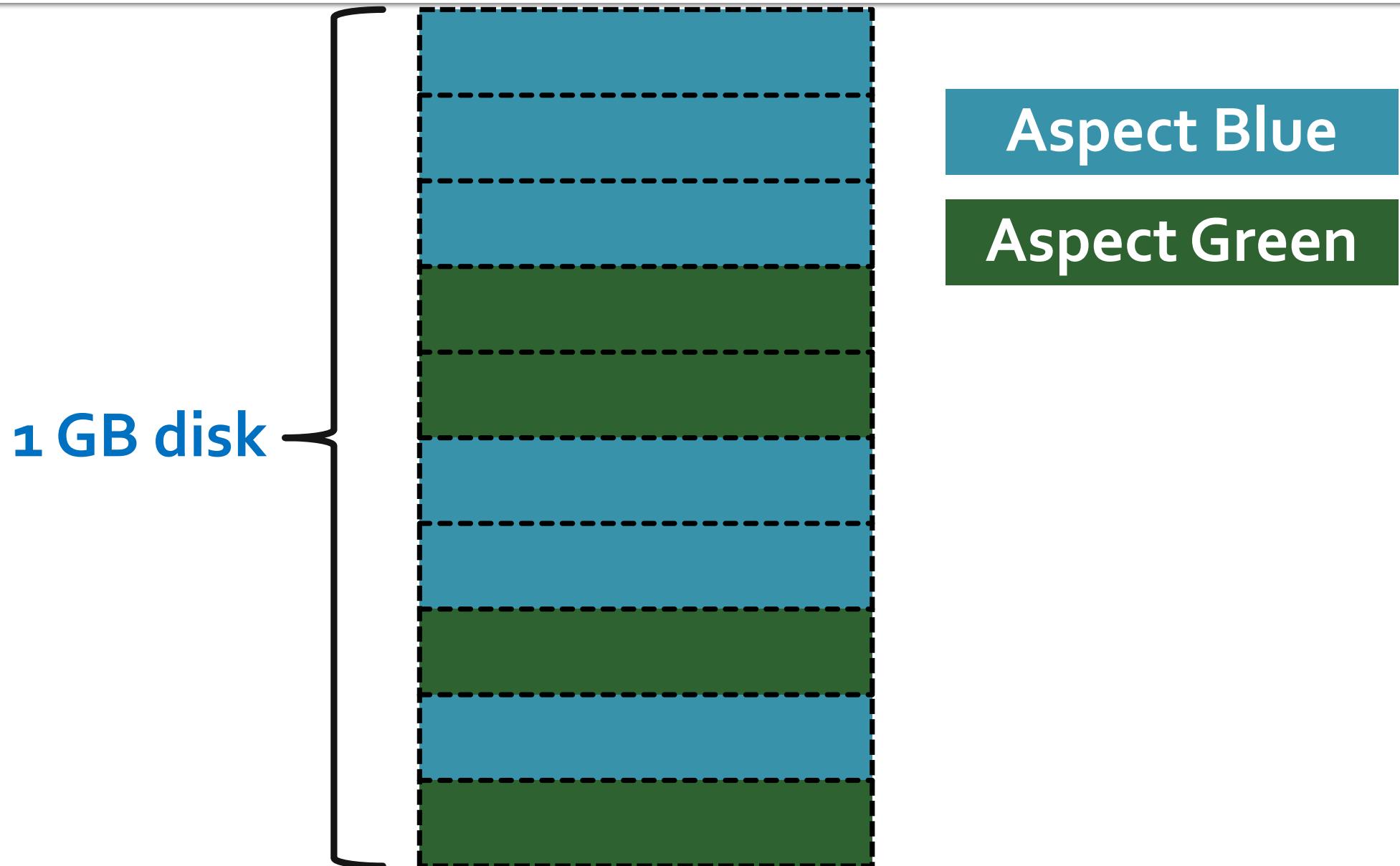
Rubberhose File System



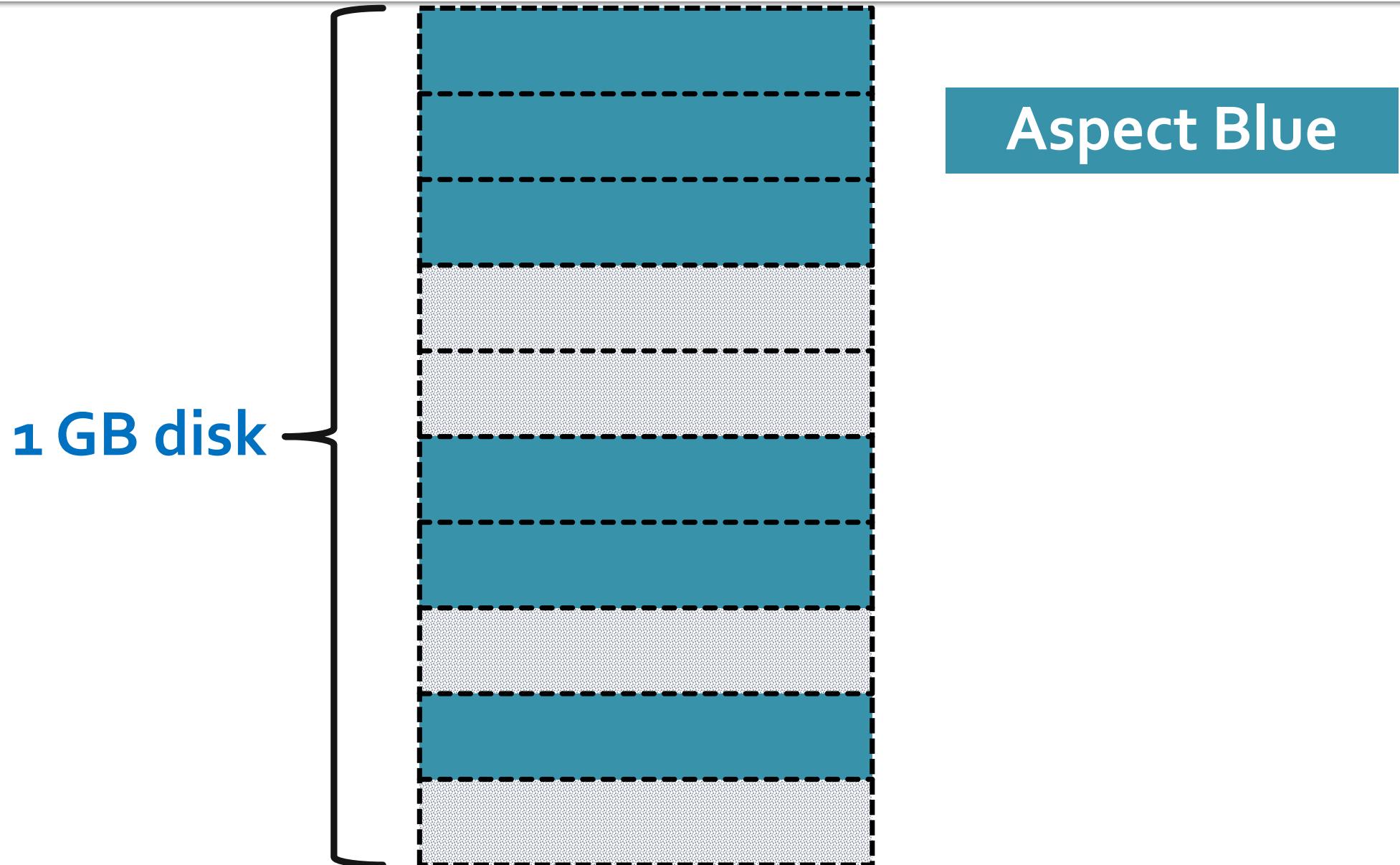
Aspect Blue

Aspect Green

Rubberhose File System



Rubberhose File System



Rubberhose File System



Apple vs FBI

- FBI wanted Apple to electronically sign new software that would enable the FBI to unlock a dead shooters iPhone 5c
- Phone is encrypted with key derived from passcode, phone wipes itself after N incorrect guesses
- FBI wanted software that removed the guess limit
 - Not possible on iPhone 6 (guess enforced in hardware)
- The FBI ultimately bought a vulnerability from a cyber-arms dealer to break into the phone

Apple vs FBI: Arguments

- Pro Apple:
 - Increases risk of crypto implementation errors
 - Exposes legitimate users to potential gov't abuse
 - Either gives foreign competitors an advantage, or gives foreign governments opportunity for abuse
- Pro FBI:
 - Laws do allow access with appropriate court order
 - Think of the children!

Encrypted Mail: PGP

- Modern implementations: GnuPG, Keybase
- Each user has:
 - A public encryption key, paired with a private decryption key
 - A private signature key, paired with a public verification key

Encrypted Mail: PGP

To send a message:

- Sign with your signature key
- Encrypt message and signature with recipient's public encryption key

To receive a message:

- Decrypt with your private key to get message and signature
- Use sender's public verification key to check sig

Encrypted Mail: PGP

- How do you obtain Bob's public key?
 - Get it from Bob's website? (☹)
 - Get it from Bob's website, verify using out-of-band communication
 - Keys are unwieldy → use **fingerprints** instead
 - A fingerprint is a cryptographic hash of a key
 - What if you don't personally know Bob?
 - Web of Trust (WoT)
 - Social Network (Keybase)

PGP Drawbacks

- Metadata is not encrypted
 - Sender, receiver, time sent, approx. msg length, subject, etc...
- What if Bob's machine was compromised?
 - His private key material becomes known
 - Past messages can be decrypted and read
 - Senders of email to Bob must trust his ability and desire to keep their messages private (which he did not do...)

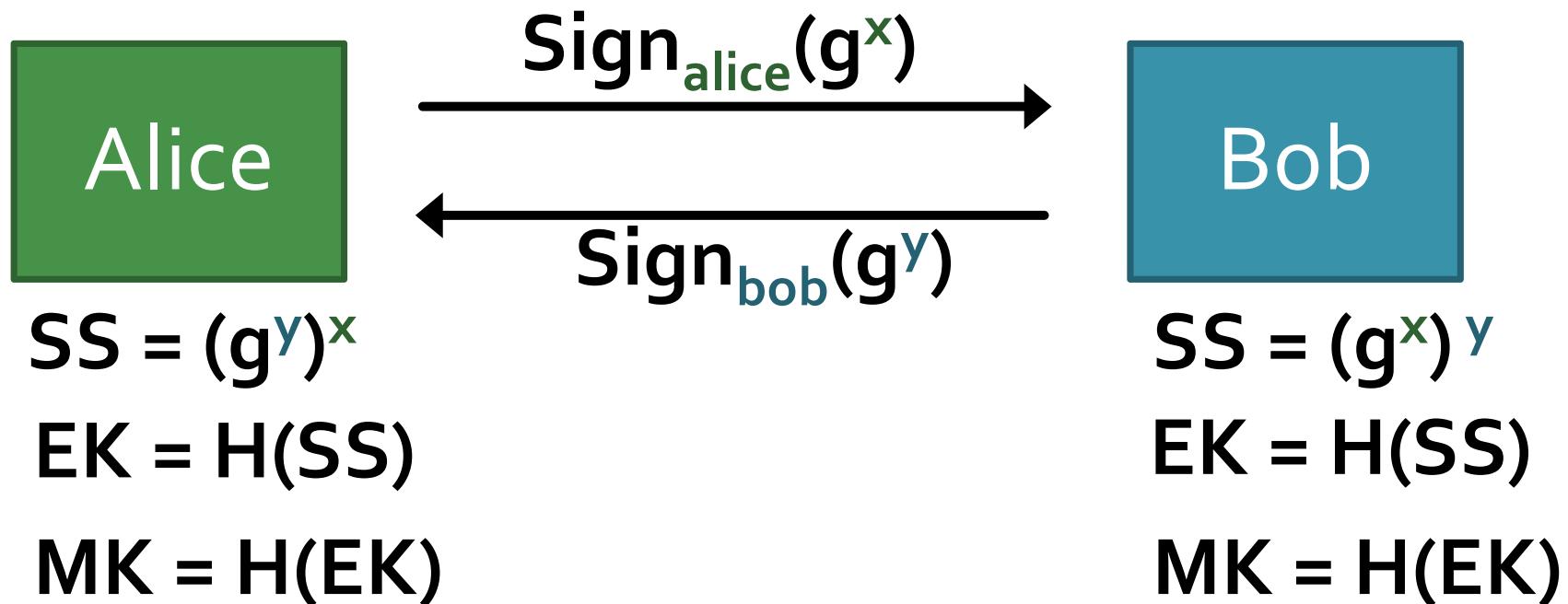
Off-the-Record (OTR) Messaging

Motivation: Alice and Bob want to communicate securely online (say via chat)



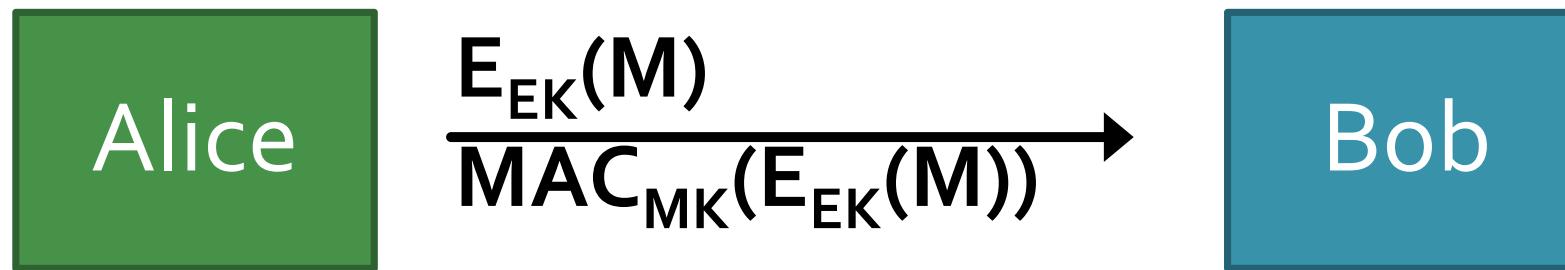
Off-the-Record (OTR) Messaging

1. Use *authenticated* Diffie-Hellman to establish a Shared Secret and then two, short-lived session keys (i.e. for Encryption and MAC)



Off-the-Record (OTR) Messaging

2. Then use *symmetric* encryption on message M and authenticate using a MAC.



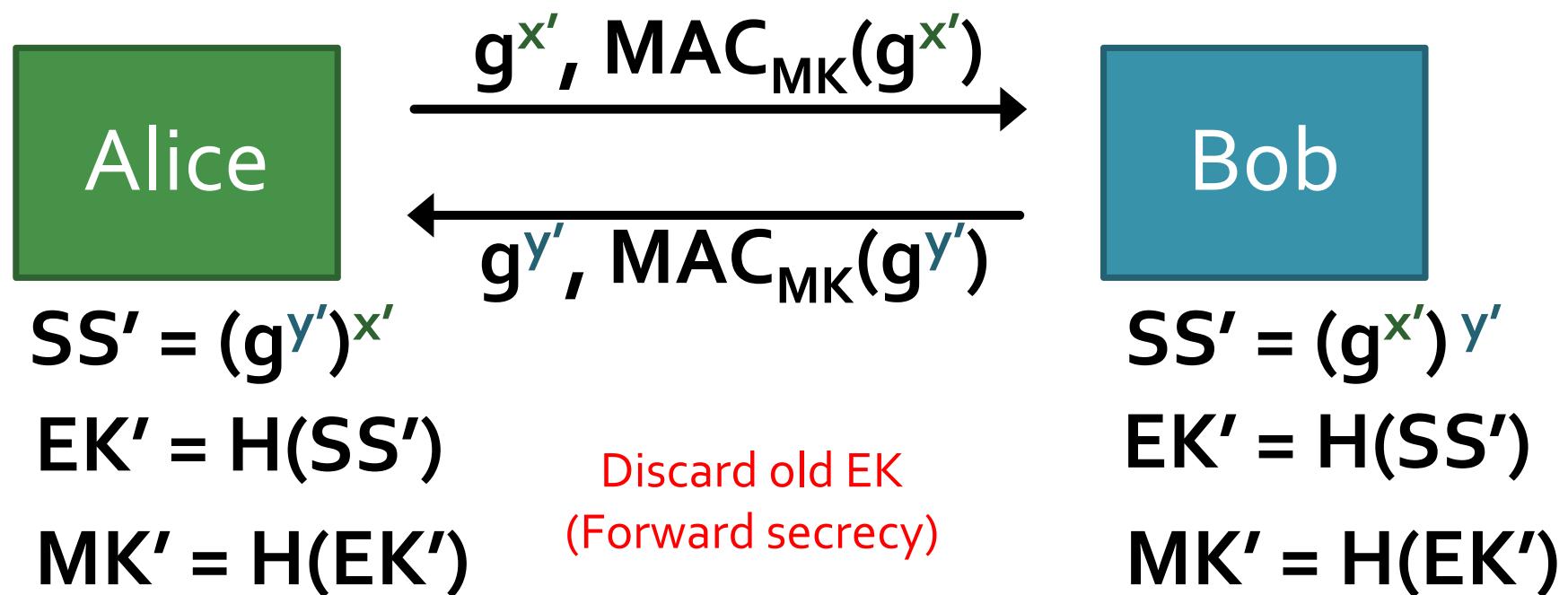
$SS = (g^y)^x$
 $EK = H(SS)$
 $MK = H(EK)$

SS: Shared Secret
EK: Encryption Key
MK: MAC Key

$SS = (g^x)^y$
 $EK = H(SS)$
 $MK = H(EK)$

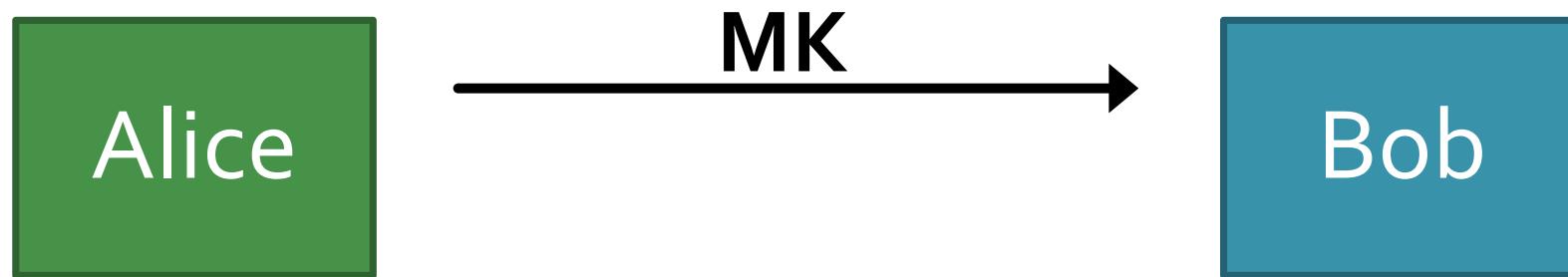
Off-the-Record (OTR) Messaging

3. Re-key often with new secrets, x' and y' , using Diffie-Hellman



Off-the-Record (OTR) Messaging

4. Stop using old MK...publish it!



$$SS' = (g^{y'})^{x'}$$

$$EK' = H(SS')$$

$$MK' = H(EK')$$

~~$$MK = H(EK)$$~~

“Deniability”

$$SS' = (g^{x'})^{y'}$$

$$EK' = H(SS')$$

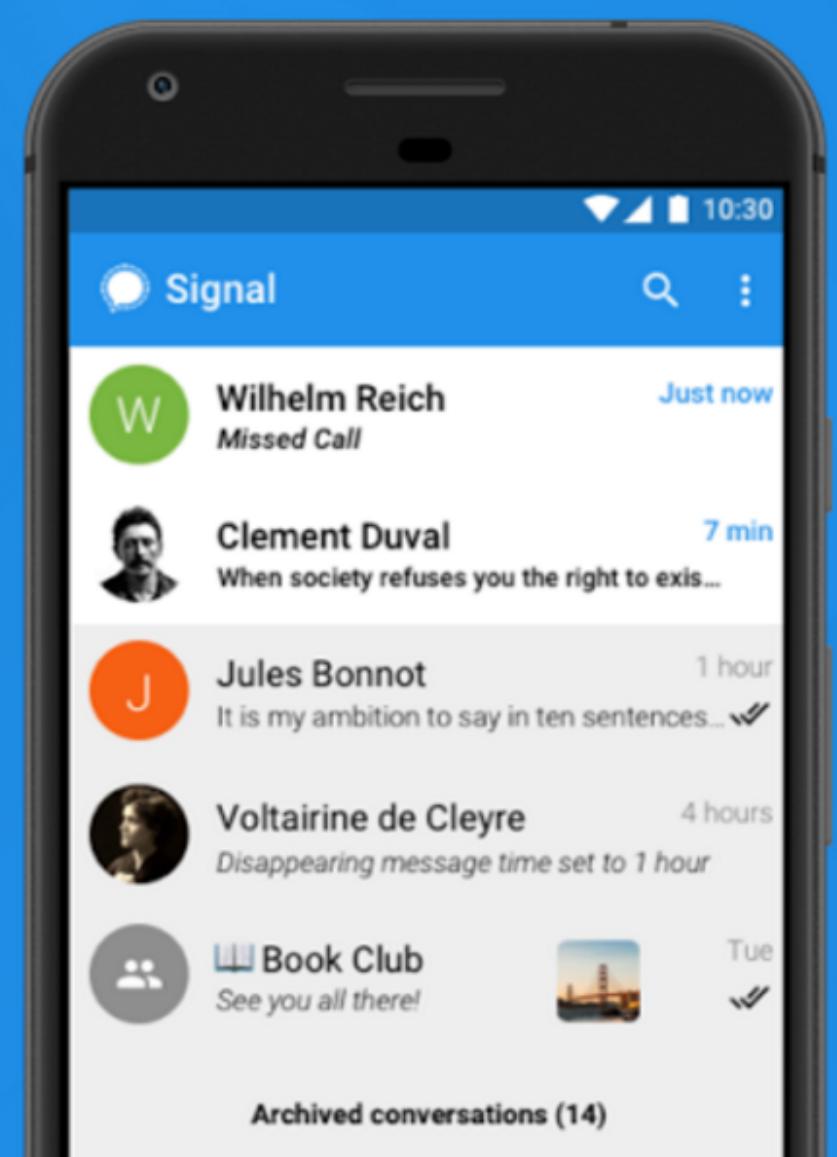
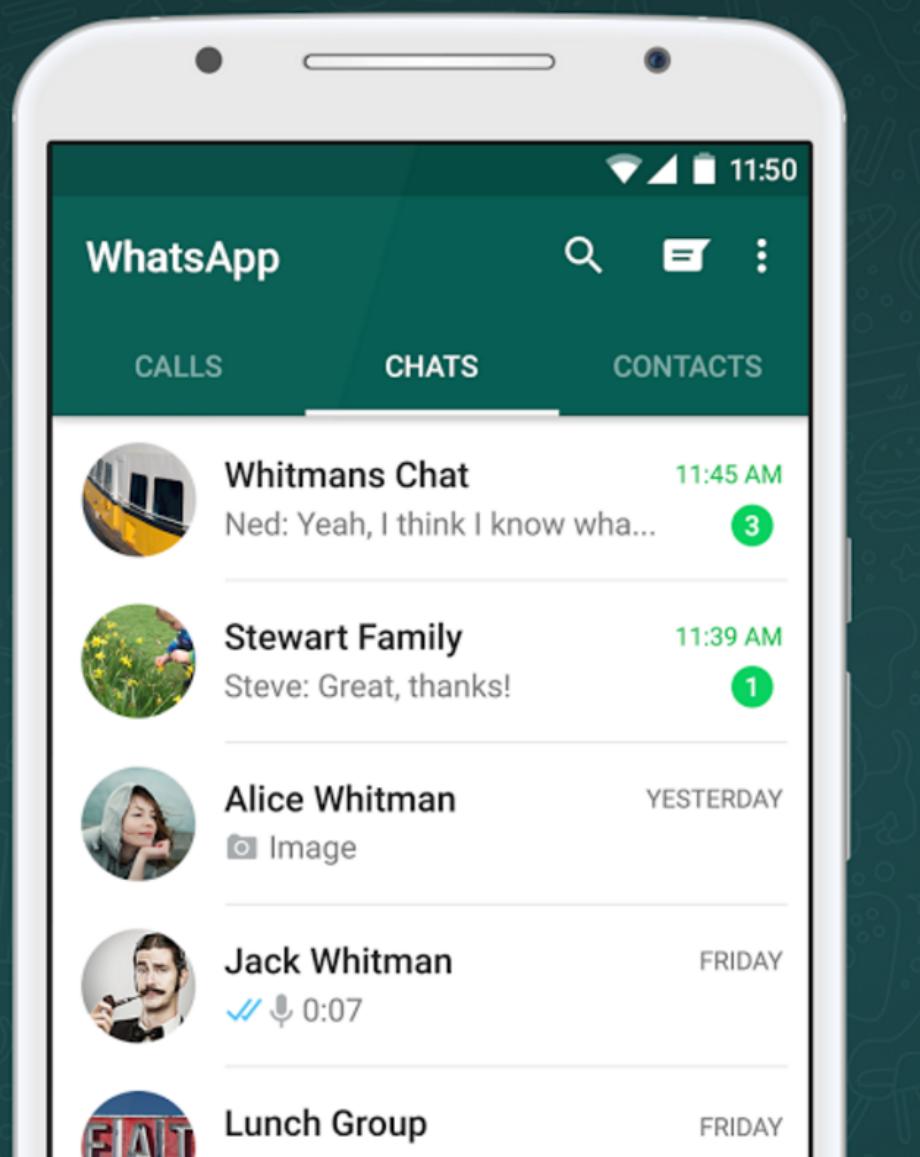
$$MK' = H(EK')$$

~~$$MK = H(EK)$$~~

Off-the-Record Messaging (OTR)

- This is suited to interactive communication (i.e. chat), not so much for email
 - We use long-term keys only to authenticate the DH protocol messages
 - The session key will be short-lived and **must be securely erased**...chat is good for this since we typically know when a chat session ends
- Recall: you must validate the counterparty's initial key fingerprint
- OTR provides:
 - message confidentiality
 - authentication
 - perfect forward secrecy
 - deniability

OTR's Descendants



Anonymous Networking

- Anonymity: Concealing your identity
- In the context of the Internet, we may want anonymous communications
 - **Communications where the identity of the source and/or destination are concealed**
- Not to be confused with confidentiality
 - Confidentiality is about contents, anonymity is about identities

Anonymous Networking

- Internet anonymity is *hard**
 - Difficult if not impossible to achieve on your own
 - Right there in every packet is the source and destination IP address...and your ISP knows who you are
- * But it's easy for "bad guys".
- "State of the art" technique:
 - Ask/Force someone else to send it for you
- A more devious approach (from the "bad guys"):
 - Steal, or hack, other machines, and then use them to create a chain of compromised machines

Anonymity for browsing?

You

Server

Naive approach VPNs



Proxies

- Proxy: Intermediary that relays our traffic
- Needs trusted 3rd party (e.g. hidemyass.com)
 - You set up an encrypted VPN to their site
 - All of your traffic goes through them
- Why easy for bad guys?
Compromised machines as proxies.

VPNs

So who do you trust?



HMA! Blog - News, updates, and all things privacy related.

Lulzsec fiasco

Posted on September 23, 2011

We have received concerns by users that our VPN service was utilized by a member or members of the hacktivist group 'lulzsec'. Lulzsec have been ALLEGEDLY been responsible for a number of high profile cases such as:

- The hacking of the Sony Playstation network which compromised the names, passwords, e-mail addresses, home addresses and dates of birth of thousands of people.
- The DDOS attack which knocked the British governments SOCA (Serious Organised Crime Agency) and other government websites offline.
- The release of various sensitive and confidential information from companies such as AT&T, Viacom, Disney, EMI, NBC Universal, and AOL.
- Gaining access to NATO servers and releasing documents regarding the communication and information services (CIS) in Kosovo.
- The defacement of British newspaper websites The Sun & The Times.
- The hacking of 77 law enforcement sheriff websites.

It first came to our attention when leaked IRC chat logs were [released](#), in these logs participants discussed about various VPN services they use, and it became apparent that some members were using our service. No action was taken, after all there was no evidence to suggest wrongdoing and nothing to identify which accounts with us they were using. At a later date it came as no surprise to have received a court order asking for information relating to an account associated with some or all of the above cases. As stated in our terms of service and privacy policy our service is not to be used for illegal activity, and as a legitimate company we will cooperate with law enforcement if we receive a court order (equivalent of a subpoena in the US).

VPNs

The screenshot shows a portion of the Hide My Ass! website. At the top, there's a navigation bar with links for Home, Privacy, and Privacy Policy. Below the navigation is a logo featuring a cartoon character wearing a hat and holding a shield, with the text "HIDE MY ASS!" underneath. A yellow horizontal bar contains the text "HEXA Blog - News, opinion, and all things privacy related". On the left, there's a sidebar with a list of blog posts. The main content area contains a large block of text in a bold, black, sans-serif font, enclosed in a white box with a thin black border. The text reads:

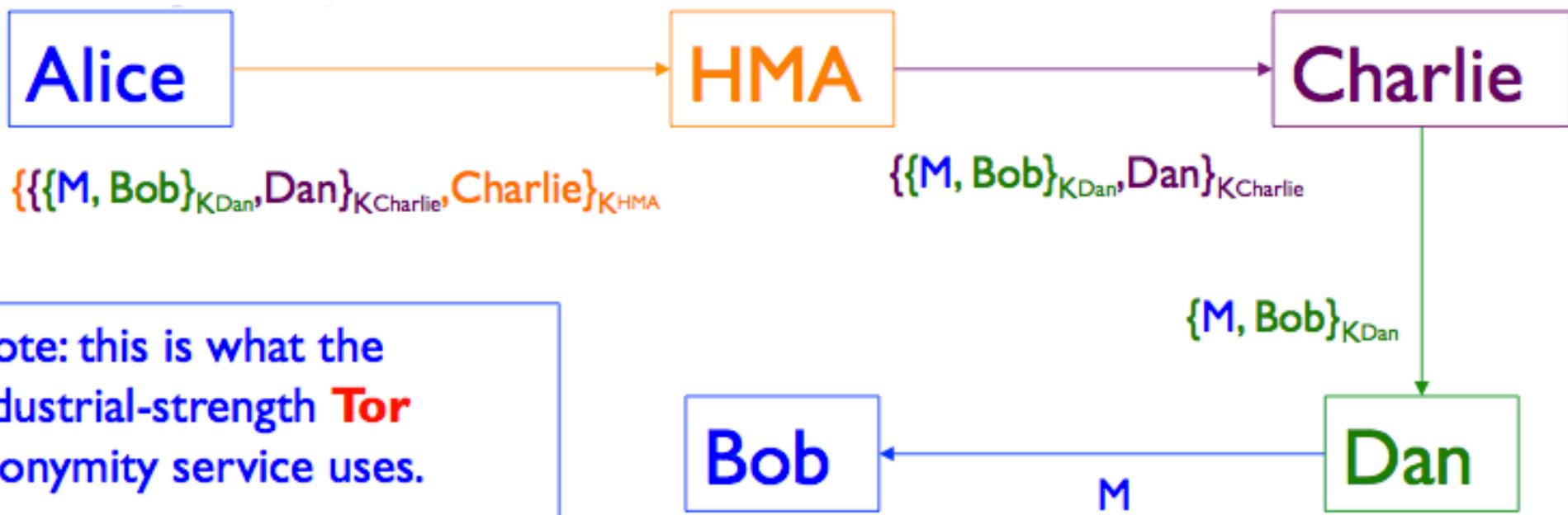
“...received a **court order** asking for information relating to an account associated with some or all of the above cases. As stated in our terms of service and **privacy policy** our service is not to be used for illegal activity, and as a legitimate company ***we will cooperate with law enforcement if we receive a court order***”

Better Approach: Tor

- Works at the transport layer
- Allows you to make TCP connections without revealing your IP address
- Popular for web connections
- Tor network made up of volunteer-run **nodes**, or **onion routers**, located all over the world
 - It's a *distributed anonymity service*

Basic idea: Alice wants to connect to a web server without revealing her IP address

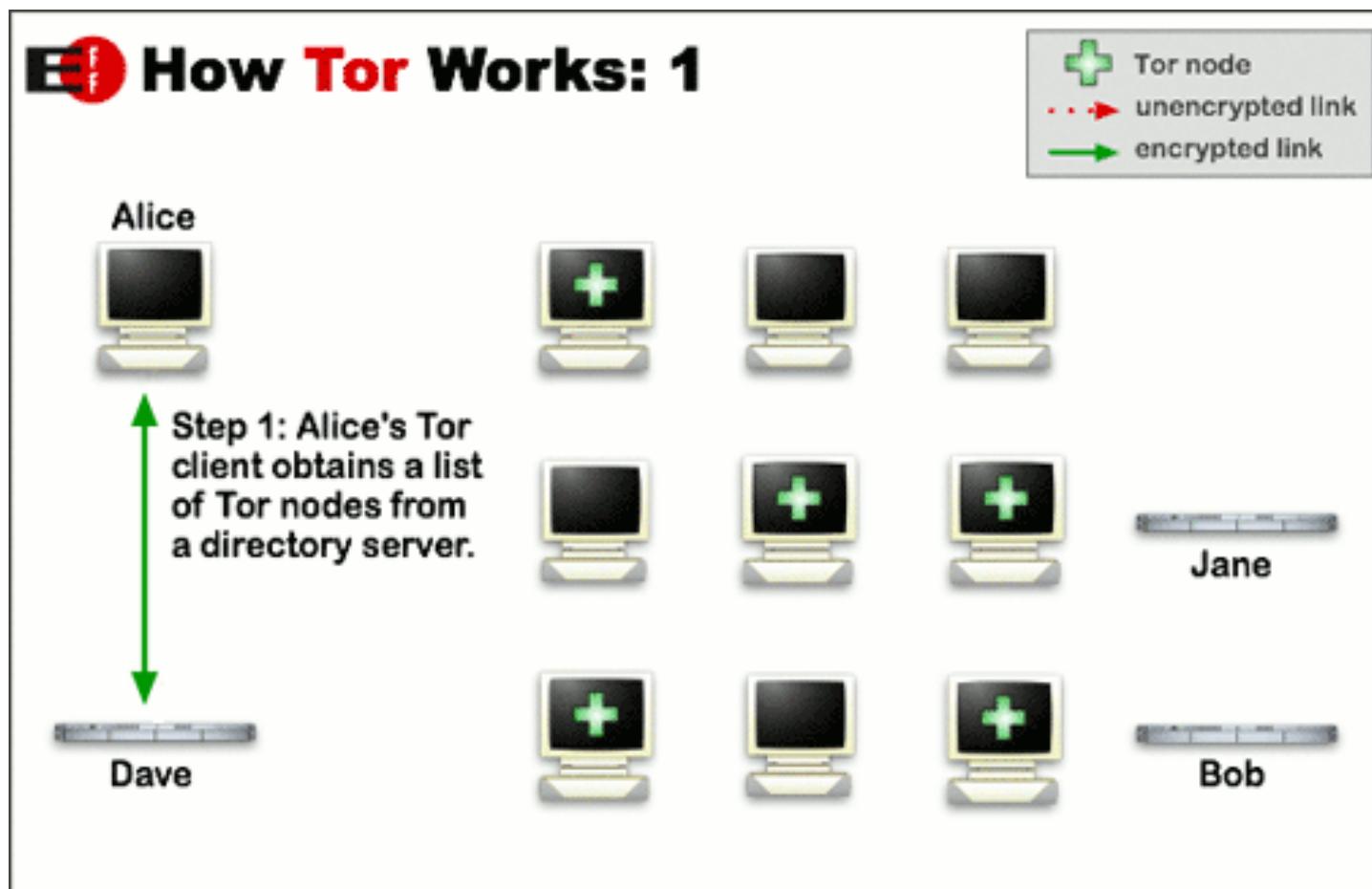
Onion Routing



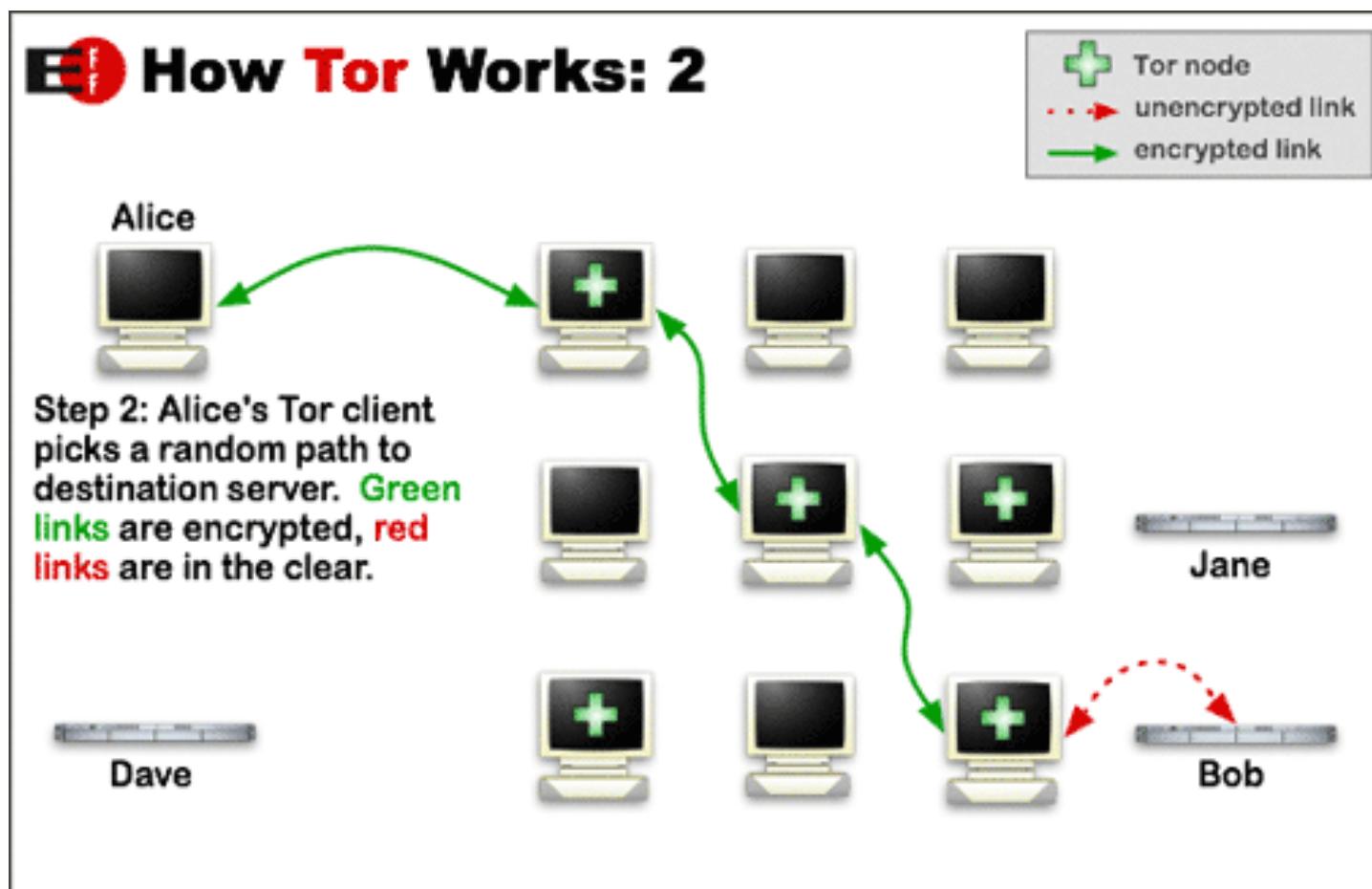
Note: this is what the industrial-strength **Tor** anonymity service uses.
(It also provides bidirectional communication)

Key concept: No one relay knows both you and the destination!

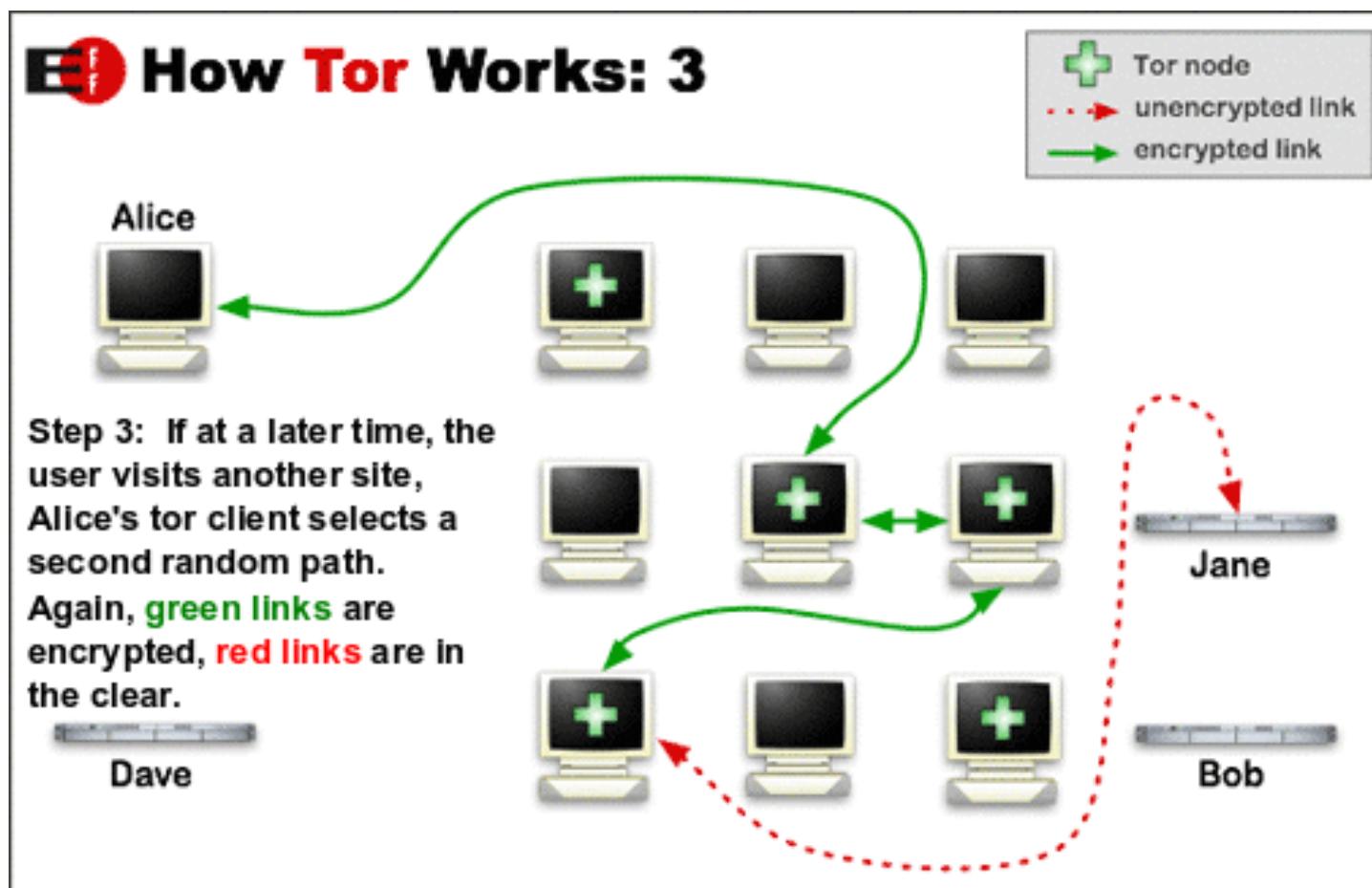
Tor



Tor



Tor



Trust in Tor

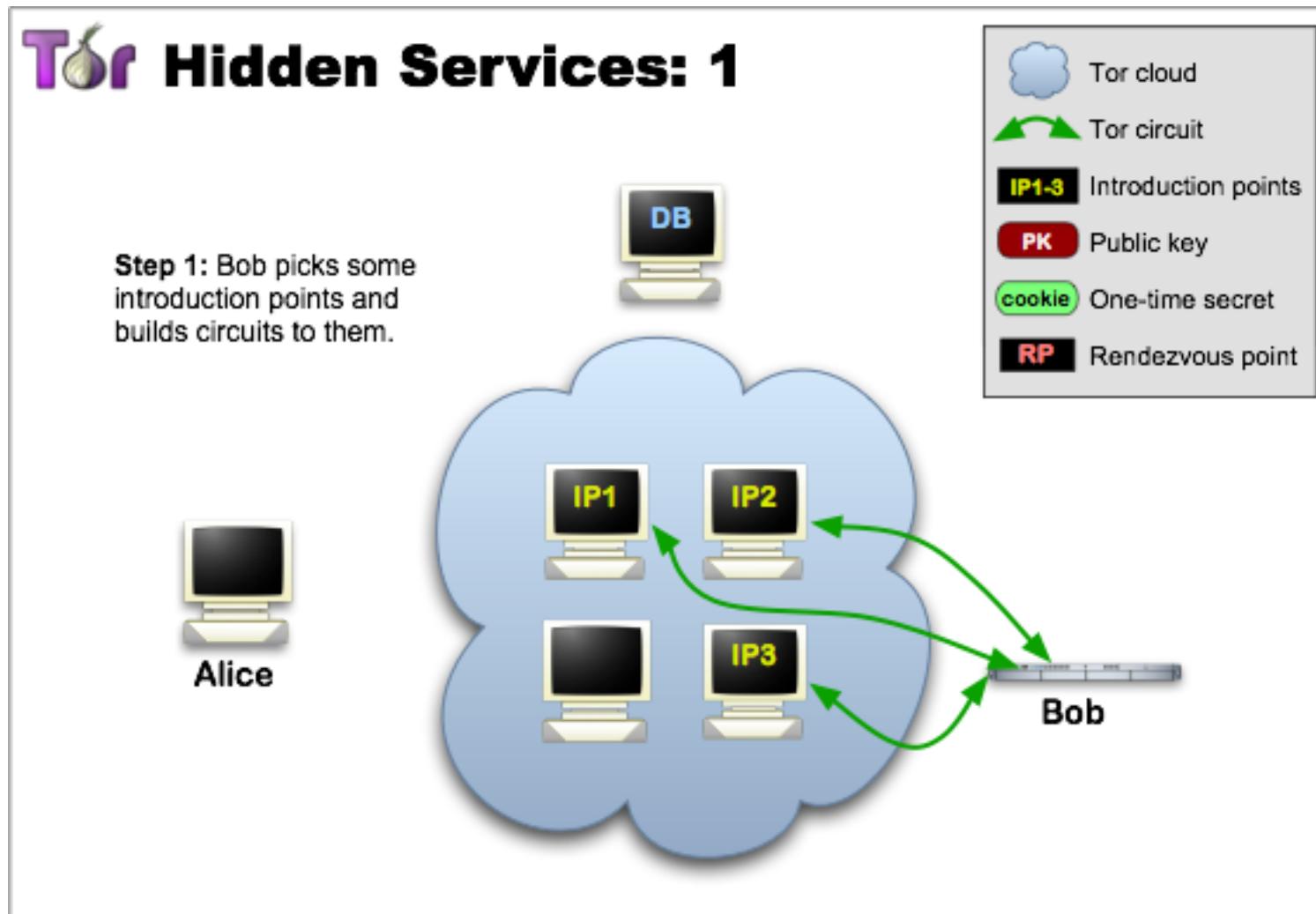
- **Entry node:** knows Alice is using Tor, and identity of middle node, but not destination
- **Exit node:** knows some Tor user is connecting to destination, but not which user
- **Destination:** knows a Tor user is connecting to it via the exit node

Tor does not provide encryption between exit and destination (that's what HTTPS is for!)

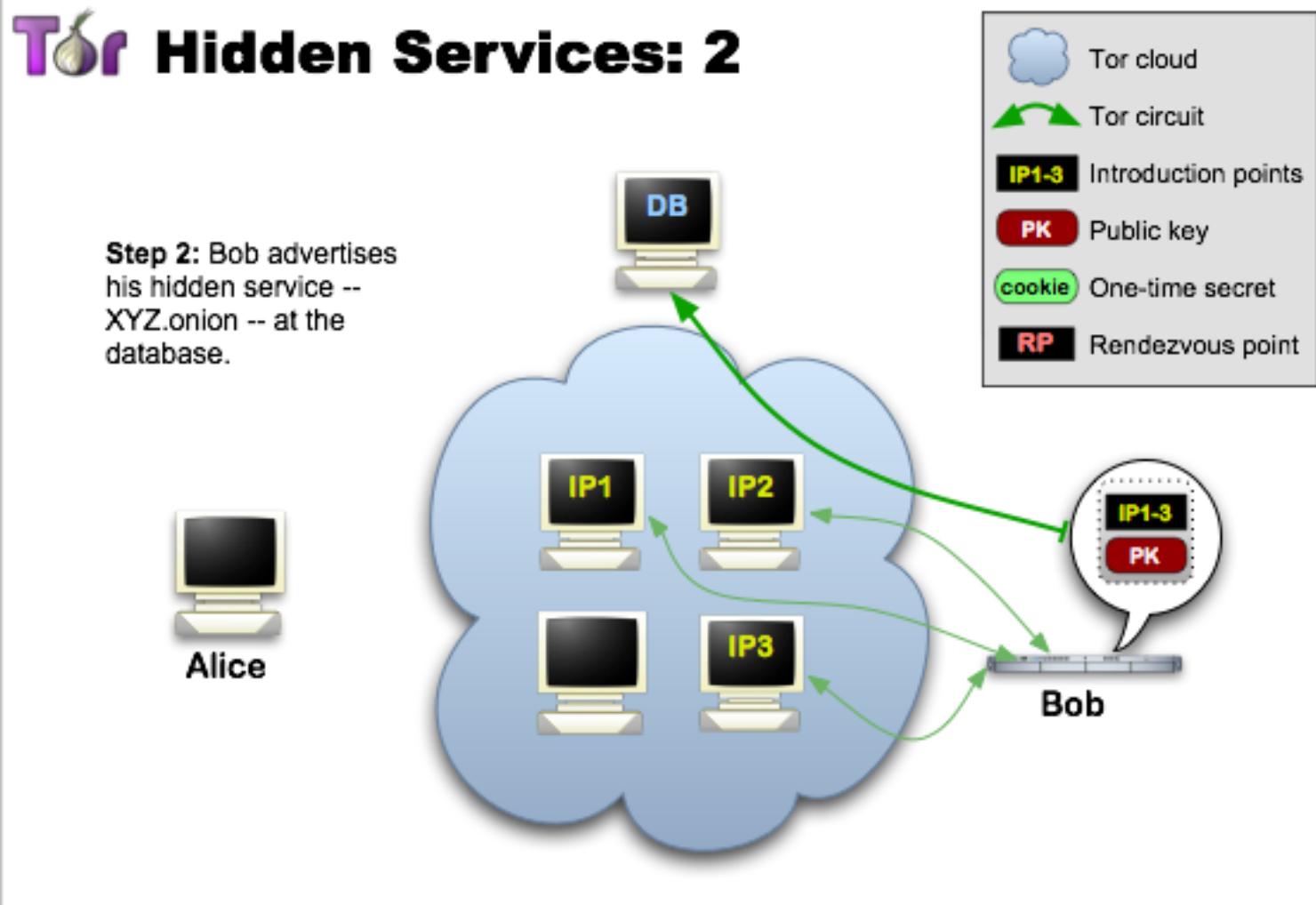
Onion Routing Issues/Attacks?

- Performance: message bounces around a lot
- Attack: rubber-hose cryptanalysis of certain nodes
 - Defense: use nodes in different countries
- Attack: adversary operates many/all of the nodes
 - Defense: have lots of nodes (Tor today: ~2,000)
- Attack: adversary exploits timing information (side channel attack) and observes when Alice sends and Bob receives (and links the two together)
 - Defenses: pad messages, introduce significant delays
 - Tor does the former, but notes that it's not enough for defense

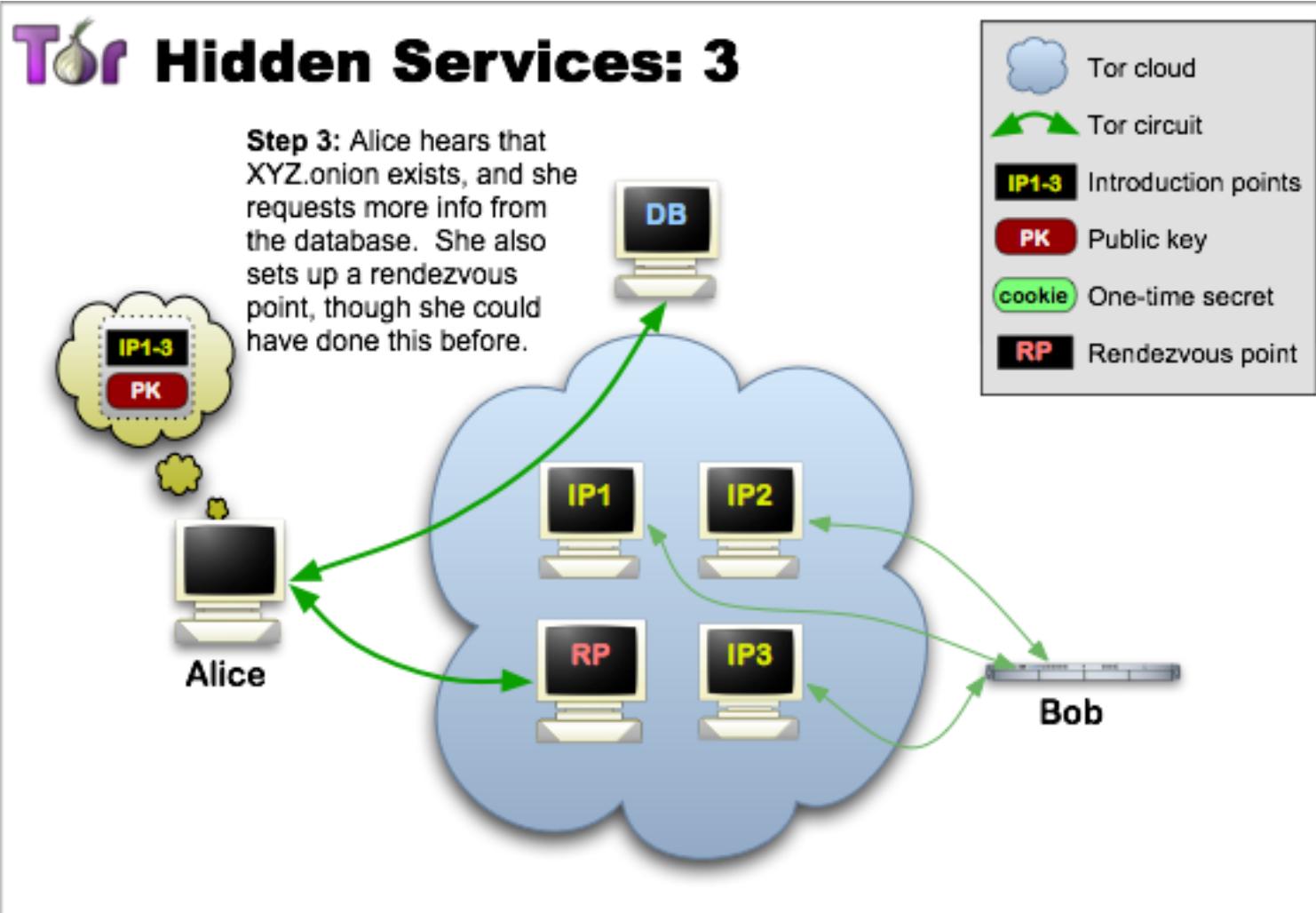
Tor Hidden Services: Overview



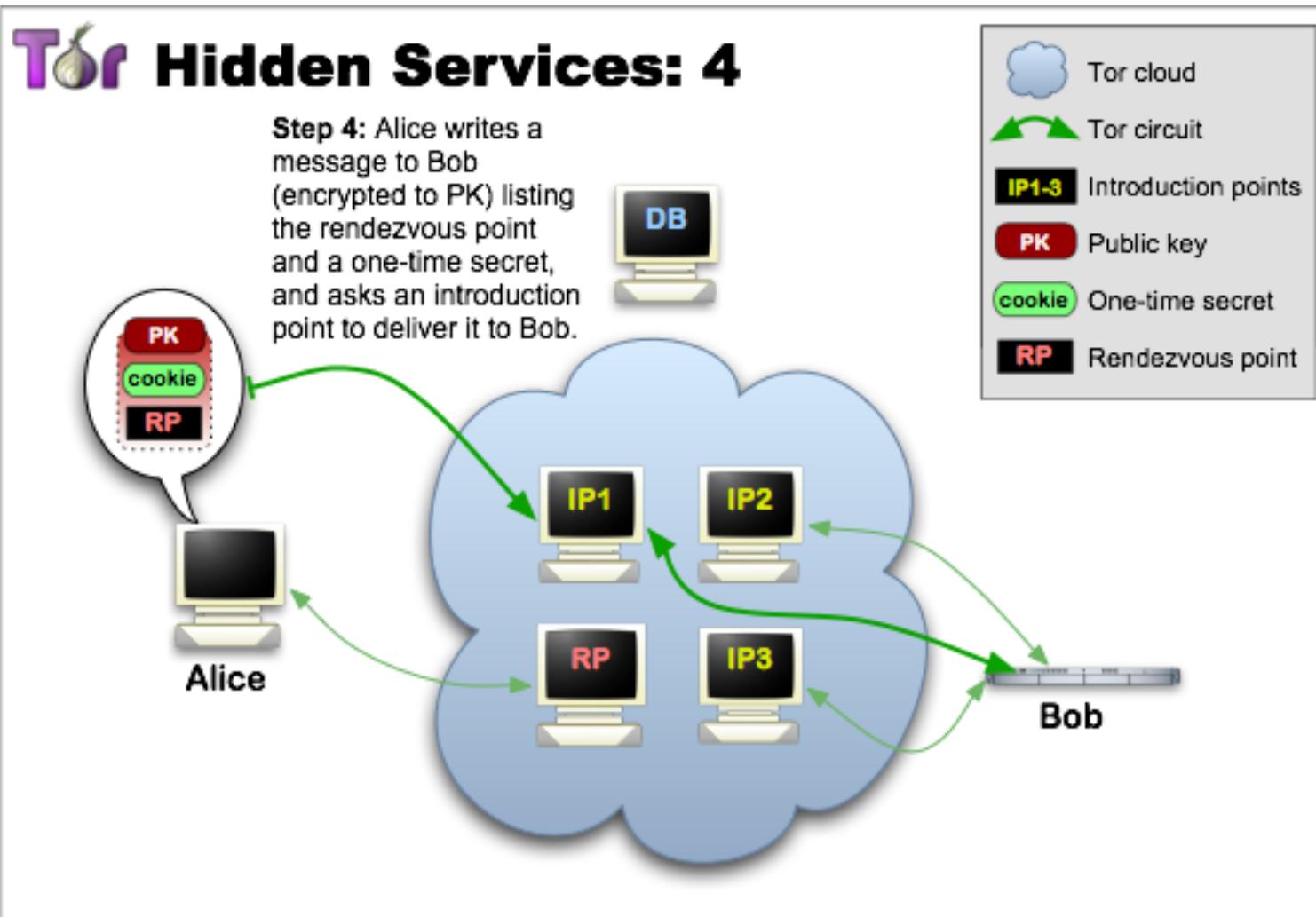
Tor Hidden Services



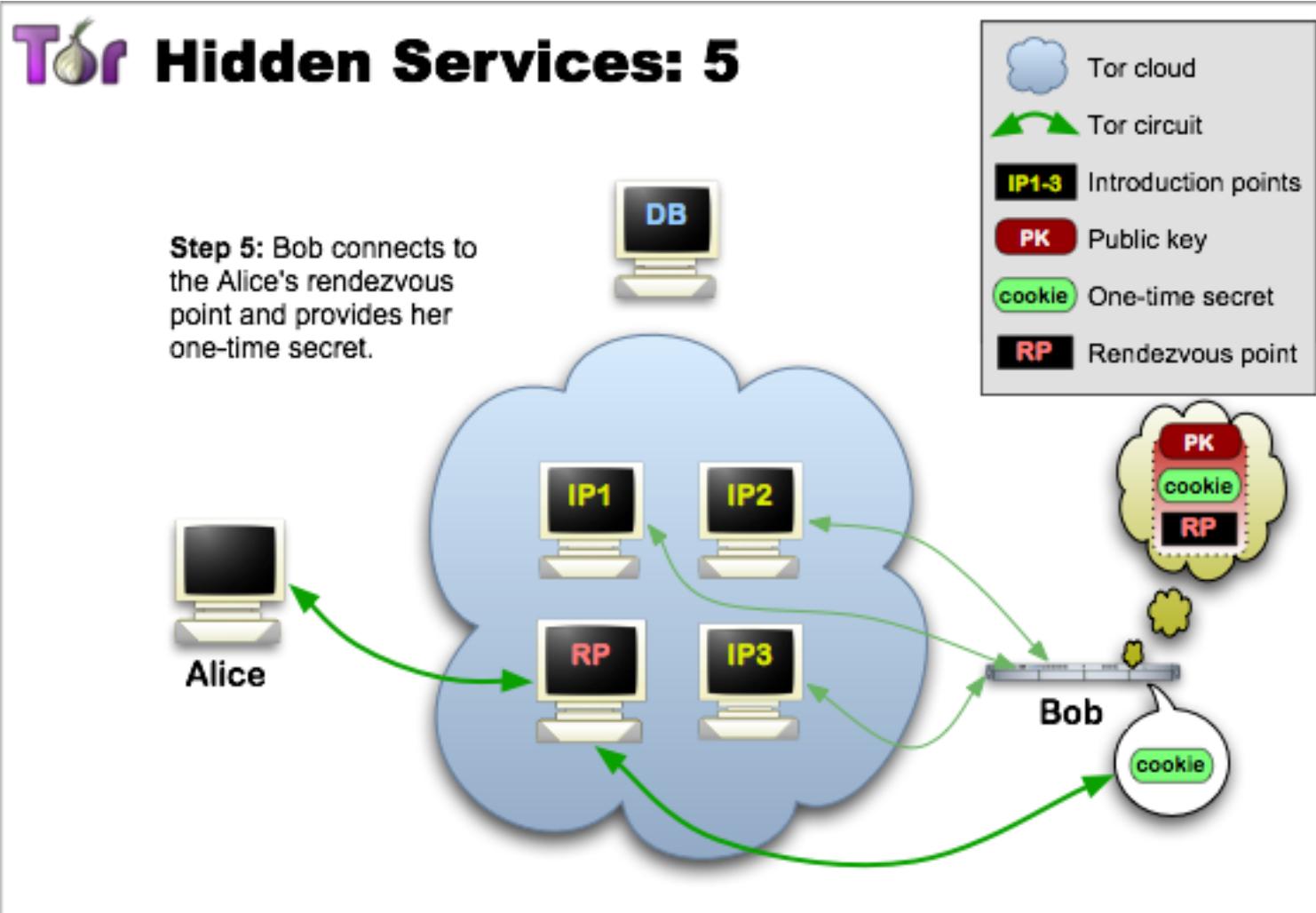
Tor Hidden Services



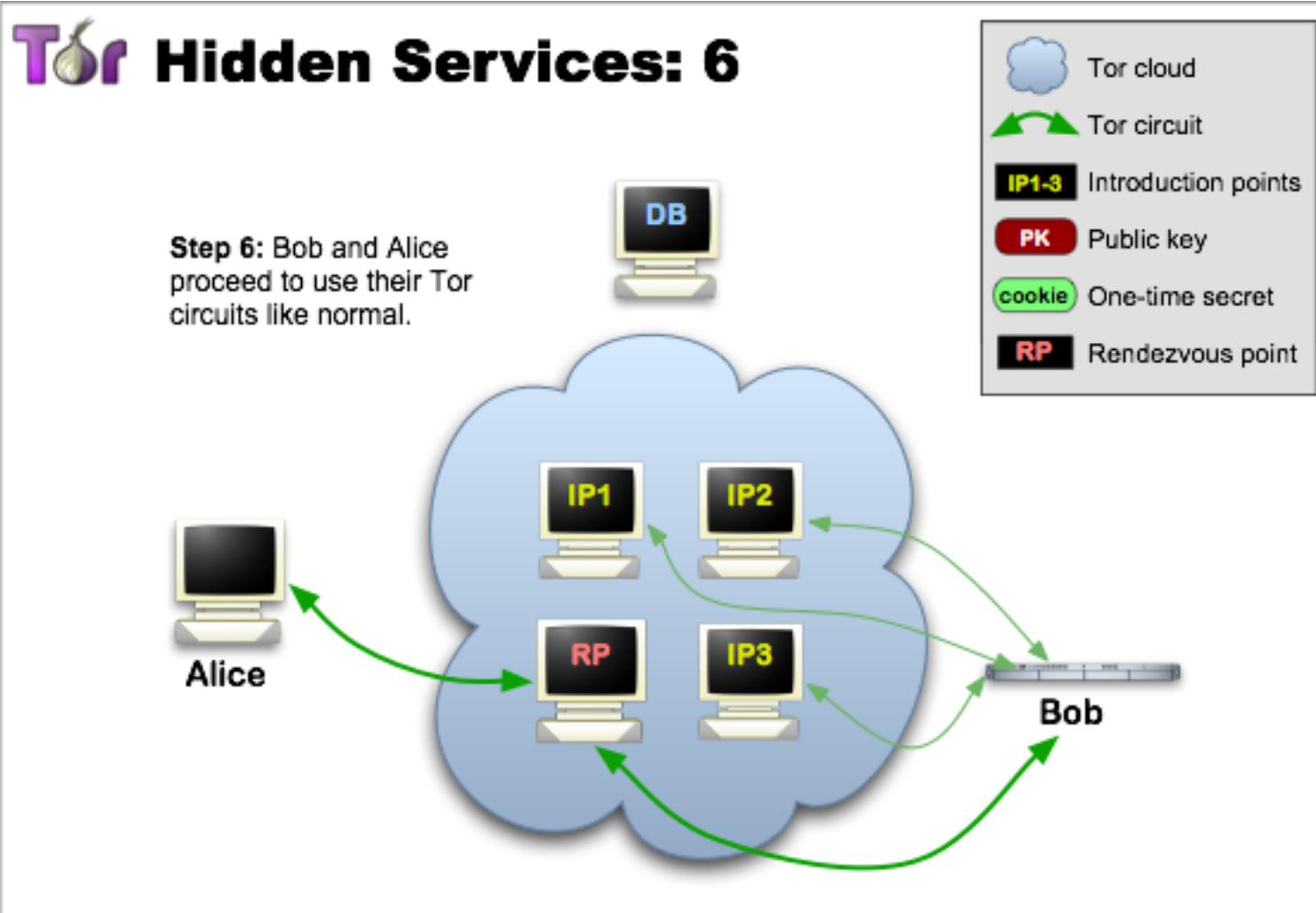
Tor Hidden Services



Tor Hidden Services



Tor Hidden Services



SilkRoad Marketplace



Welcome nowOpen!

[messages\(0\)](#) | [orders\(0\)](#) | [account\(\\$0\)](#) | [settings](#) | [log out](#)

 search |

Shop by category:

Drugs(752)
Cannabis(280)
Ecstasy(35)
Dissociatives(11)
Psychedelics(84)
Opioids(62)
Stimulants(53)
Other(107)
Benzos(70)

Lab Supplies(6)
Digital goods(98)
Services(48)
Money(55)
Weaponry(15)
Home & Garden(14)

Food(4)
Electronics(5)

Books(49)
Drug paraphernalia(28)
XXX(30)

Medical(3)
Computer equipment(4)
Apparel(4)

Musical instruments(2)
Tickets(1)
Forgeries(13)



5 Marijuana Butter Chocolate Chip...
\$8.53



4mg. TIZANIDINE (zanaflex) x25
\$2.09



US customers only Express...
\$2.79



4 x 20MG Original Lily Cialis
\$7.85



(1g) High-grade Crystal Meth
\$11.95



MindFood - Protect your brain!...
\$3.69



to US 1/4 lb (qp) BC Master Kush...
\$121.37



How to Grow Mushrooms
\$0.14



Mushroom Indoor Growing - Easy...
\$0.29

News:

- Escrow hedging update
- New feature to help protect sellers
- We are hiring! Get paid for a referral, too...
- Reclaim lost coins from [MyBitcoin.com](#)
- Seller ranking and feedback overhaul
- Change your Mt. Gox password

[recent feedback](#):

SilkRoad Marketplace



THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney's Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York



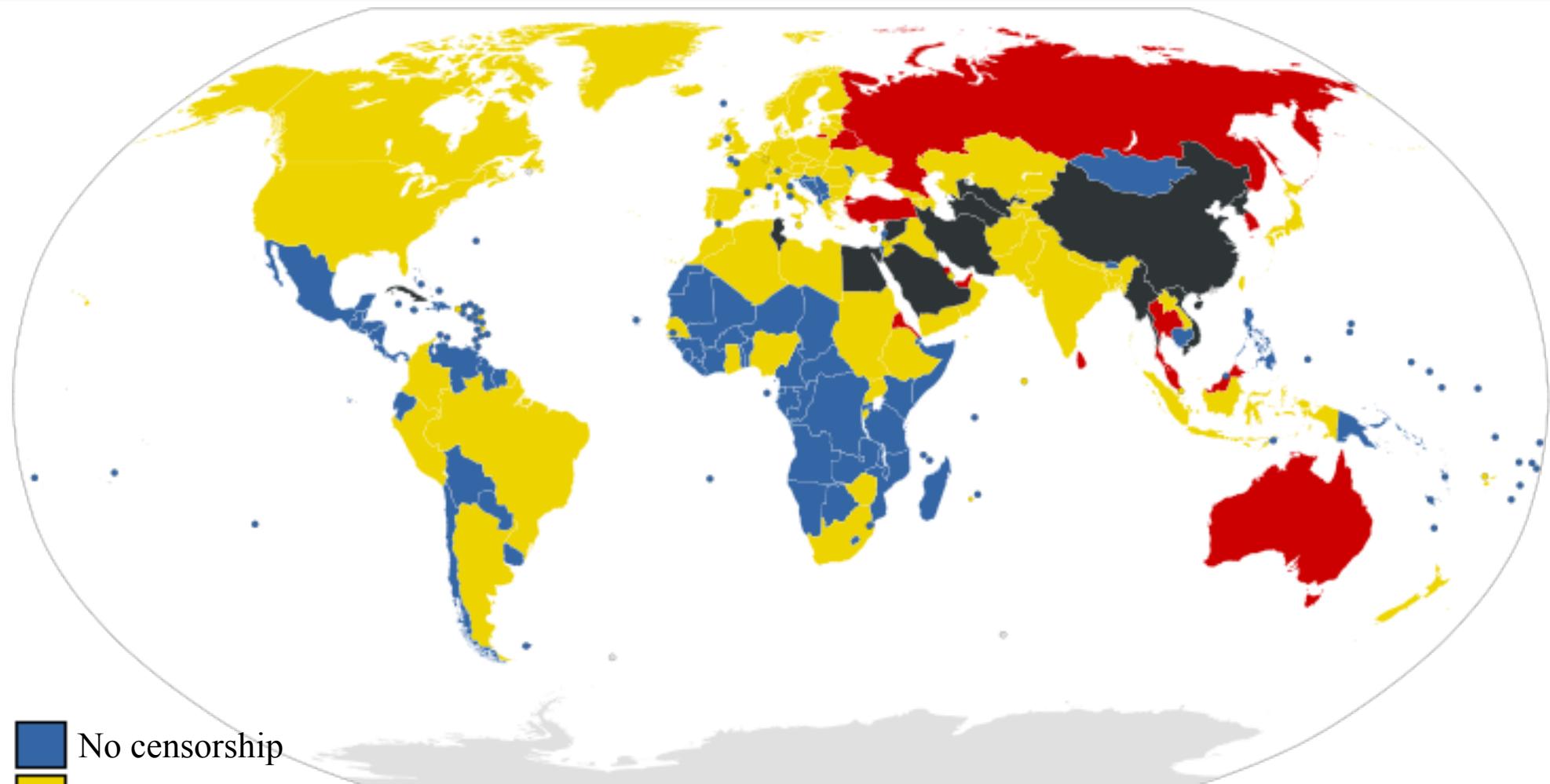
How to get Tor

- Tor Browser bundle (built on top of Firefox)
- ☺ optional exercise: download and use it!

<https://www.torproject.org/>

..or volunteer to be a part of the Tor network.

Internet Censorship



No censorship

Some censorship

Country under surveillance from Reporters Without Borders

Most heavily censored nations

Internet Censorship

Government censors

Block websites containing “offensive” content
Commonly employ blacklist approach

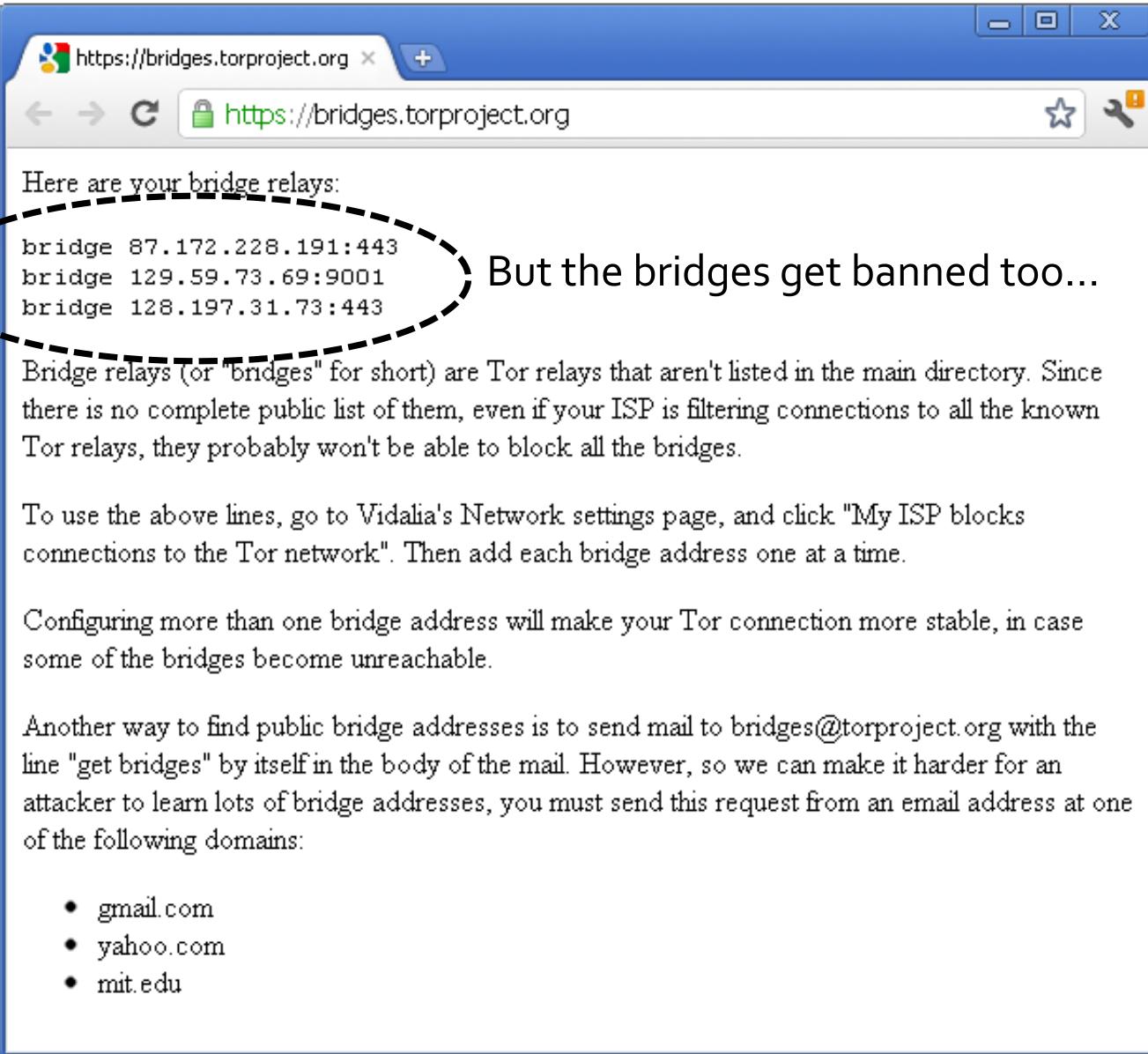
Observed techniques

IP blocking, DNS blackholes, forged RST packets

Popular countermeasures

Mostly proxy based — Tor, Freenet, Ultrasurf, ...
Problem: Cat-and-mouse game

Censorship Resistance: Tor Bridges



A screenshot of a web browser window titled "https://bridges.torproject.org". The address bar shows the same URL. The page content displays three bridge relay addresses:

```
bridge 87.172.228.191:443  
bridge 129.59.73.69:9001  
bridge 128.197.31.73:443
```

A dashed oval highlights the first three lines of text. To the right of the oval, the text "But the bridges get banned too..." is displayed.

Bridge relays (or "bridges" for short) are Tor relays that aren't listed in the main directory. Since there is no complete public list of them, even if your ISP is filtering connections to all the known Tor relays, they probably won't be able to block all the bridges.

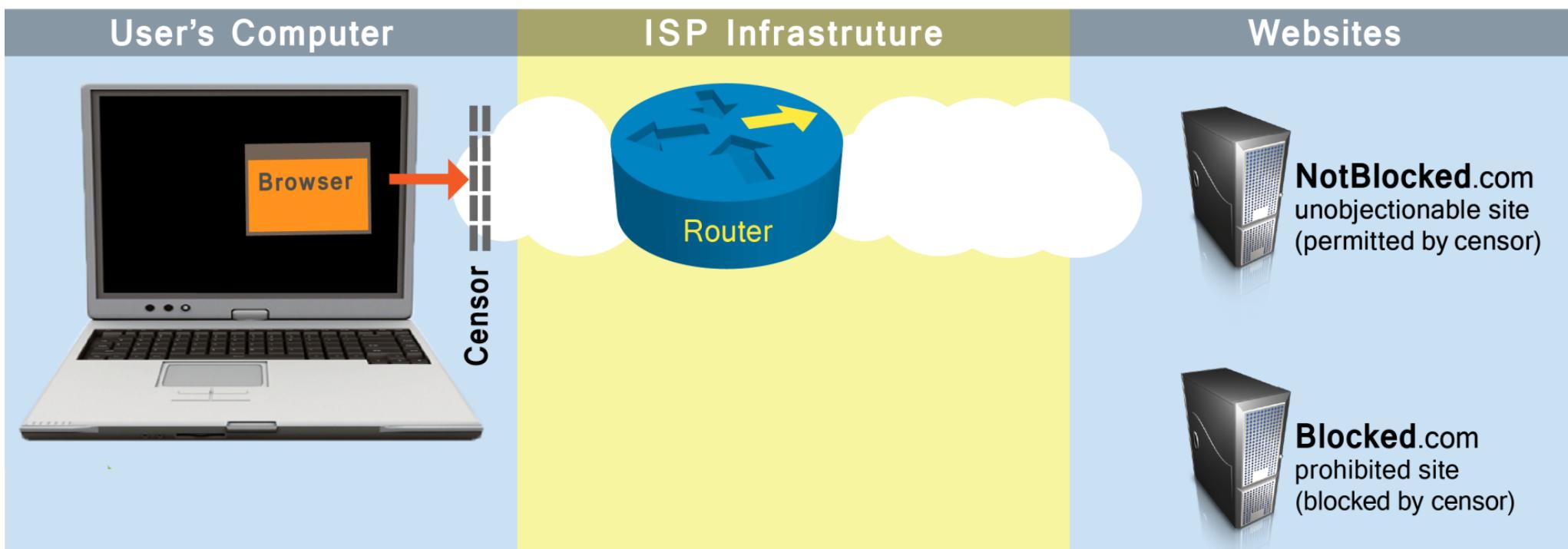
To use the above lines, go to Vidalia's Network settings page, and click "My ISP blocks connections to the Tor network". Then add each bridge address one at a time.

Configuring more than one bridge address will make your Tor connection more stable, in case some of the bridges become unreachable.

Another way to find public bridge addresses is to send mail to bridges@torproject.org with the line "get bridges" by itself in the body of the mail. However, so we can make it harder for an attacker to learn lots of bridge addresses, you must send this request from an email address at one of the following domains:

- gmail.com
- yahoo.com
- mit.edu

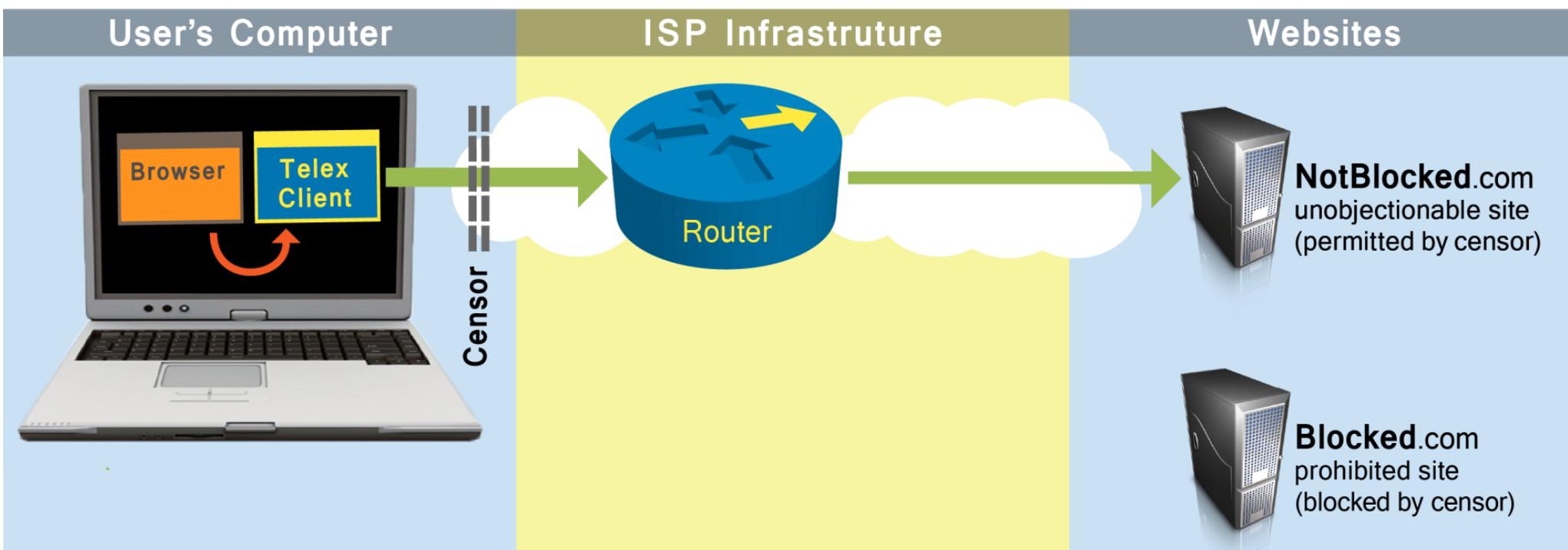
New Approach: Telex



→ Request for **permitted** site

→ Request for **prohibited** site

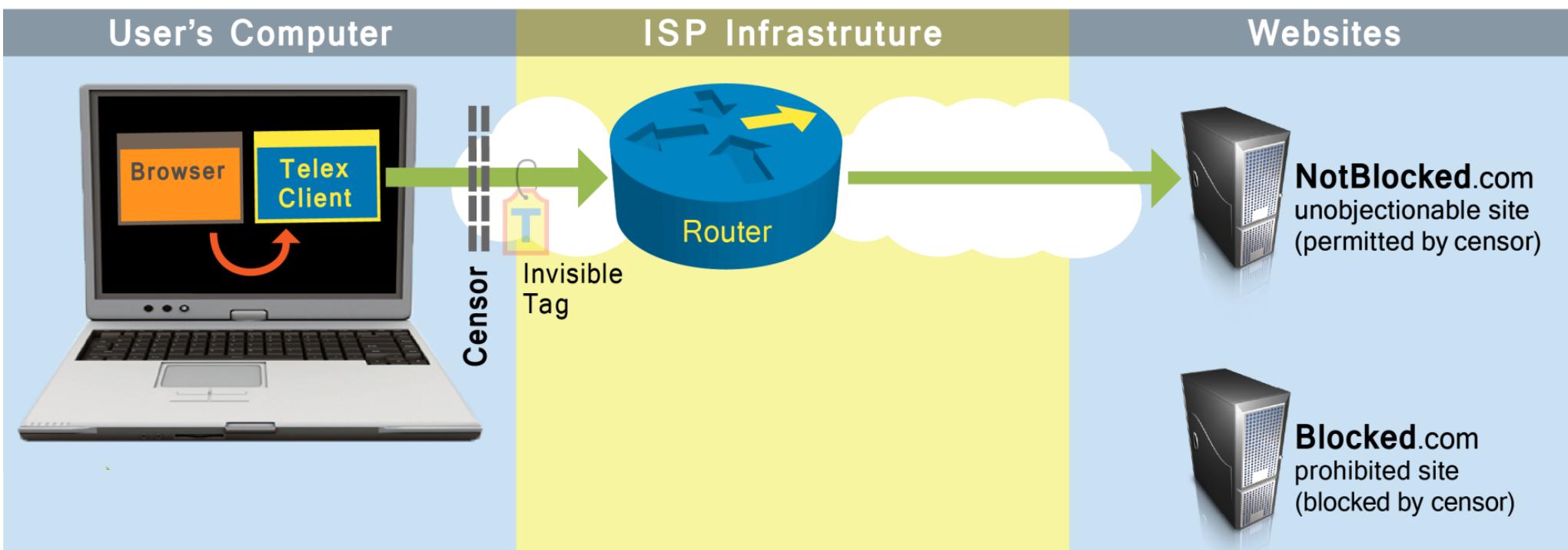
New Approach: Telex



→ Request for **permitted** site

→ Request for **prohibited** site

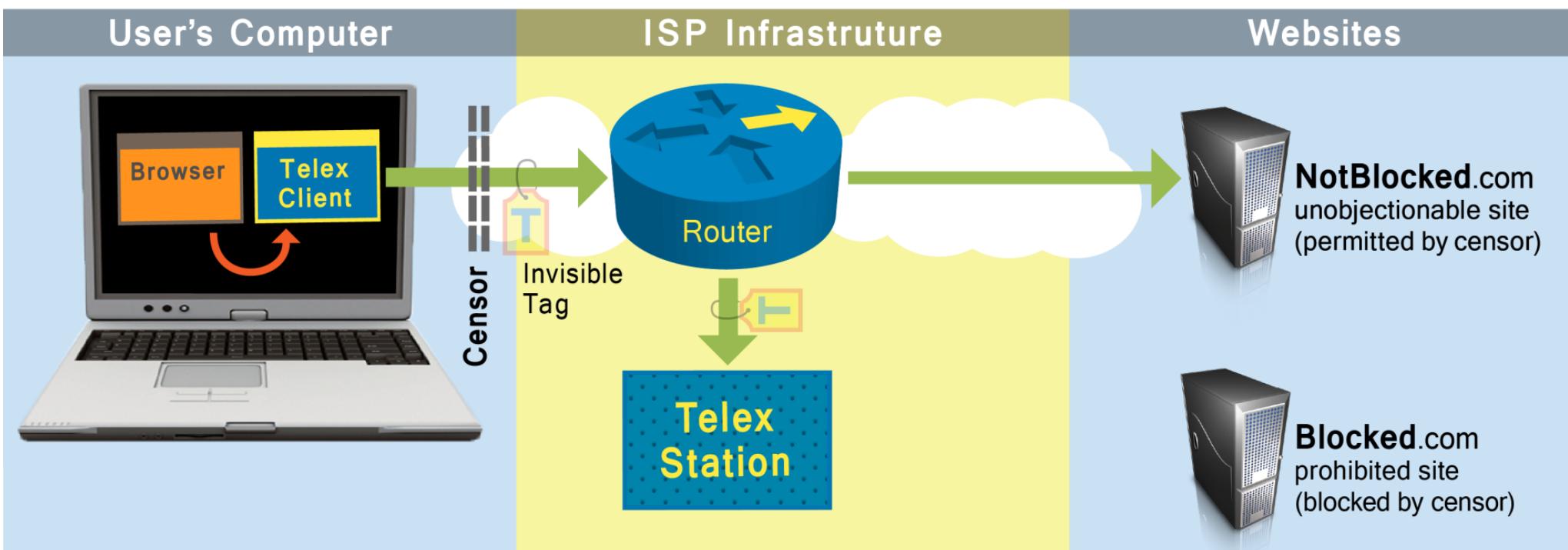
New Approach: Telex



→ Request for **permitted** site

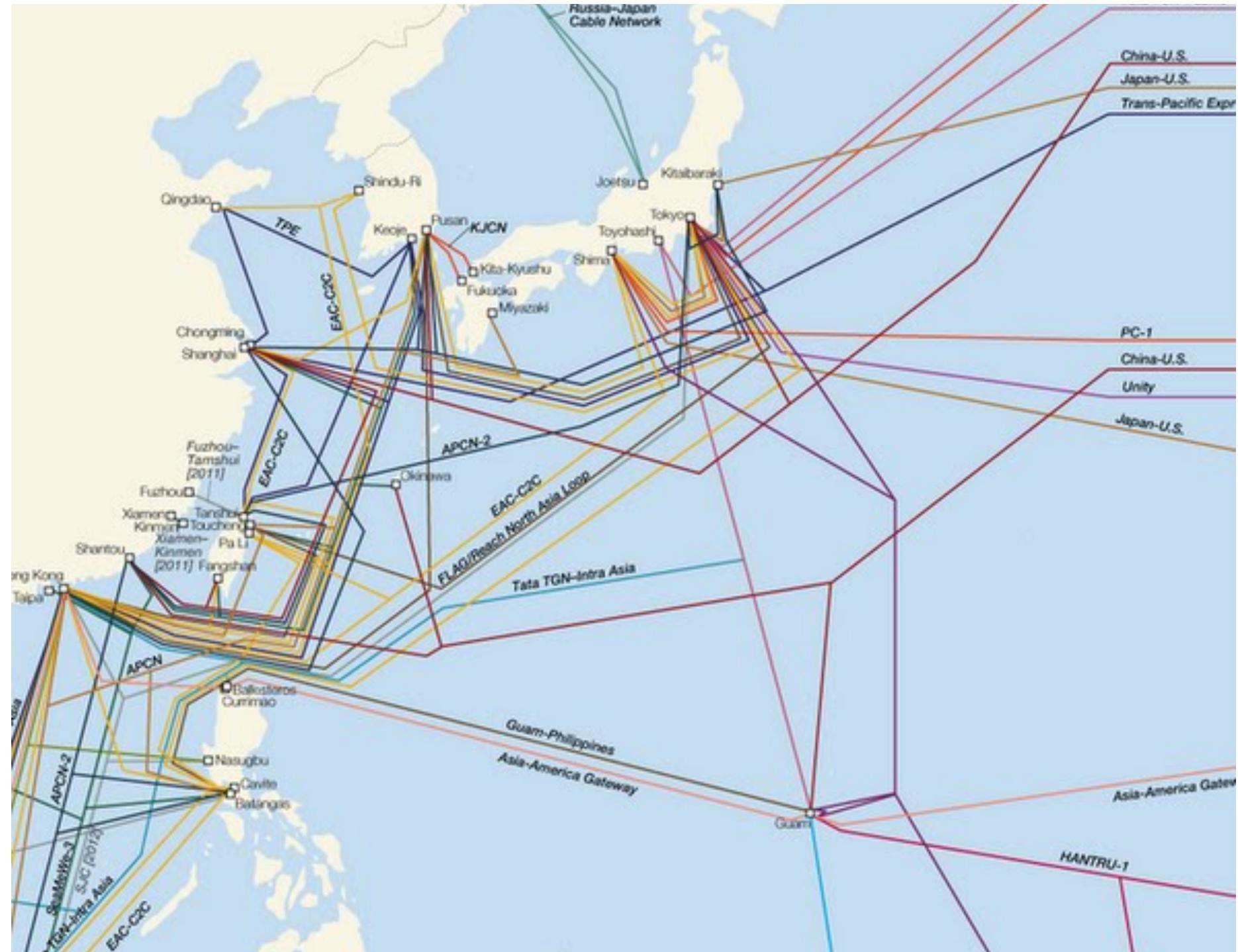
→ Request for **prohibited** site

New Approach: Telex

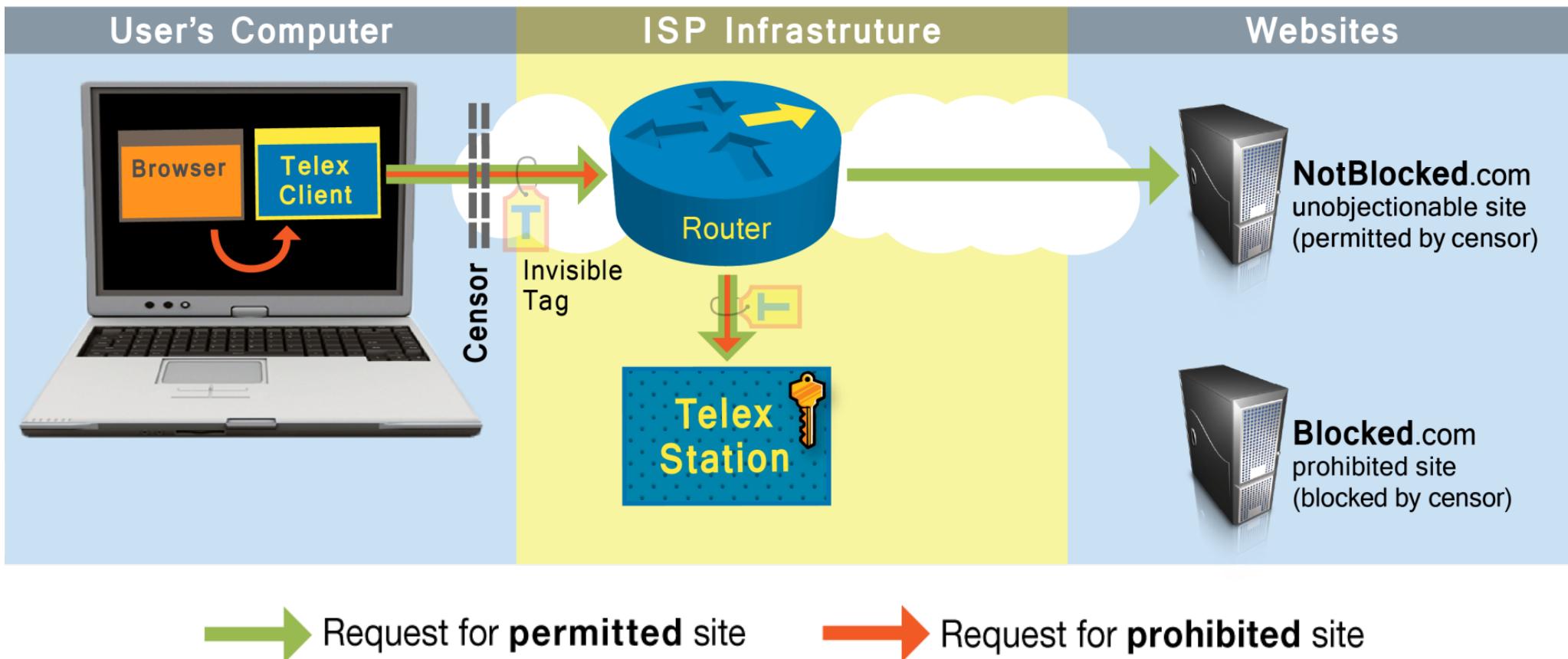


→ Request for **permitted** site

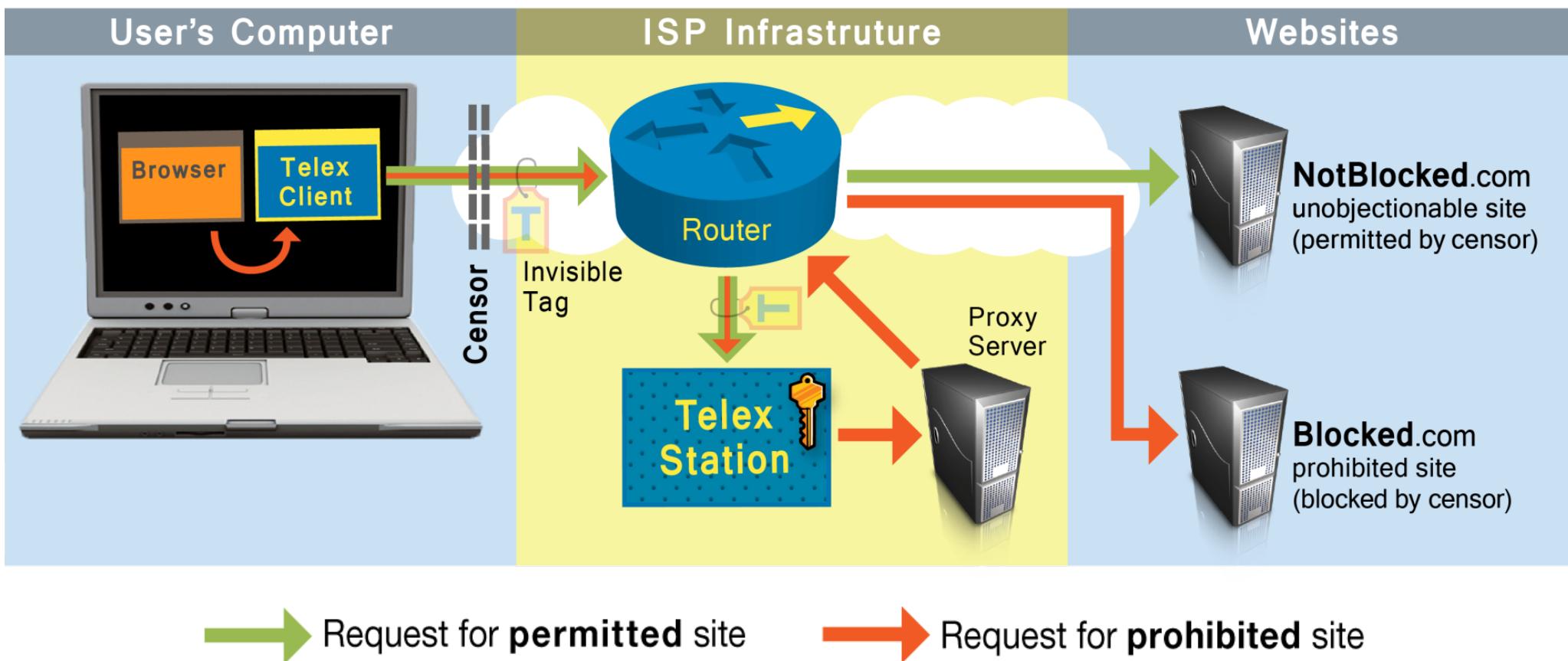
→ Request for **prohibited** site



New Approach: Telex



New Approach: Telex



Metadata

- If you talk to someone
- When you talk to someone
- How much you talk
- Who's talking
- What's being said

Metadata

- If you talk to someone
- When you talk to someone
- How much you talk
- Who's talking ← 
- What's being said ← PGP

Metadata Matters

- They know you rang a phone sex service at 2:24 am and spoke for 18 minutes. But they don't know what you talked about.
- They know you called the suicide prevention hotline from the Golden Gate Bridge. But the topic of the call remains a secret.
- They know you spoke with an HIV testing service, then your doctor, then your health insurance company in the same hour. But they don't know what was discussed.
- They know you received a call from the local NRA office while it was having a campaign against gun legislation, and then called your senators and congressional representatives immediately after. But the content of those calls remains safe from government intrusion.
- They know you called a gynecologist, spoke for a half hour, and then called the local Planned Parenthood's number later that day. But nobody knows what you spoke about.

Optional Exercises

Experiment with the following tools and defenses:

- Encrypted storage (desktop and mobile)
- Tor (Tor Browser bundle)
- PGP (Keybase or GnuPG)
- OTR (or Signal)