Privacy, Anonymity, and Censorship Resistance

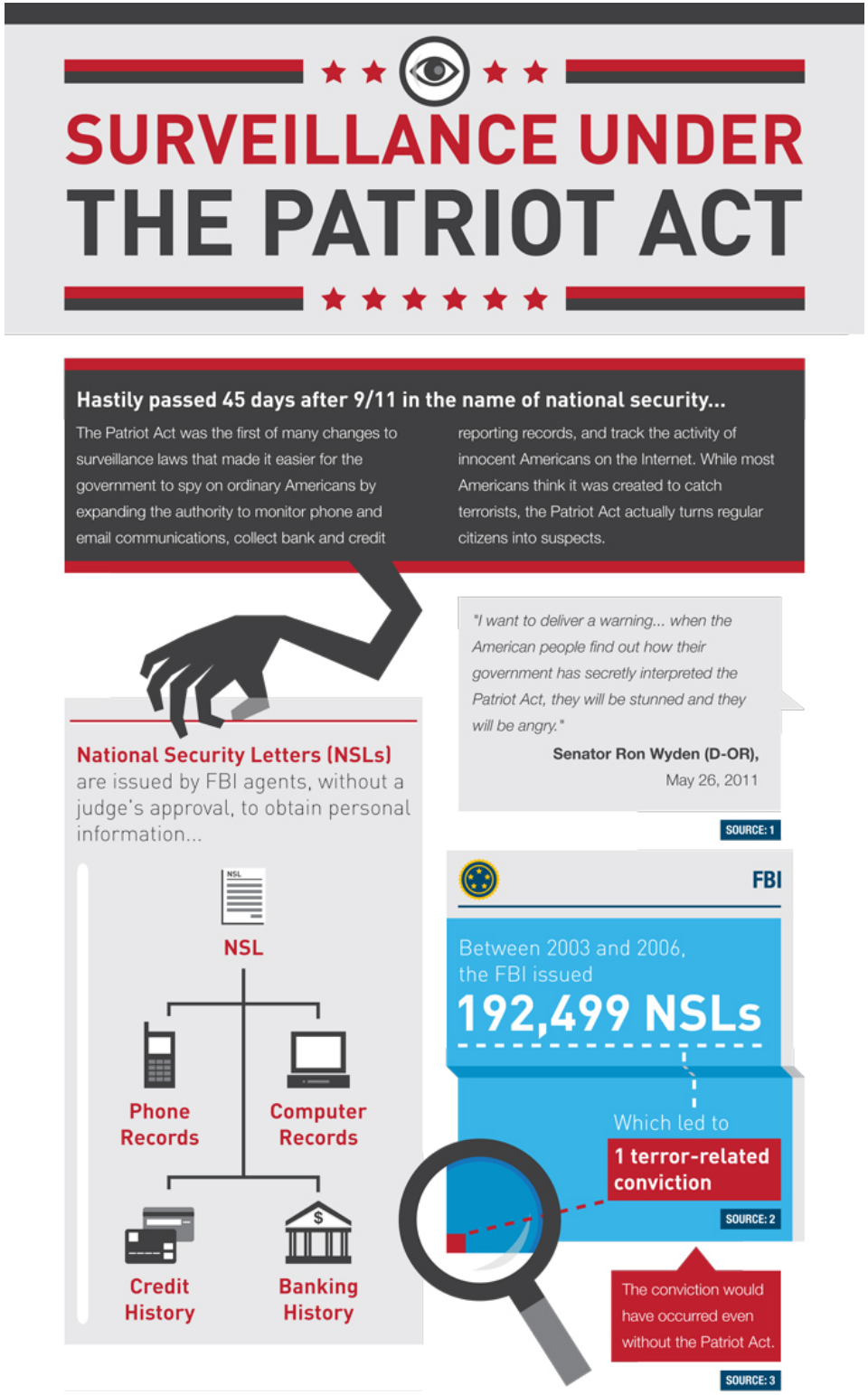
EECS 388: Intro to Security

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



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

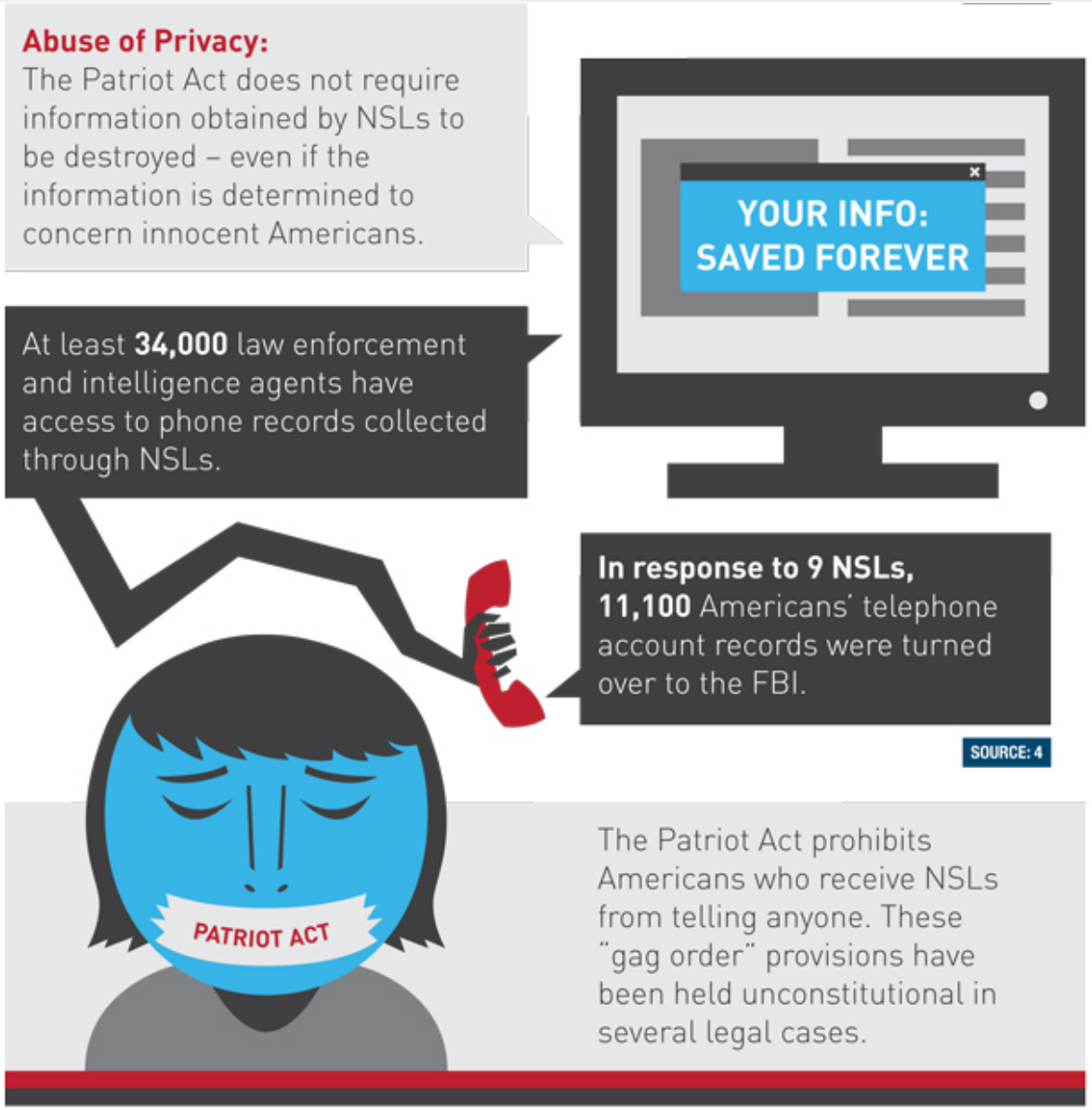


Image credit: ACLU

Surveillance under the PATRIOT Act

Image credit: ACLU

Google Transparency Report

Content requests (more significant that NSLs)

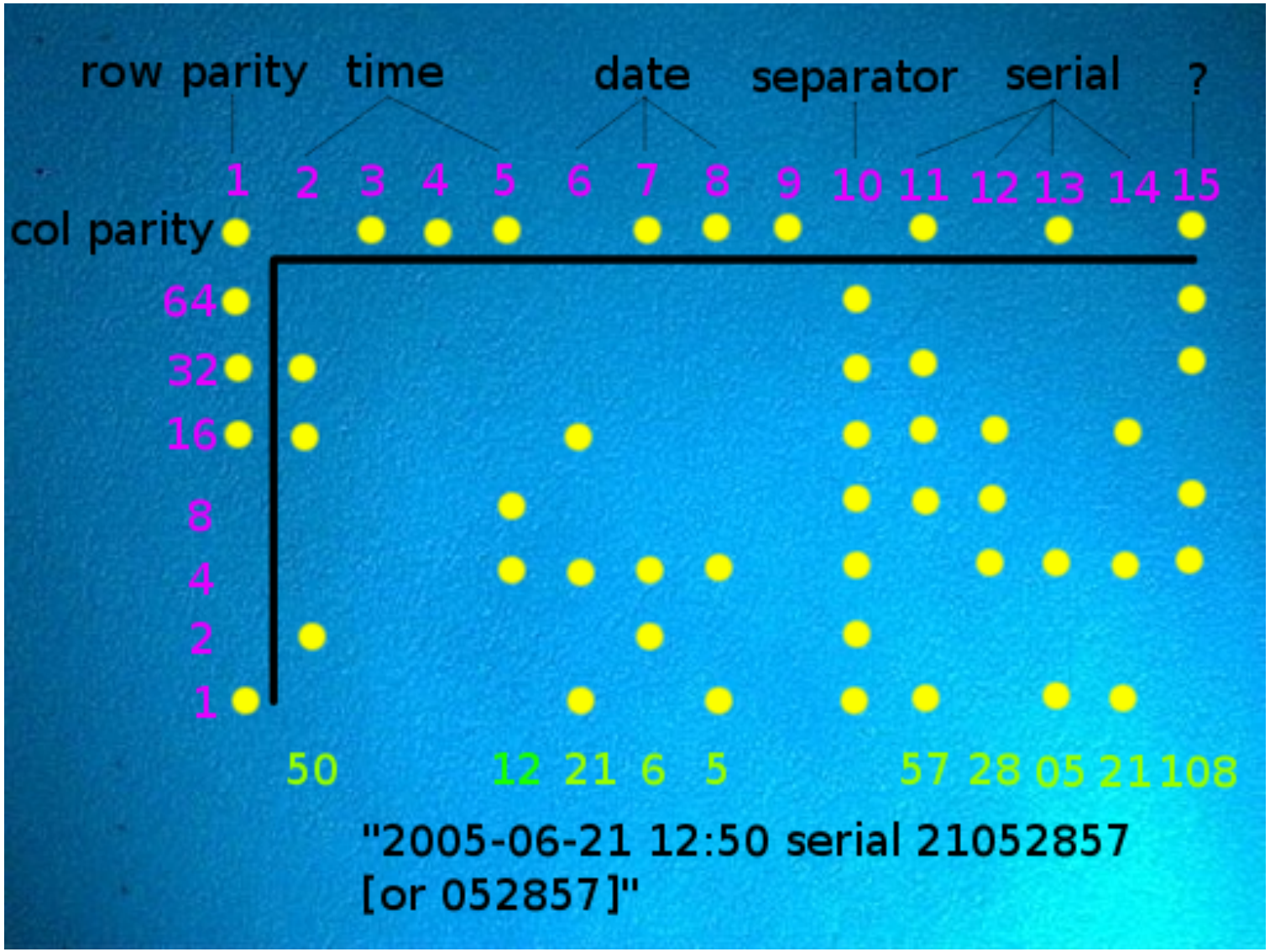
Reporting Period	Number of requests	Users/Accounts
January to June 2014	Data subject to six month reporting delay	
July to December 2013	0–999	15000–15999
January to June 2013	0–999	9000–9999
July to December 2012	0–999	12000–12999
January to June 2012	0–999	8000–8999
July to December 2011	0–999	9000–9999
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

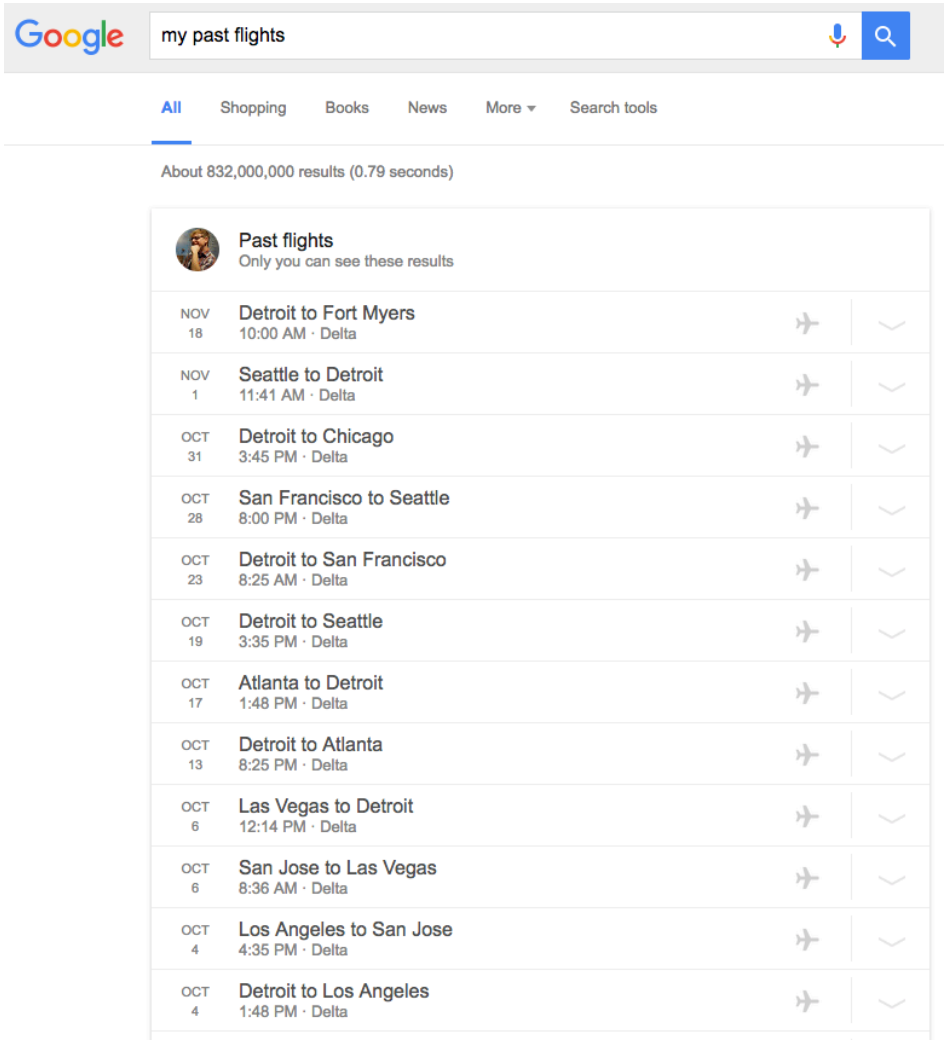
Modern day

Printer Paper

What your printer reveals about you



Privacy Risks: "Direct" sharing



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 women 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

amazon student 47 Amazon Students rated this highly ▾

4.5 out of 5 stars

List Price: ~~$19.57~~

Price: $12.98 Prime & 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	2	3
$12.98 Prime	$41.00 Prime	$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

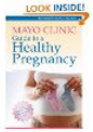
4.0 out of 5 stars 140

$20.25 Prime

One A Day Women's Prenatal One Pill, 30 Count

4.0 out of 5 stars 18

$13.48 Prime



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

3.5 out of 5 stars 19

$14.06 Prime

Nature Made Prenatal Multi Vitamin Value Size, Tablets, 250-Count

4.5 out of 5 stars 213

$16.79 Prime

Trojan Condom Pleasure Pack Lubricated, 40 Count

4.5 out of 5 stars 126

$18.12 Prime

Privacy Risks: Third-party tracking

COSMOPOLITAN LOVE | CELEBS | BEAUTY & STYLE | FITNESS

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

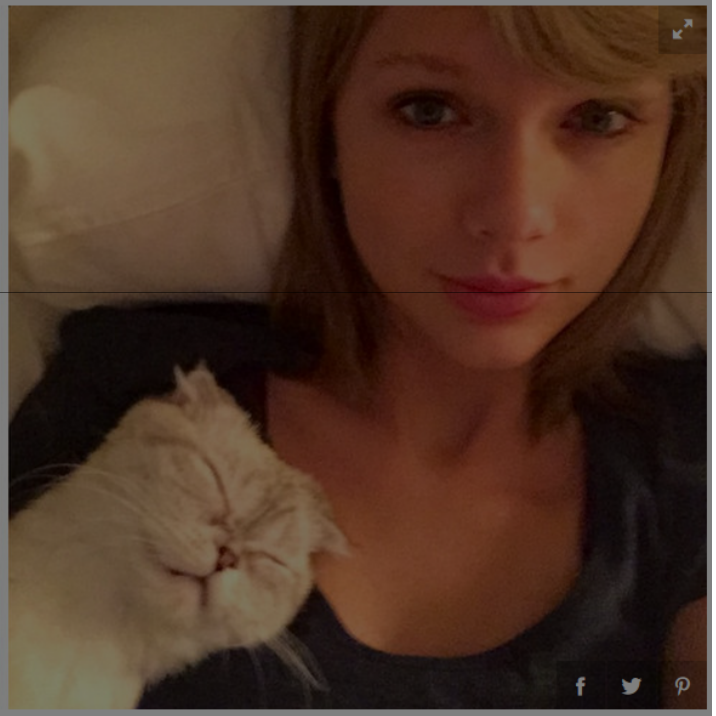
12.3k
Shares

SHARE 12.2K
TWEET 46
PIN 6

MOST READ

Does Seafood Make Guys Horny?

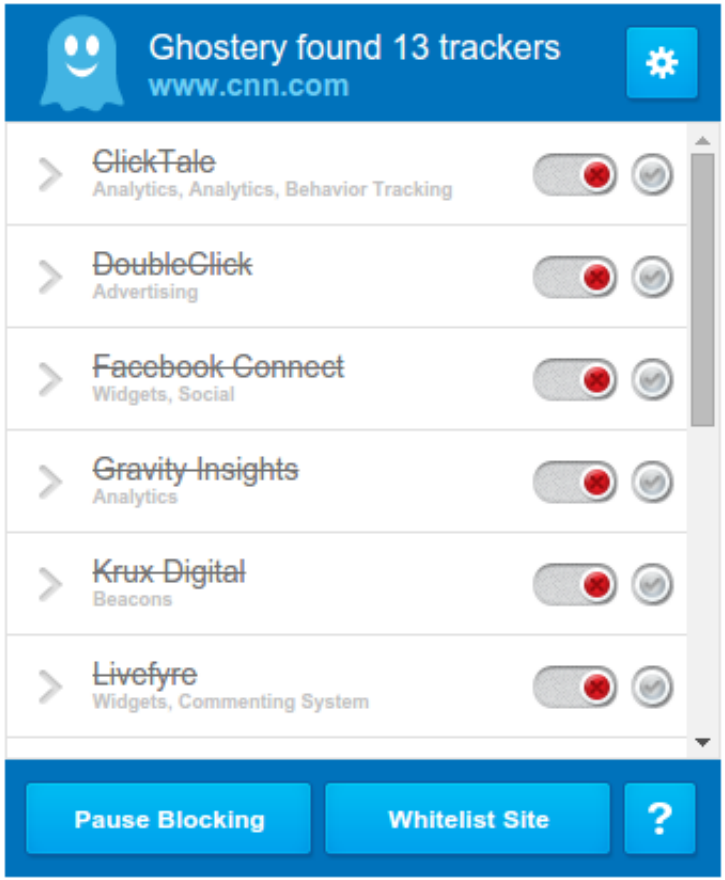
13 Things You Should Know Before Dating Someone Wh...

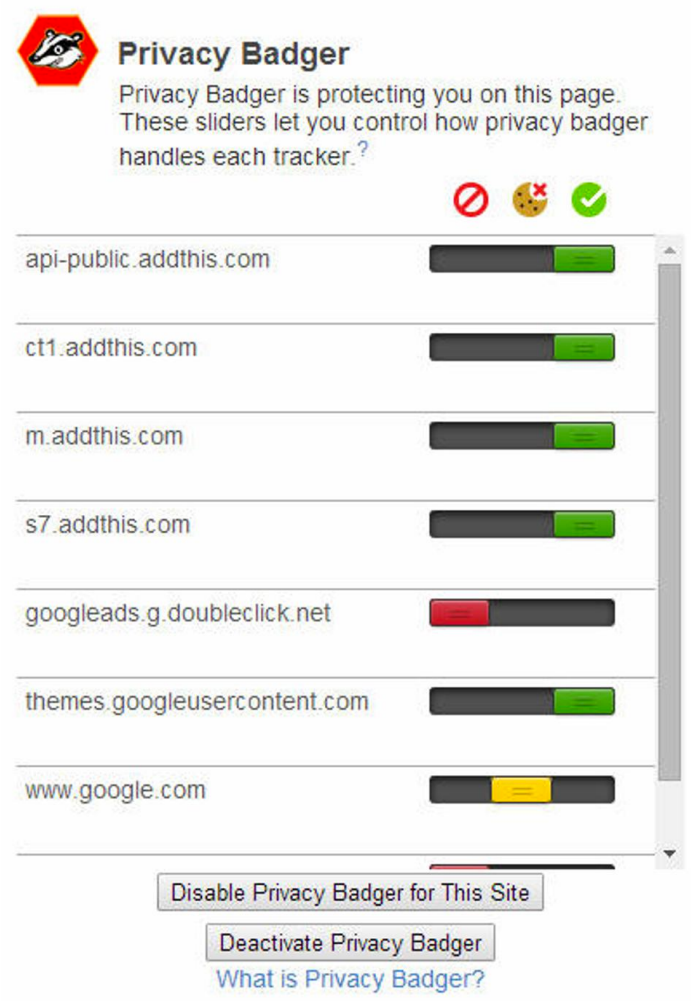


1. First of all, define "cat lady." Does one cat = cat lady? Two cats = cat lady? Does joking about being a cat lady à la sparkling, outgoing multimillionaire Taylor Swift automatically make one a cat lady? It is my personal belief that most female cat owners below the age of 40 fall into the "not a 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 hag who sits in front of your local Shop Rite with aluminum foil on her head

Blocking with Tools





Third-party cookies

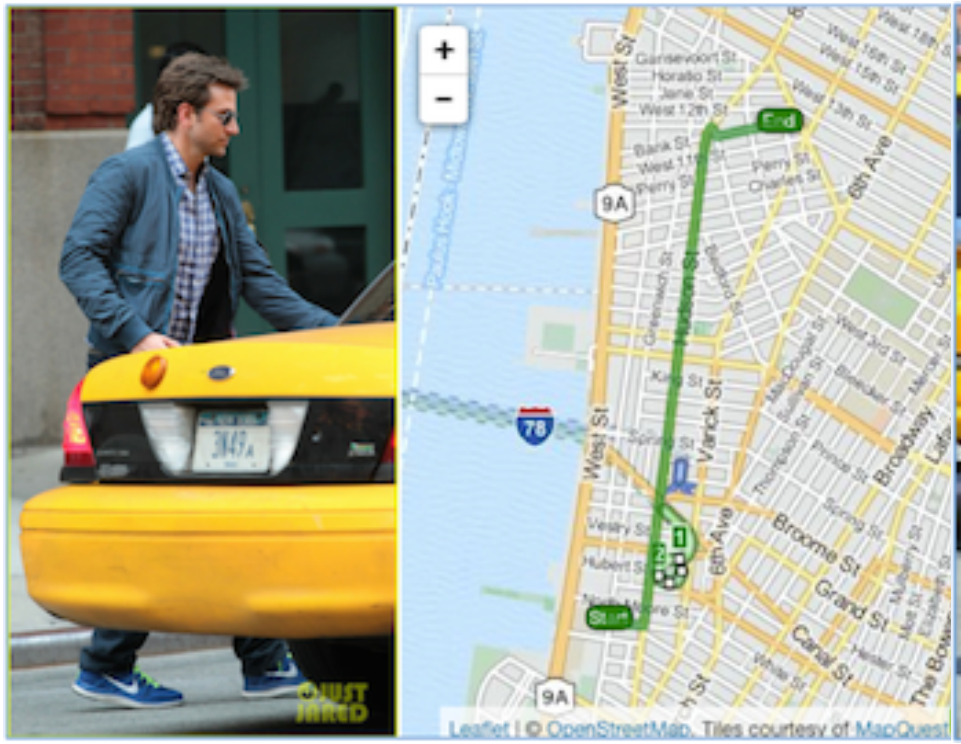
- Site A's page requests a third-party resource (image, script, iframe)
  - Normally, browser sends cookie associated with that third-party in that request

Third-party cookies

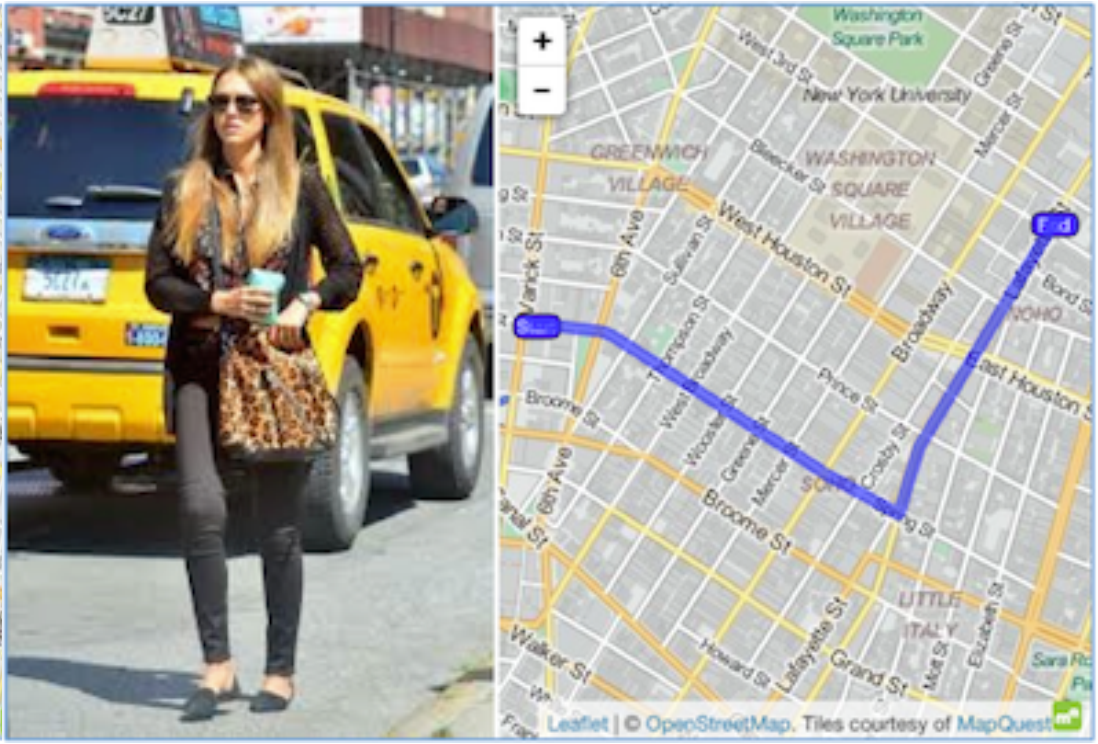
- Site A's page requests a third-party resource (image, script, iframe)
  - Normally, browser sends cookie associated with that third-party in that request

NYC Taxi Data

NYC Taxi – Tracking Celebrities

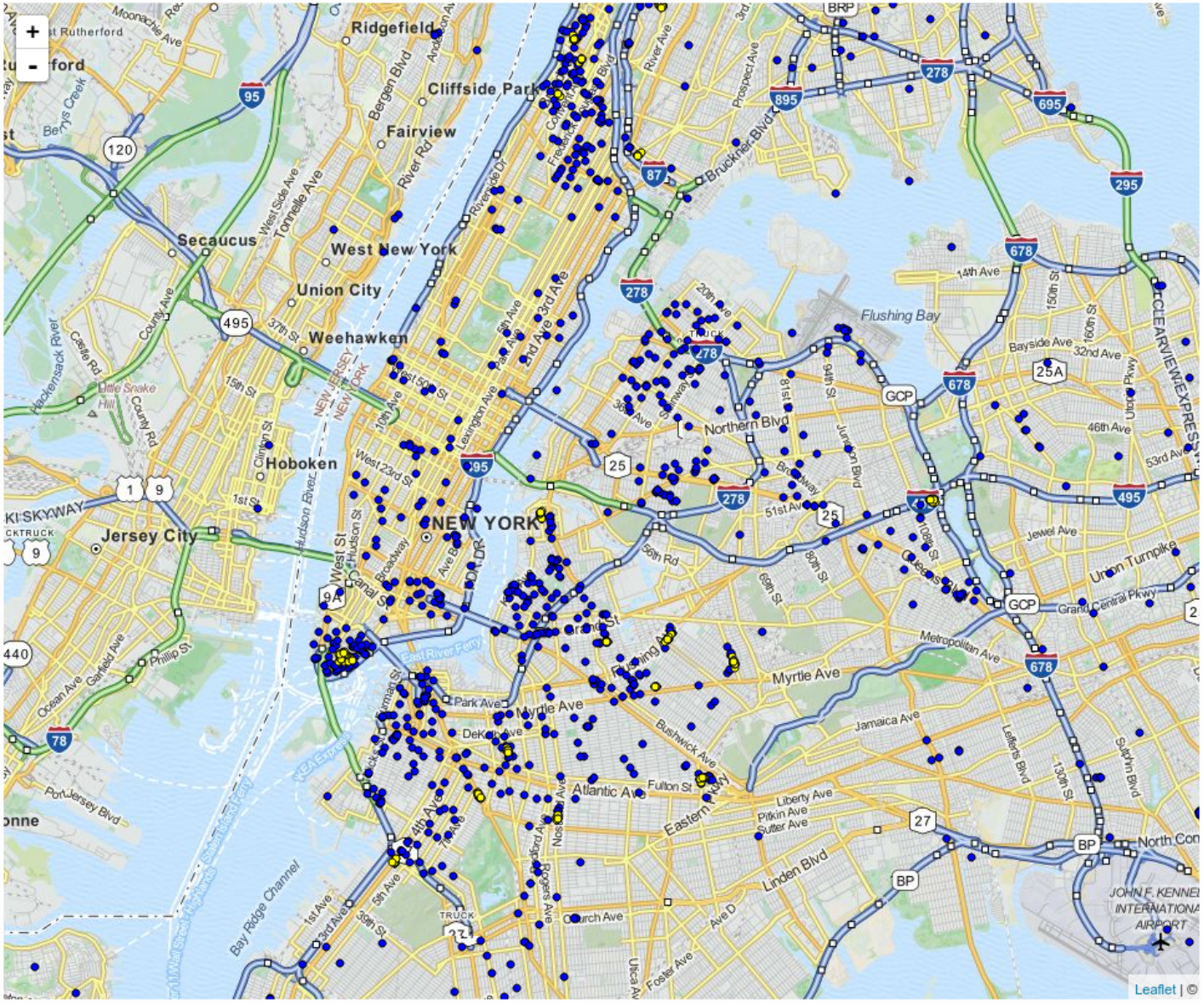


Bradley Cooper



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
4417749	60 single men
4417749	best retirement city
4417749	jarret arnold
4417749	jack t. arnold
4417749	jaylene and jarrett arnold
4417749	gwinnett county yellow pages
4417749	rescue of older dogs
4417749	movies for dogs
4417749	sinus infection

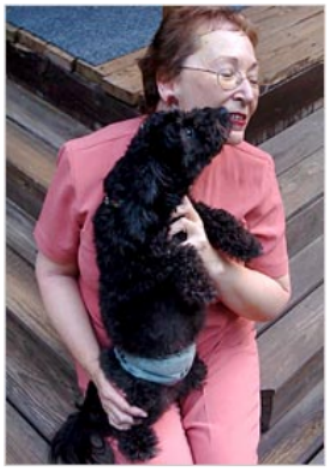
AOL Search Data Leak

A Face Is Exposed for AOL Searcher No. 4417749

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

SIGN IN TO E-MAIL THIS
PRINT
REPRINTS

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.

Multimedia

Graphic: What Revealing Search Data Reveals

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

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)

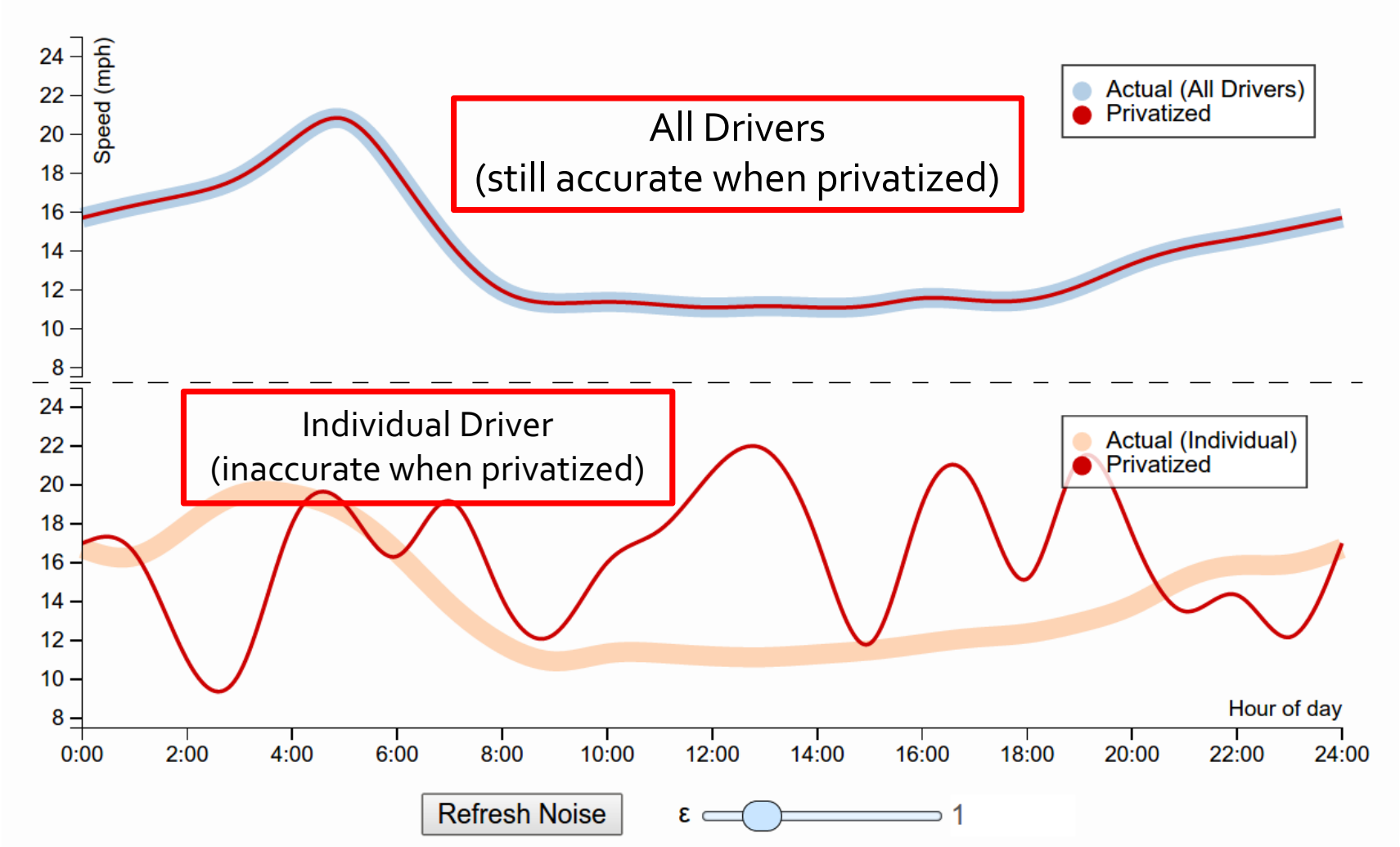
k-anonymity

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

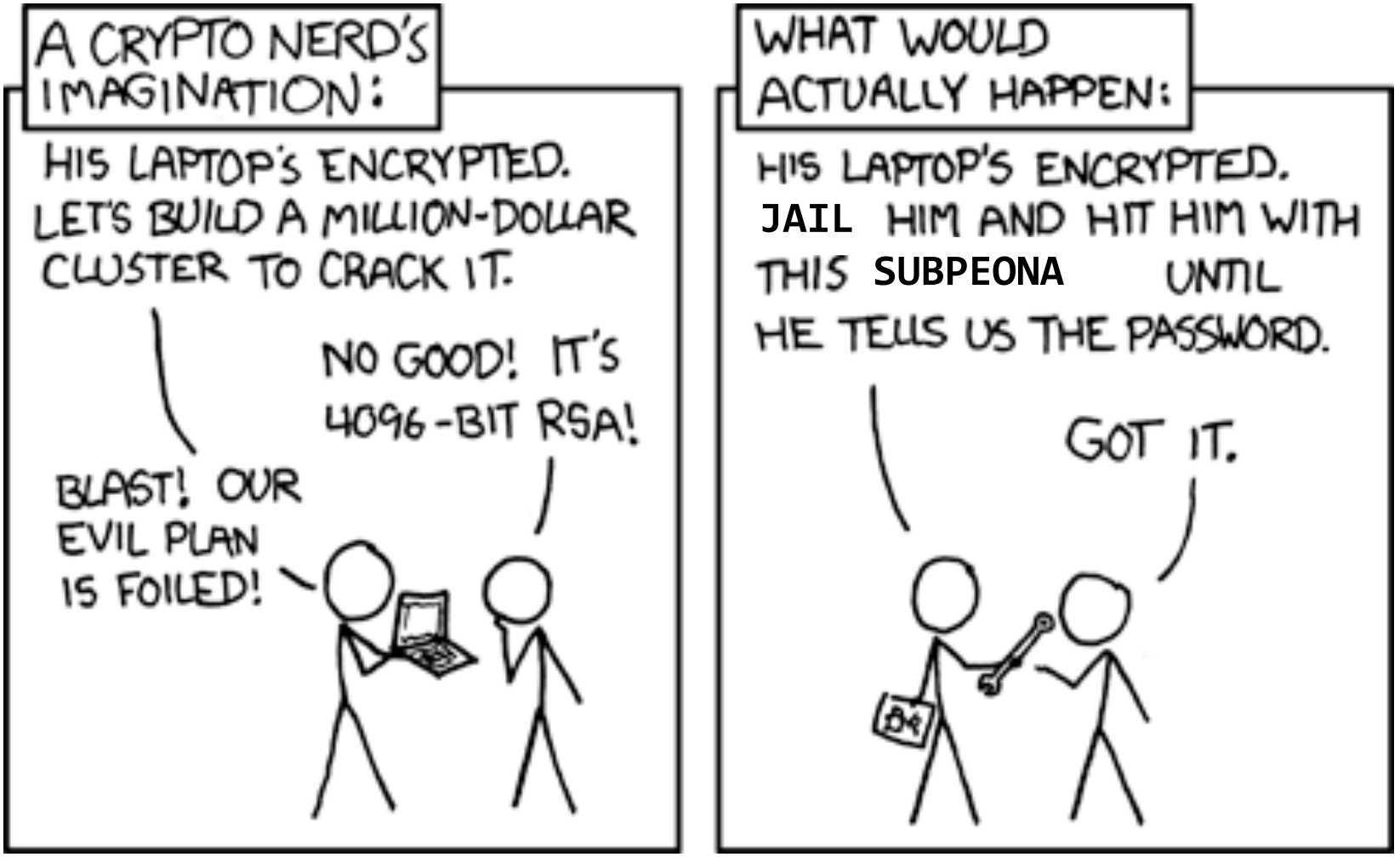
Another option: Differential Privacy

- 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.

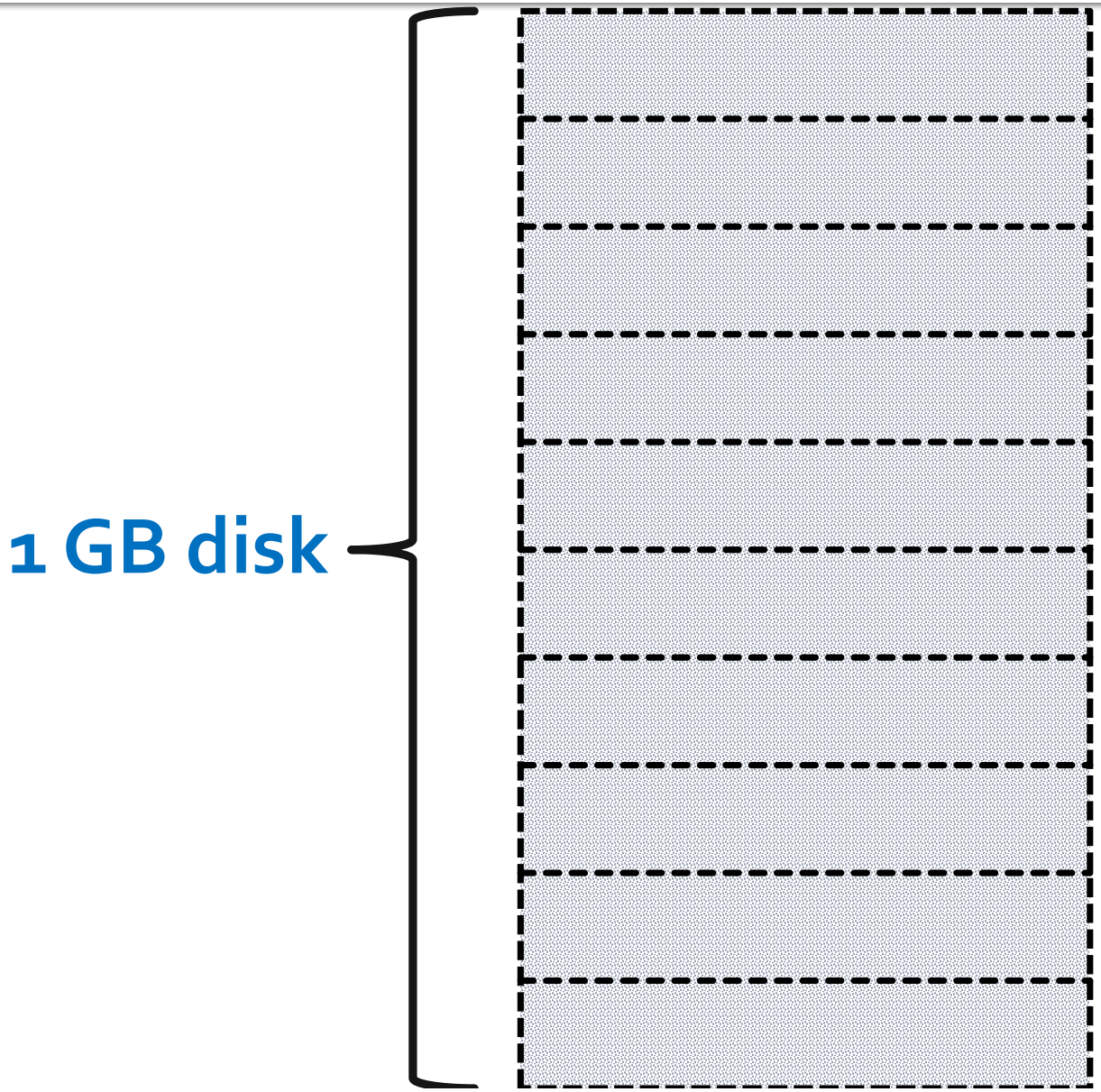
Differential Privacy



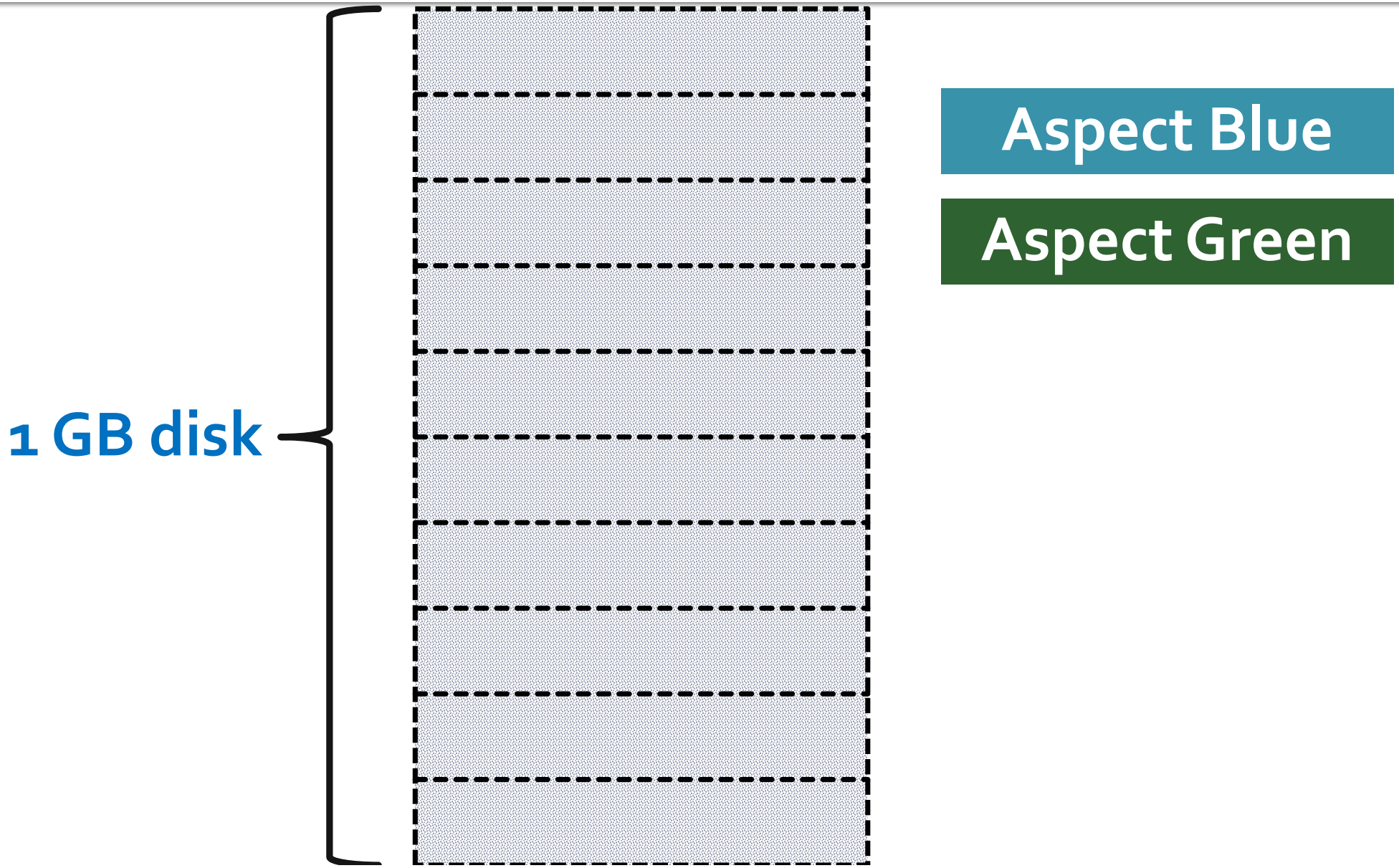
Privacy Defenses: Encrypt your filesystem(s)



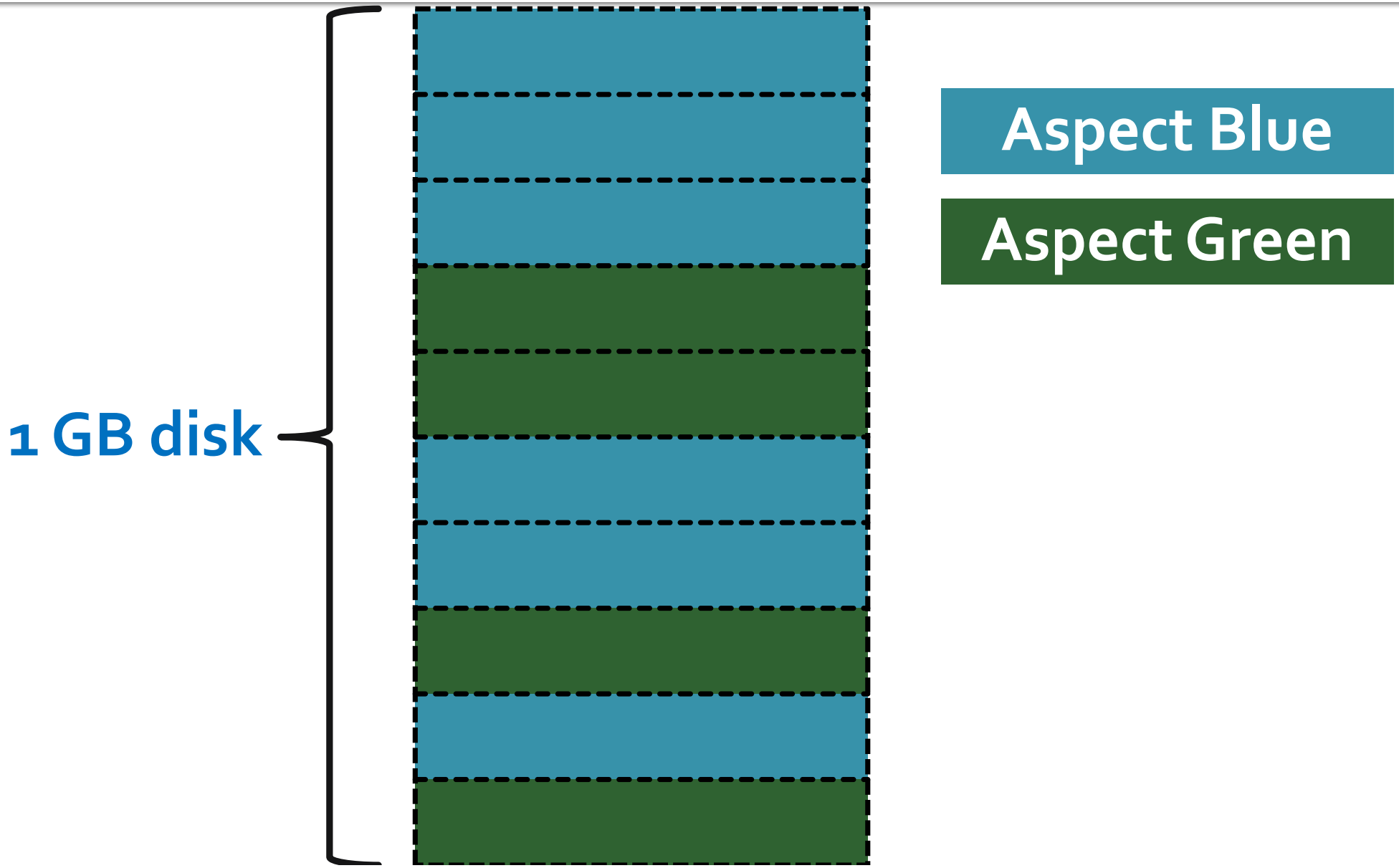
Rubberhose File System



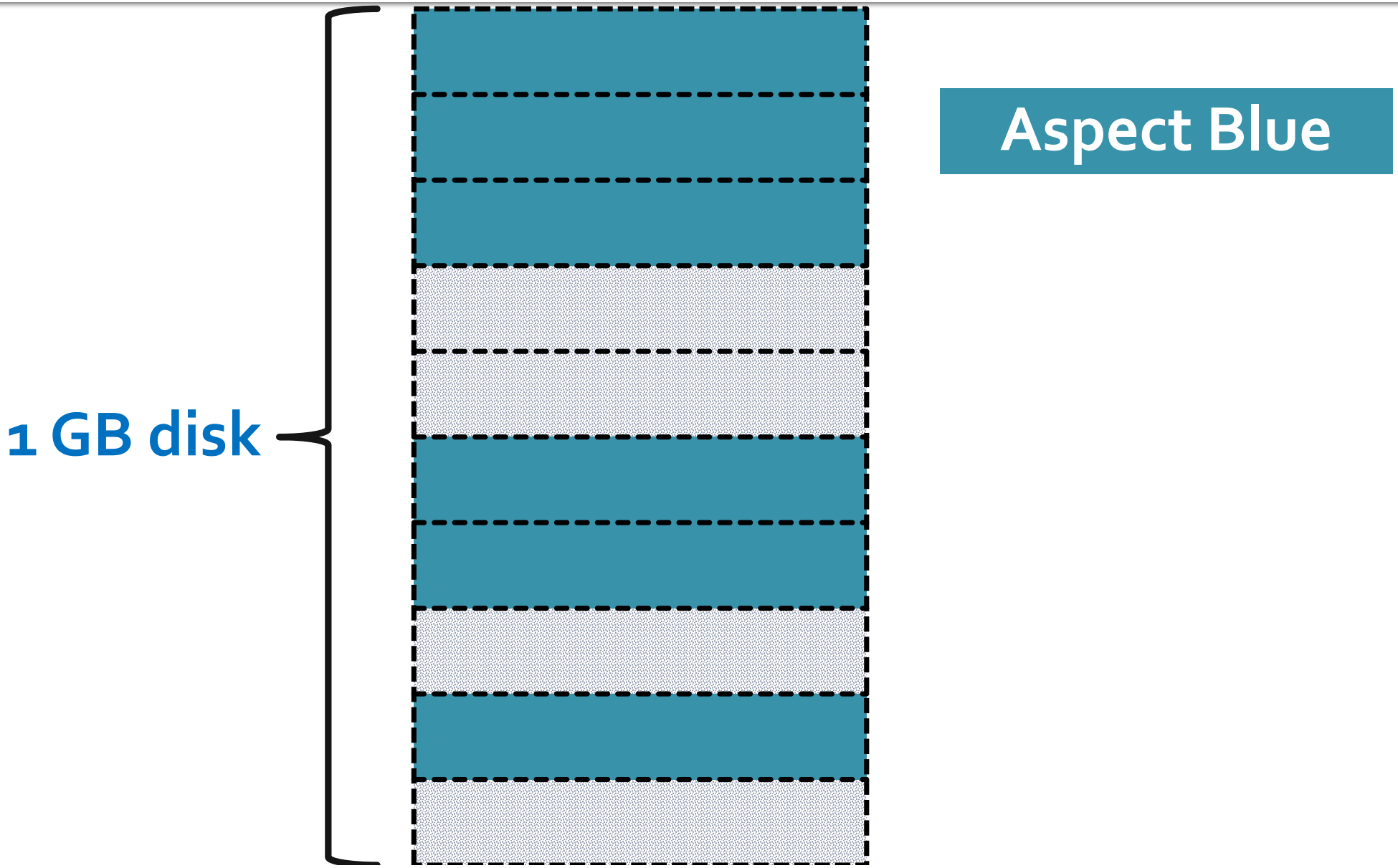
Rubberhose File System



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

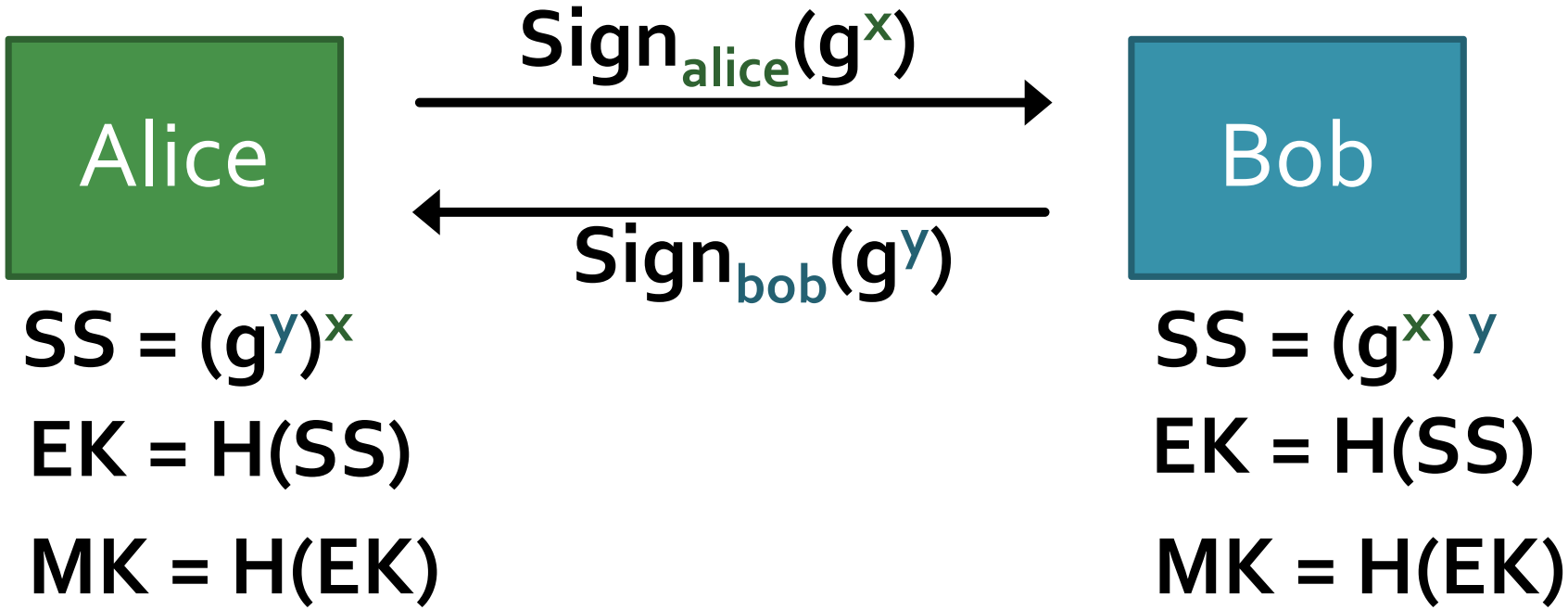
- Metadata is not encrypted
  - Sender, receiver, time sent, approx. msg length, subject, etc…
- What if Bob's machine was compromised?
  - His private key material becomes known
  - Past messages can be decrypted and read
  - Senders of email to Bob must trust his ability and desire to keep their messages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

Off-the-Record (OTR) Messaging

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

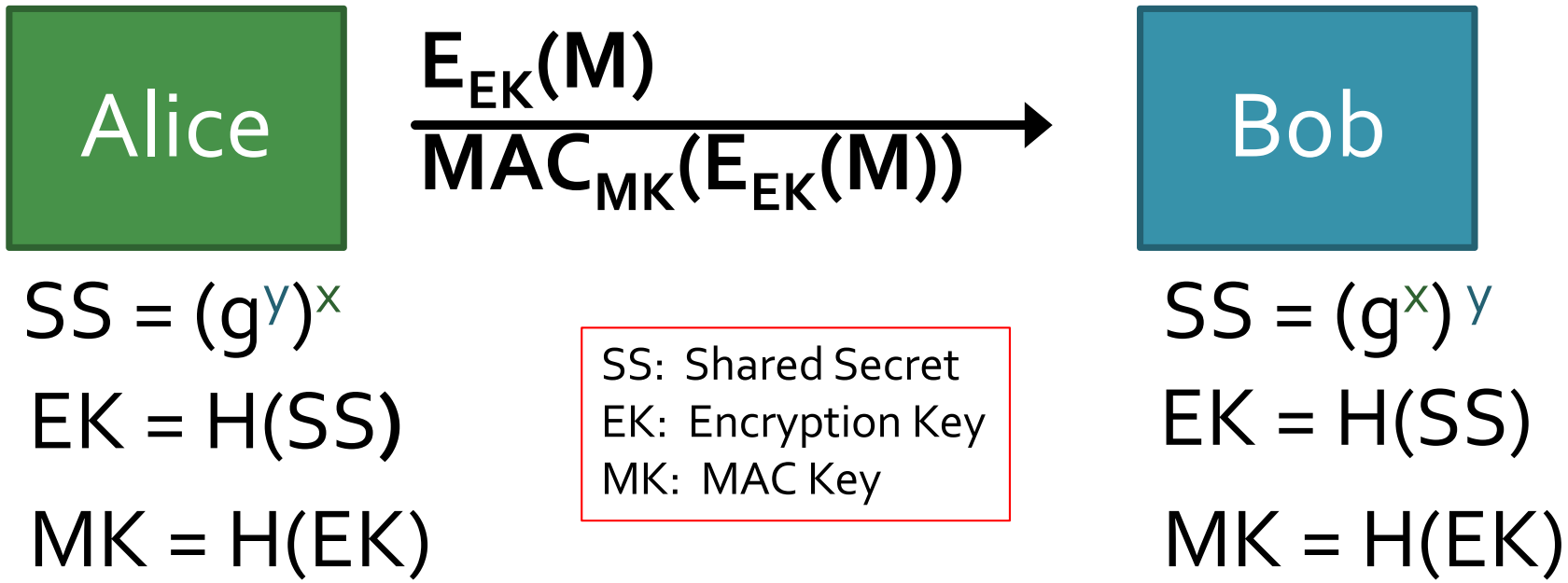
Off-the-Record (OTR) Messaging

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



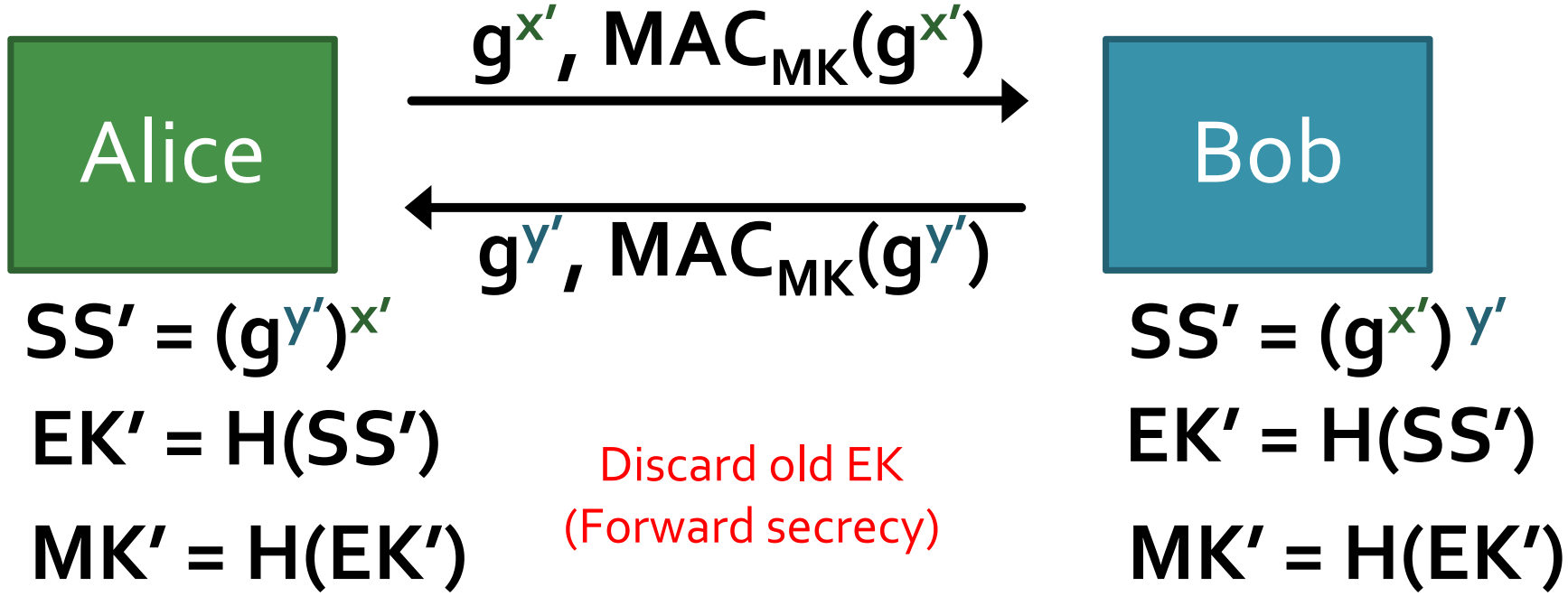
Off-the-Record (OTR) Messaging

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



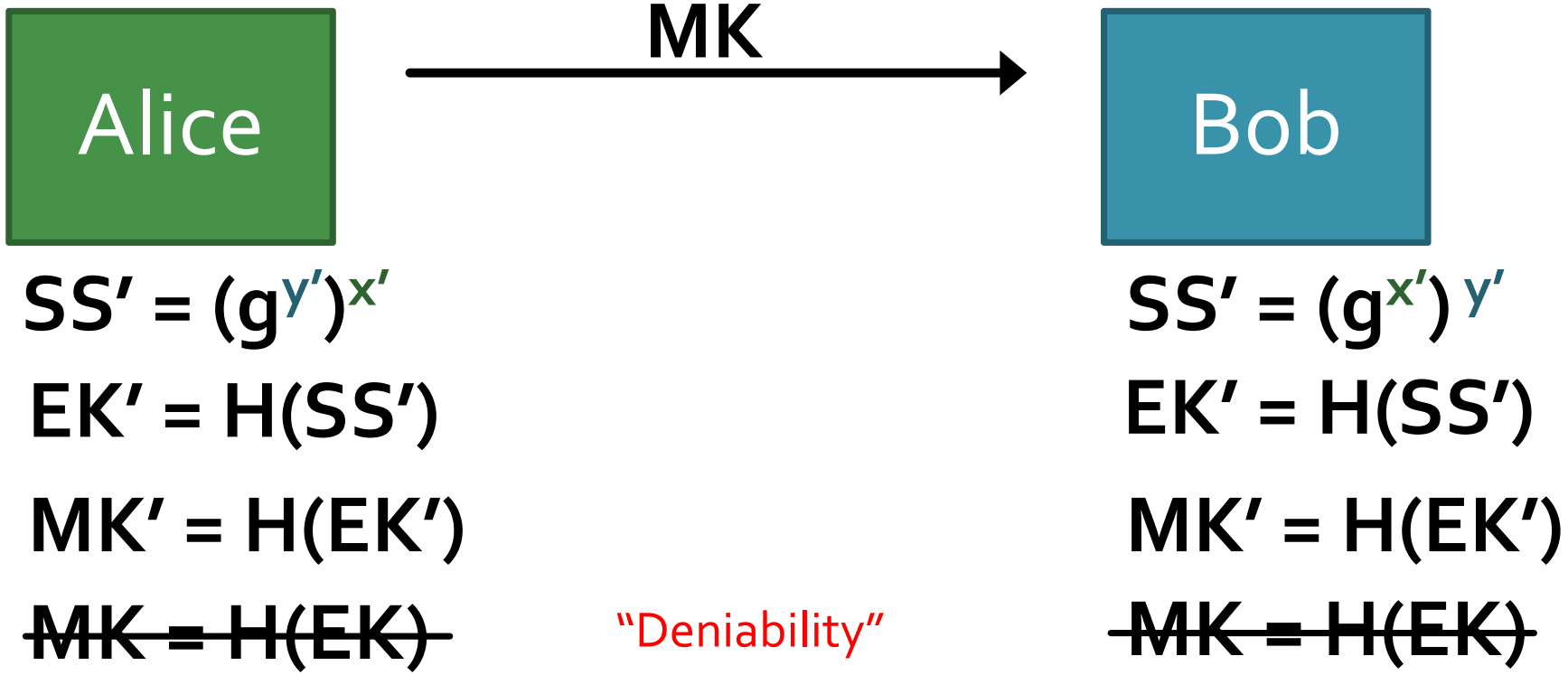
Off-the-Record (OTR) Messaging

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



Off-the-Record (OTR) Messaging

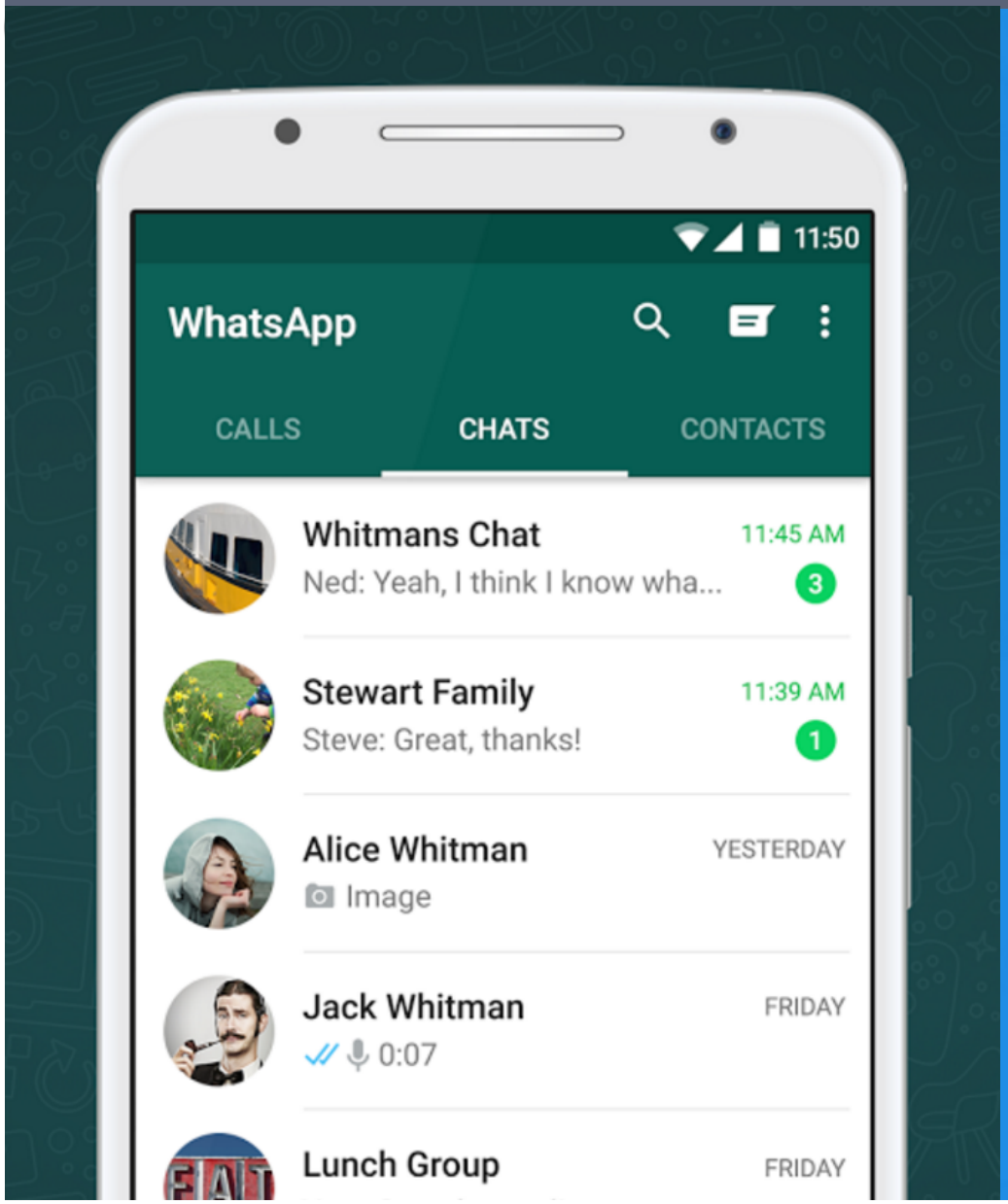
4. Stop using old MK…publish it!

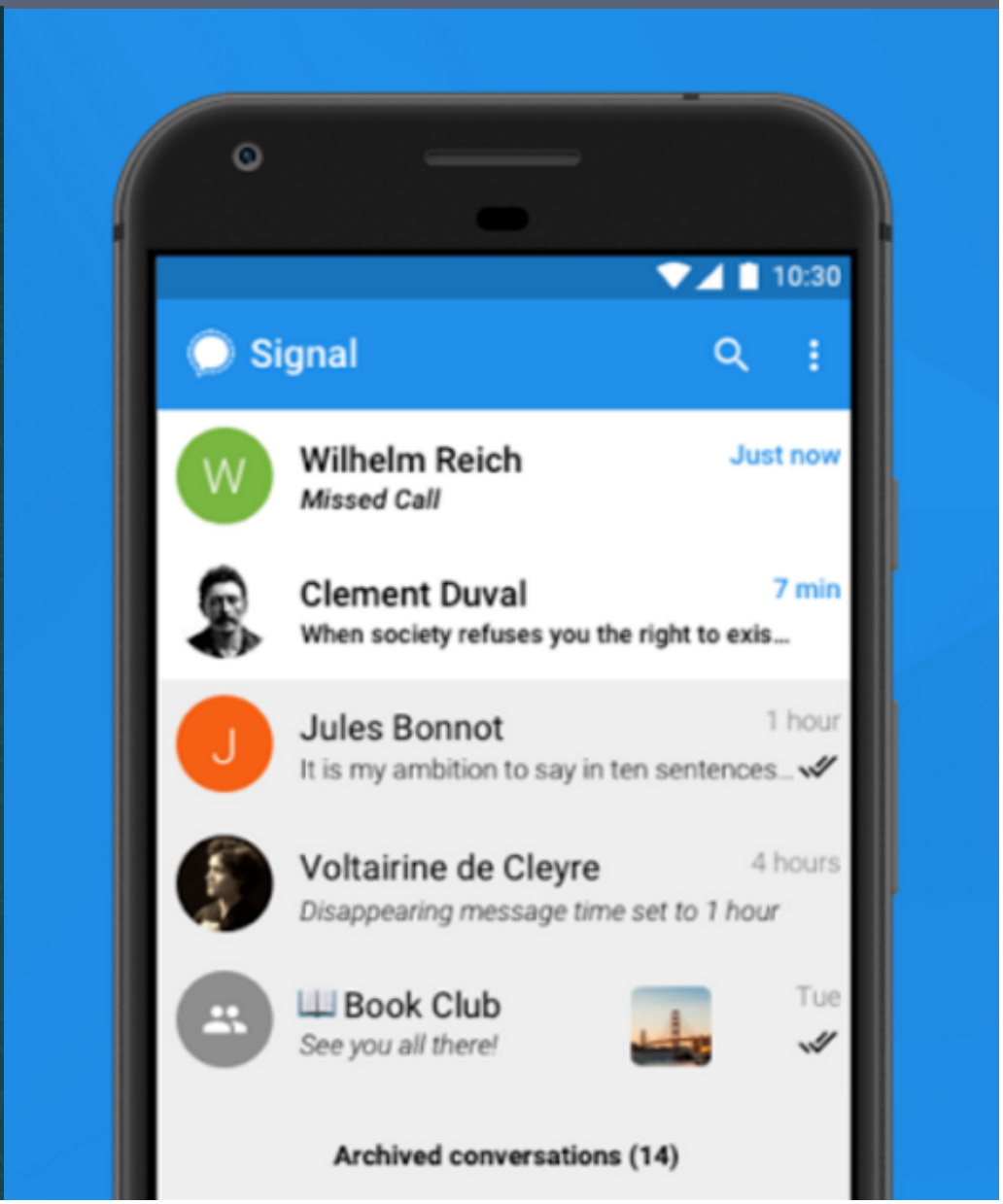


Off-the-Record Messaging (OTR)

- 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?

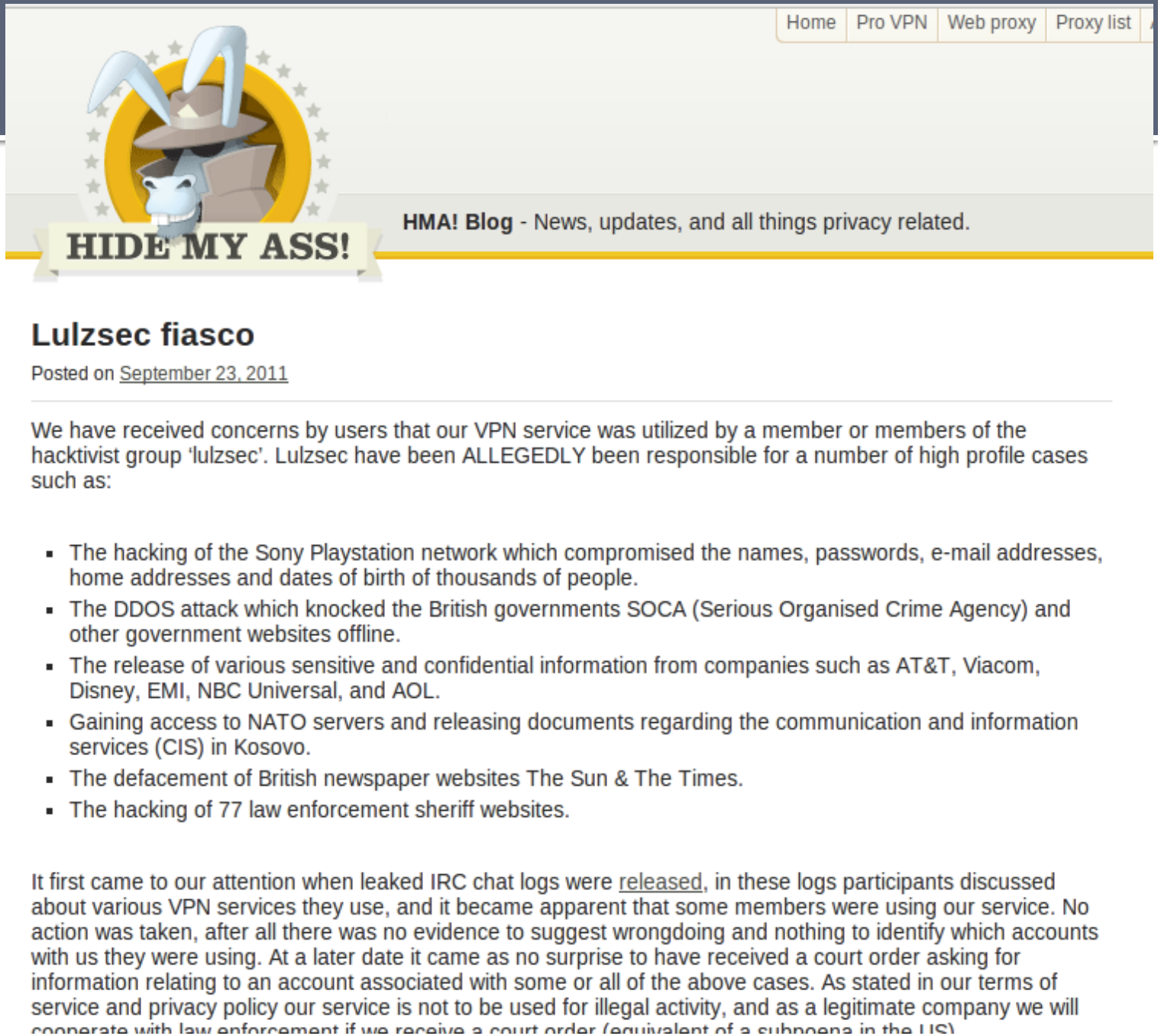
Naive approach …. VPNs

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?



VPNs

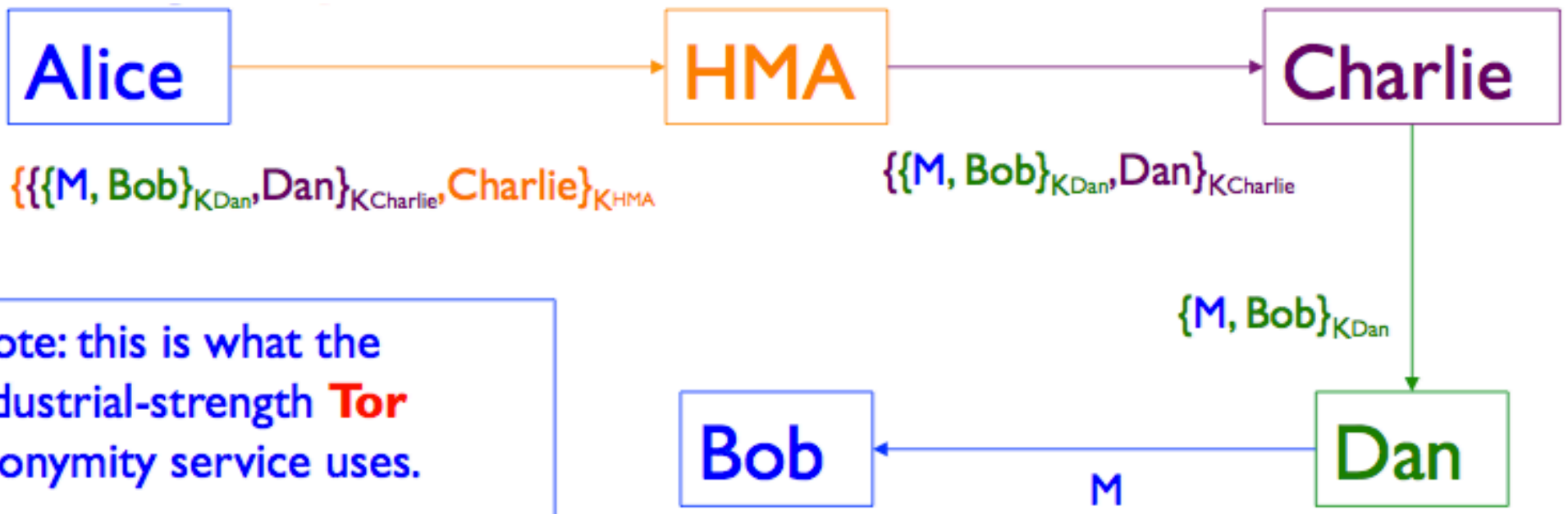
"…received a **court order** asking for information relating to an account associated with some or all of the above cases. As stated in our terms of service and **privacy policy** our service is not to be used for illegal activity, and as a legitimate company ***we will cooperate with law enforcement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

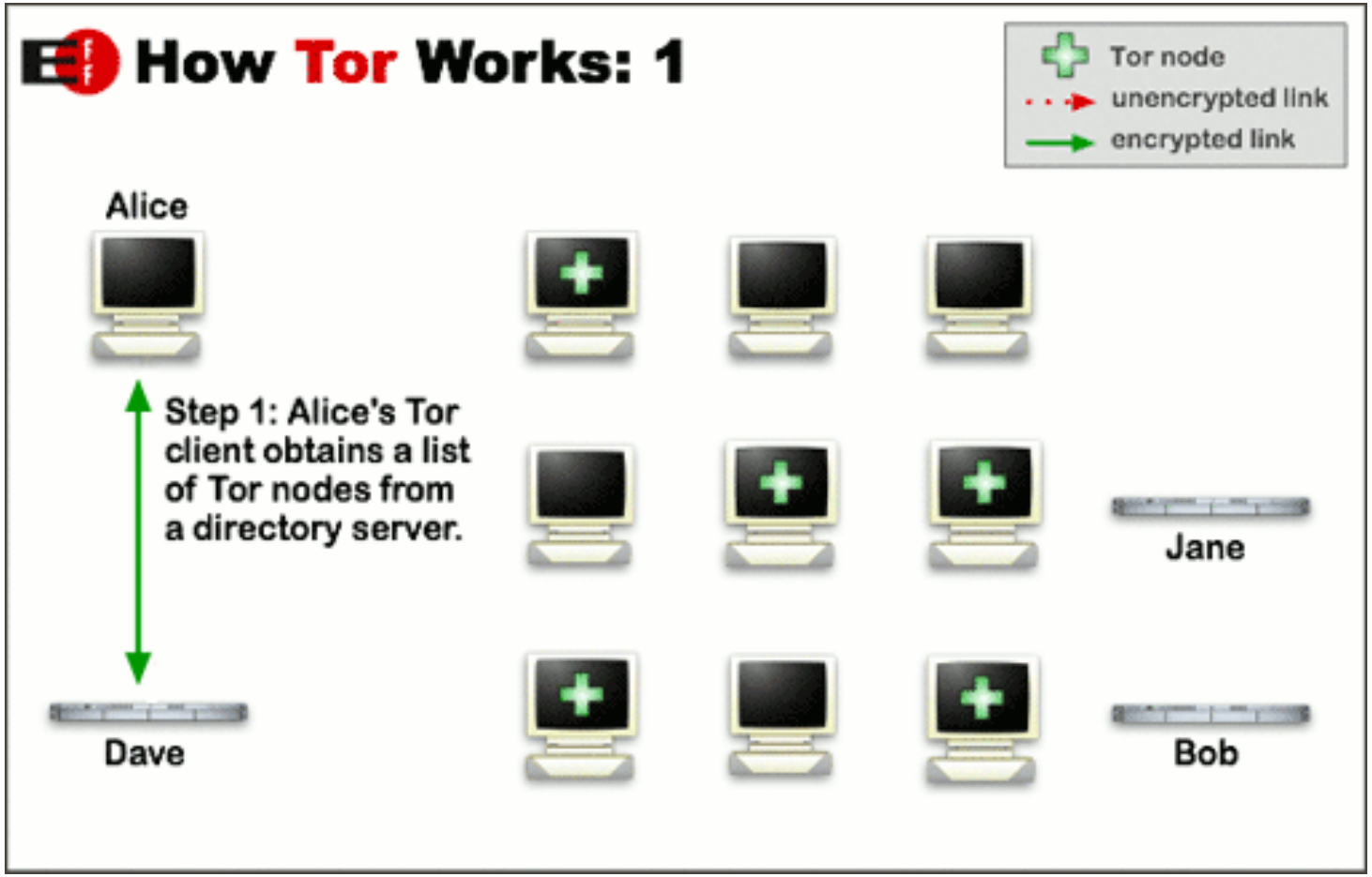


Note: this is what the industrial-strength **Tor** anonymity service uses.

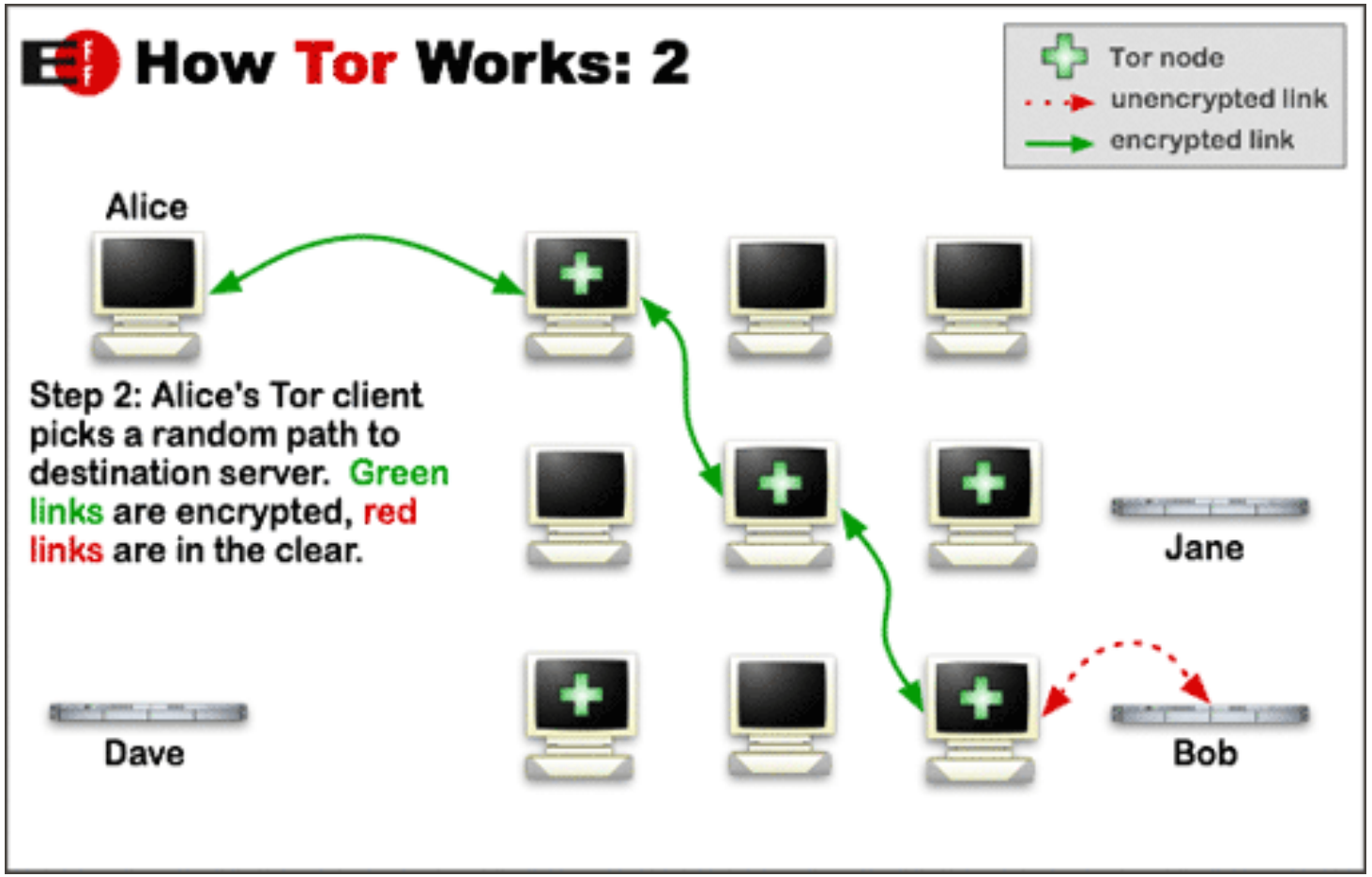
(It also provides bidirectional communication)

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

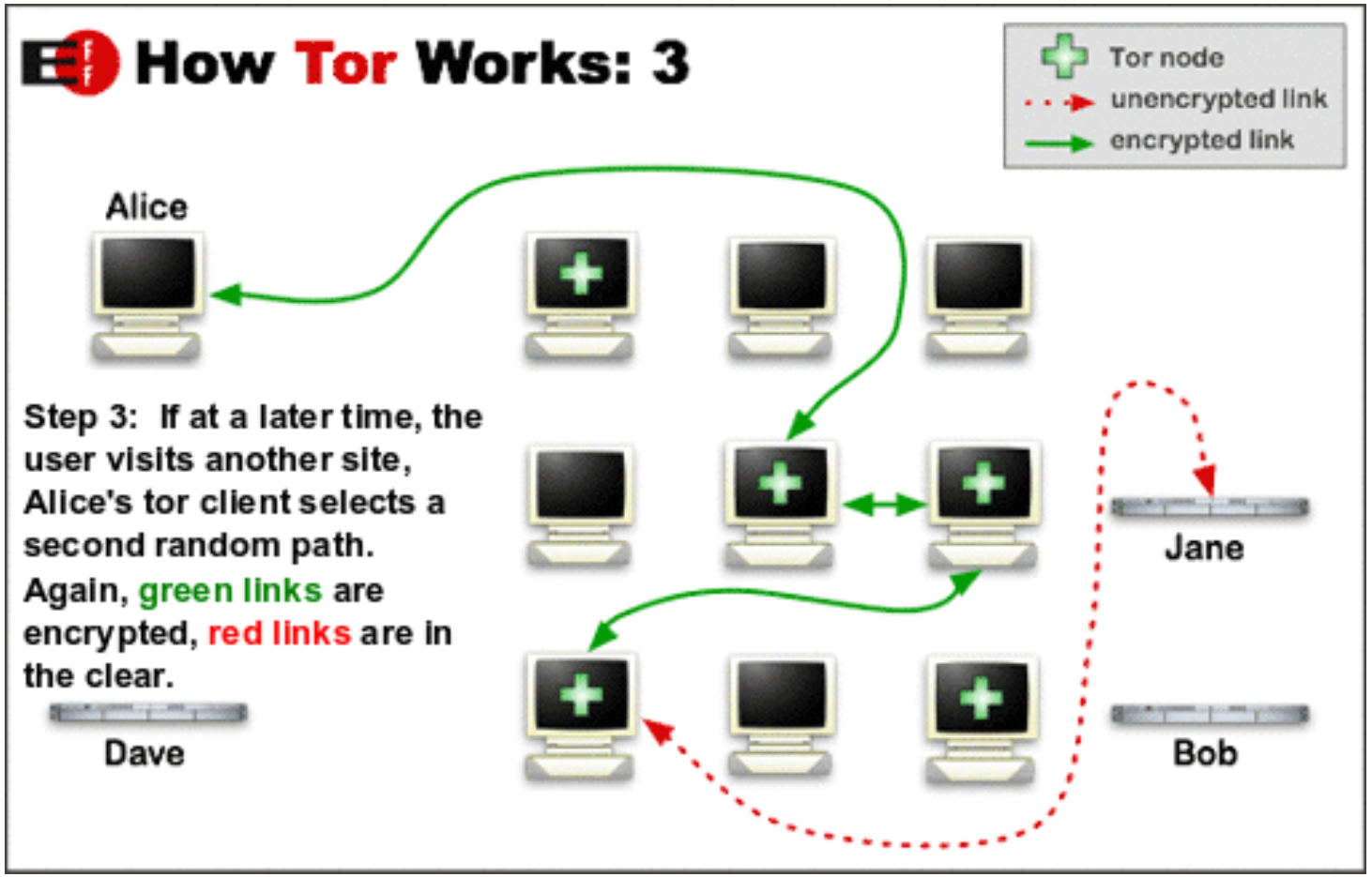
Tor


How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave
Bob

Tor


How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob

Tor


How Tor Works: 3
Tor node
unencrypted link
encrypted link
Alice
Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path.
Again, green links are encrypted, red links are in the clear.
Dave
Jane
Bob

Trust in Tor

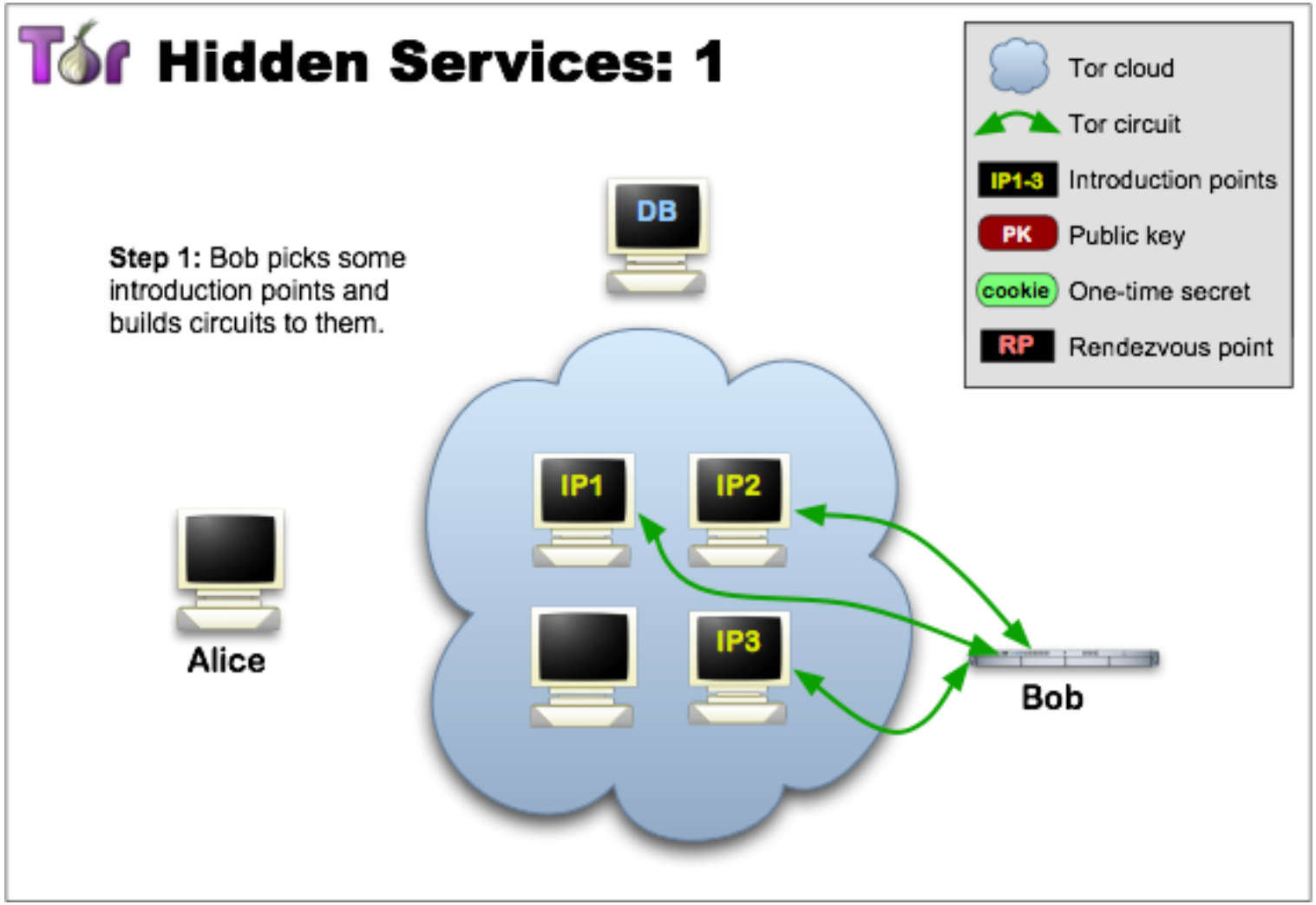
- **Entry node:** knows Alice is using Tor, and identity of middle node, but not destination
- **Exit node:** knows some Tor user is connecting to destination, but not which user
- **Destination:** knows a Tor user is connecting to it via the exit node

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

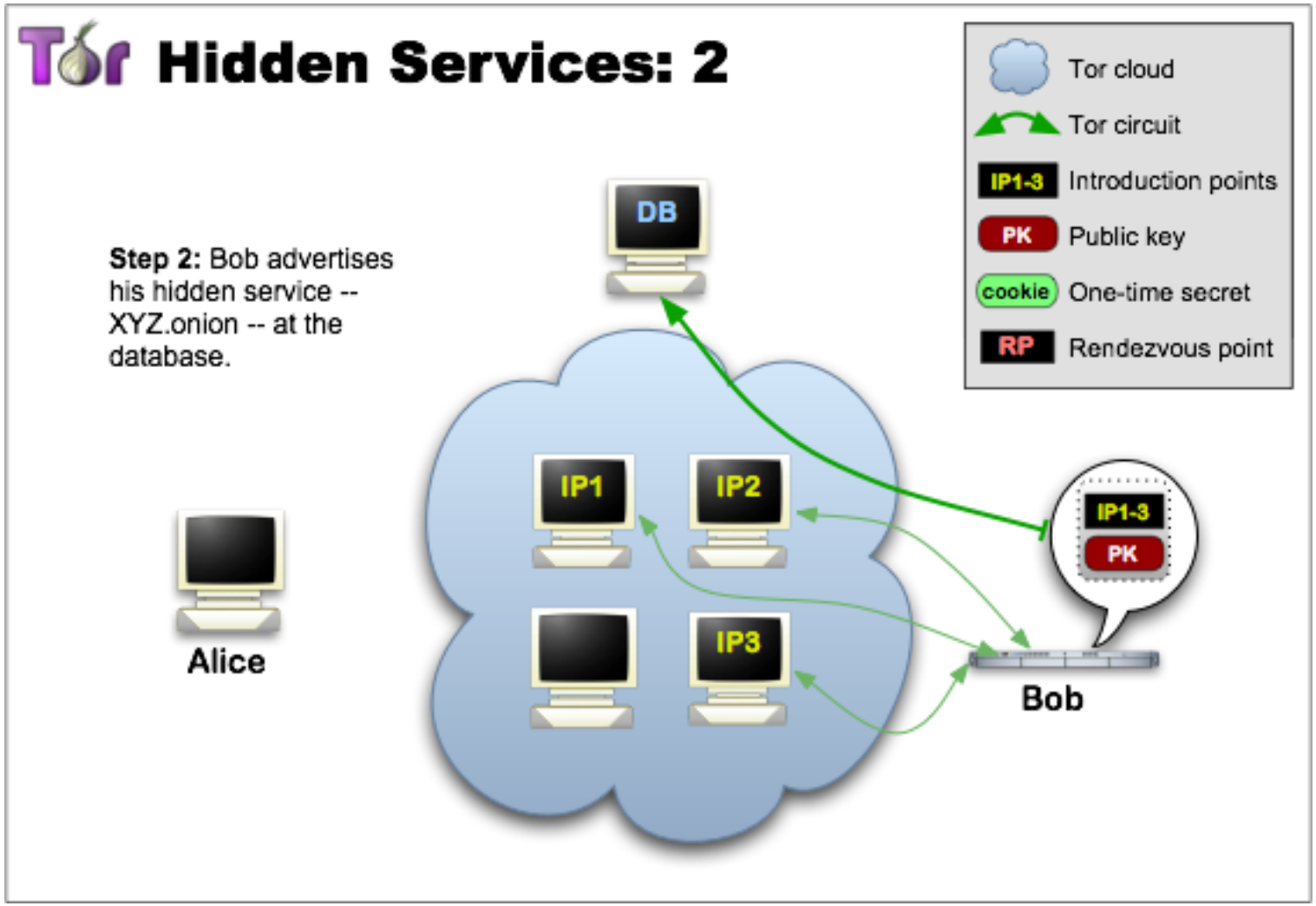
Onion Routing Issues/Attacks?

- 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

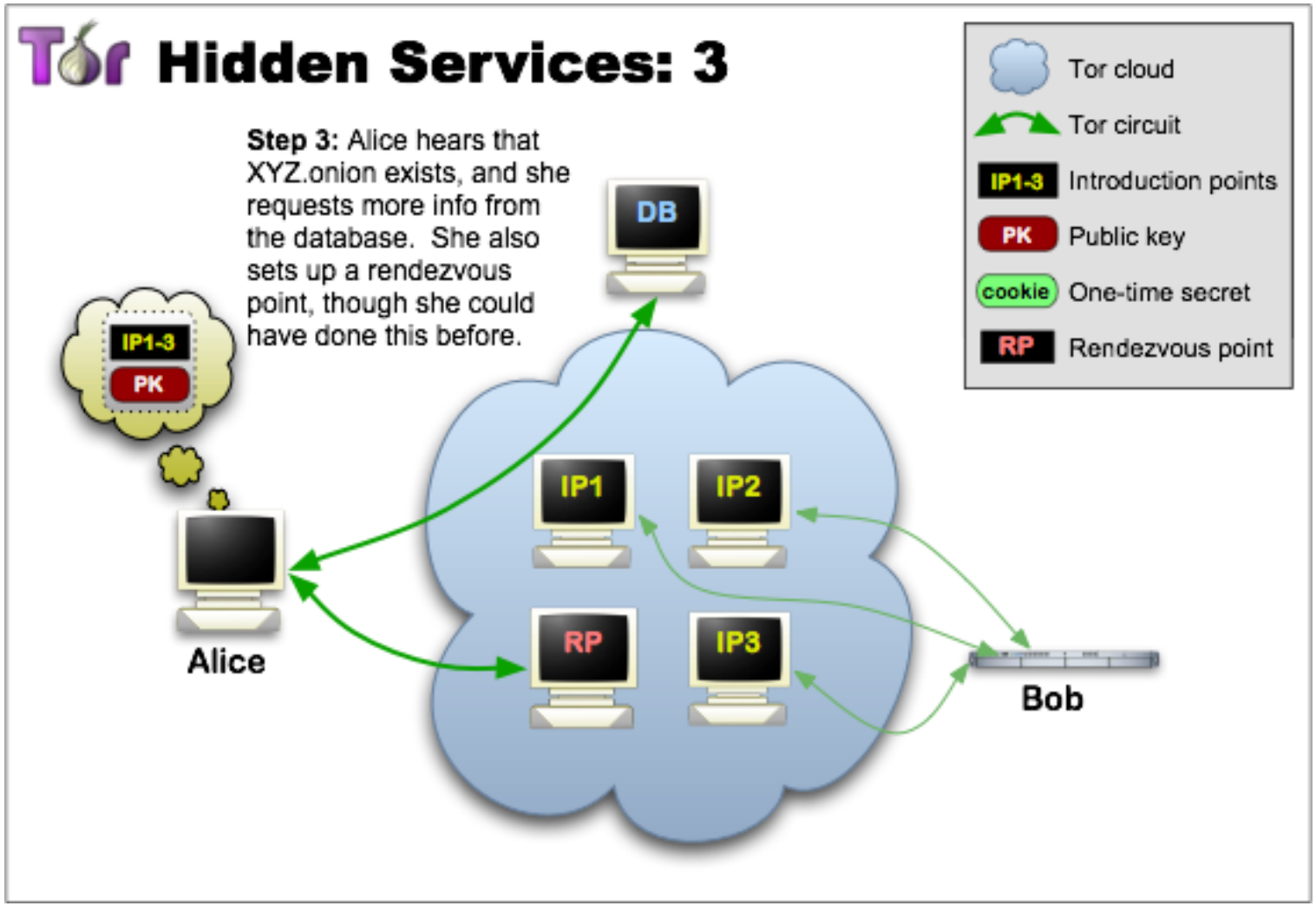
Tor Hidden Services: Overview



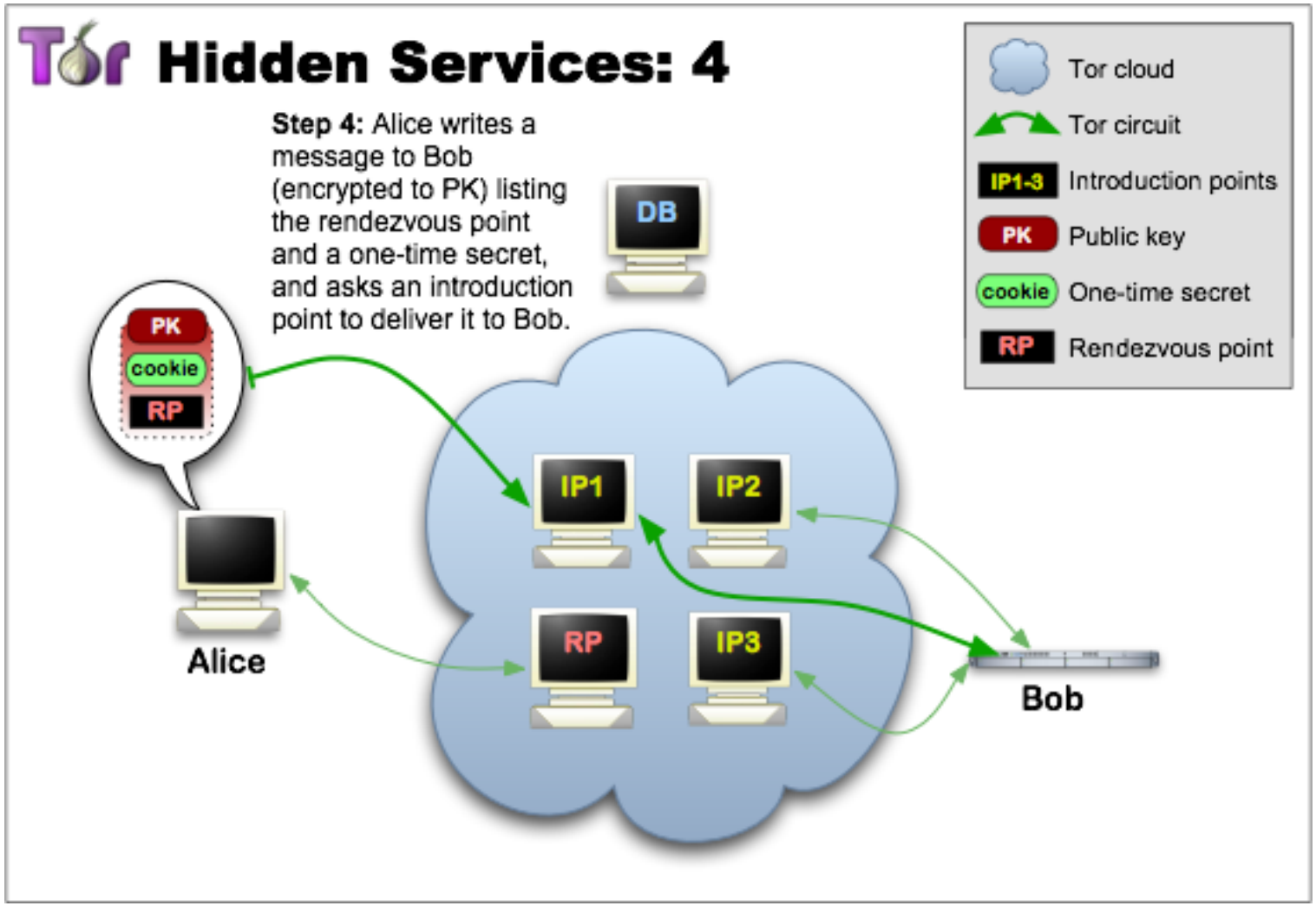
Tor Hidden Services



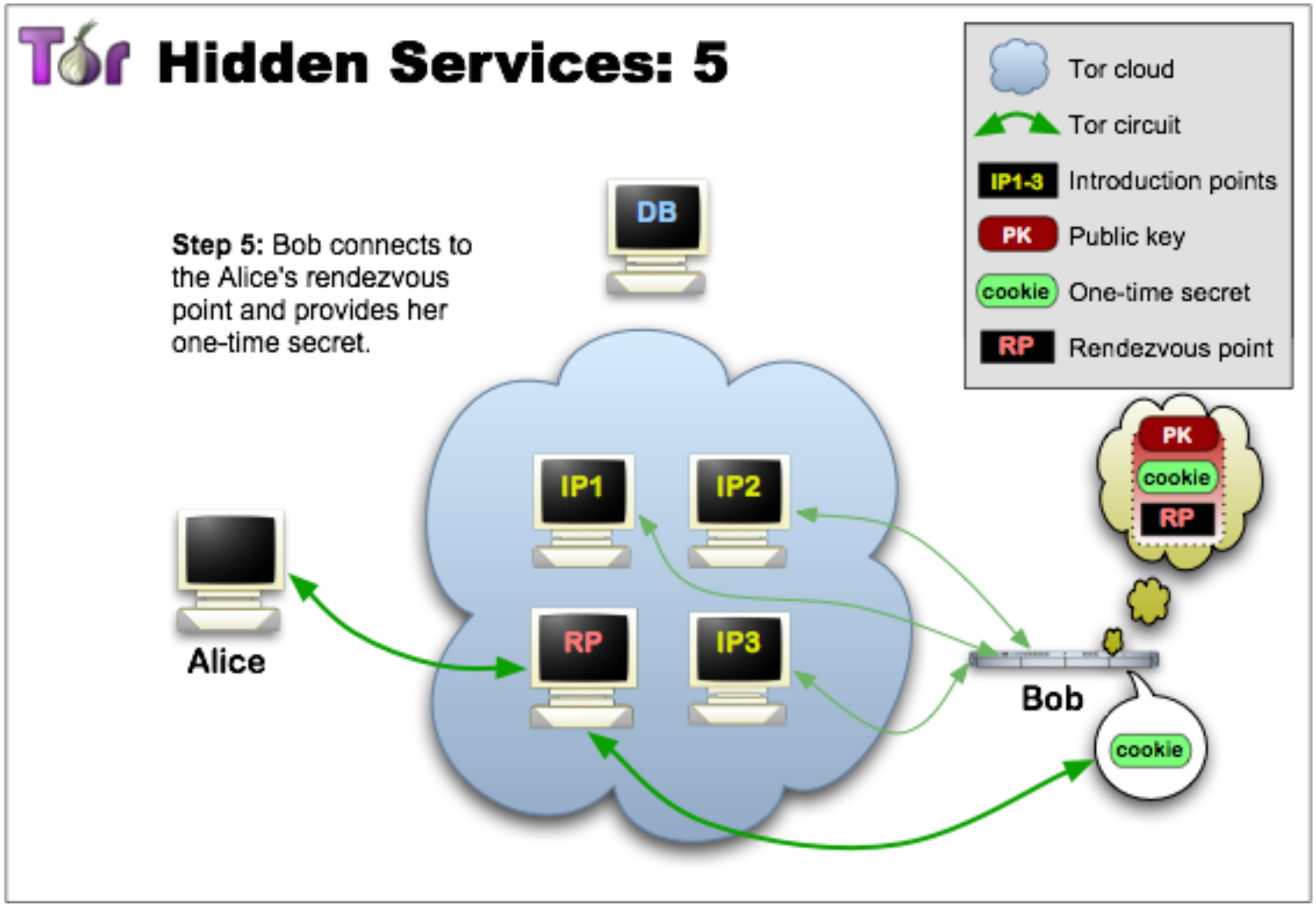
Tor Hidden Services



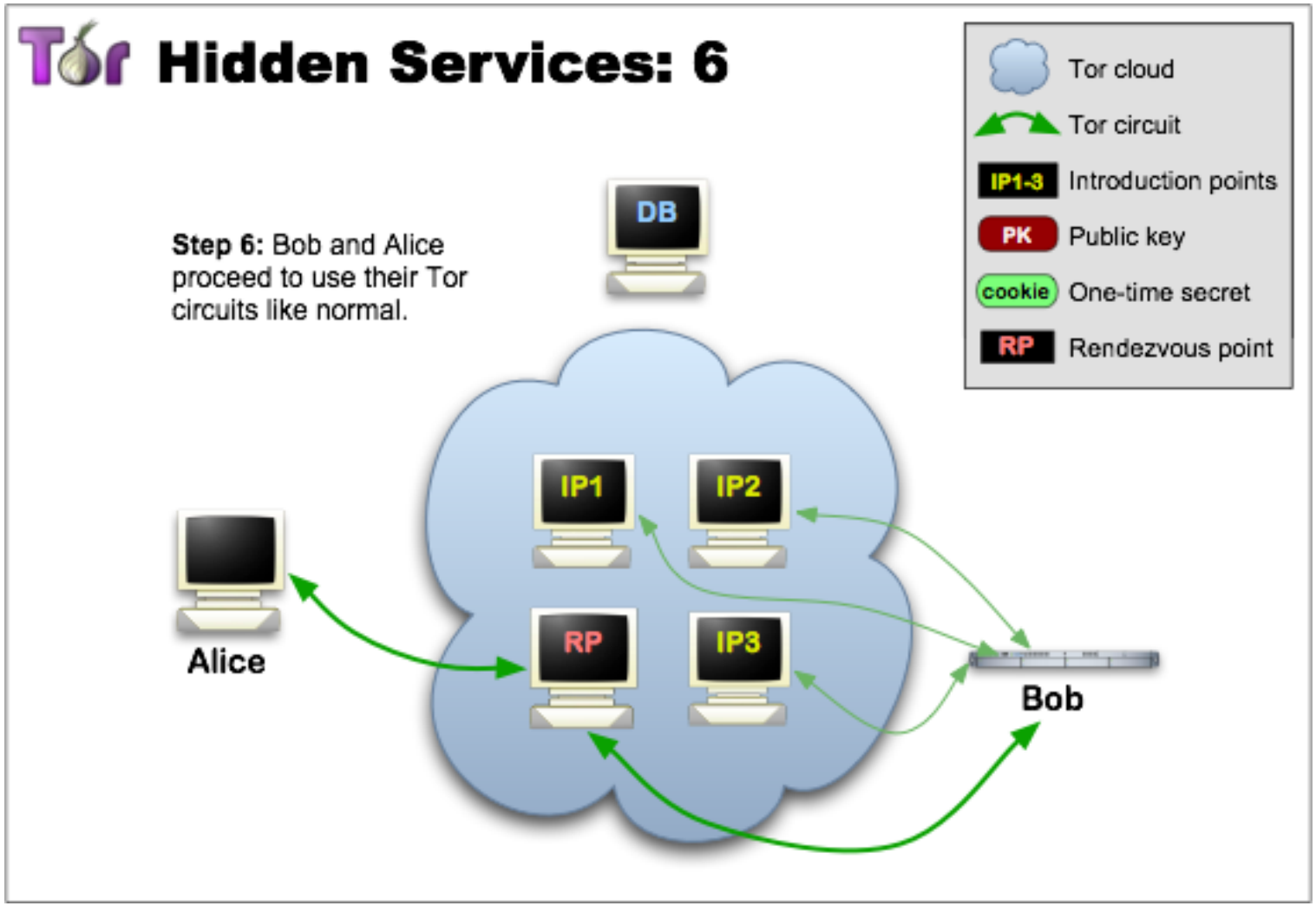
Tor Hidden Services



Tor Hidden Services



Tor Hidden Services



SilkRoad Marketplace

Silk Road
anonymous marketplace

Welcome **now0open**!
messages(0) | **orders(0)** | **account(฿0)** | **settings** | **log out**

search | (0)

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

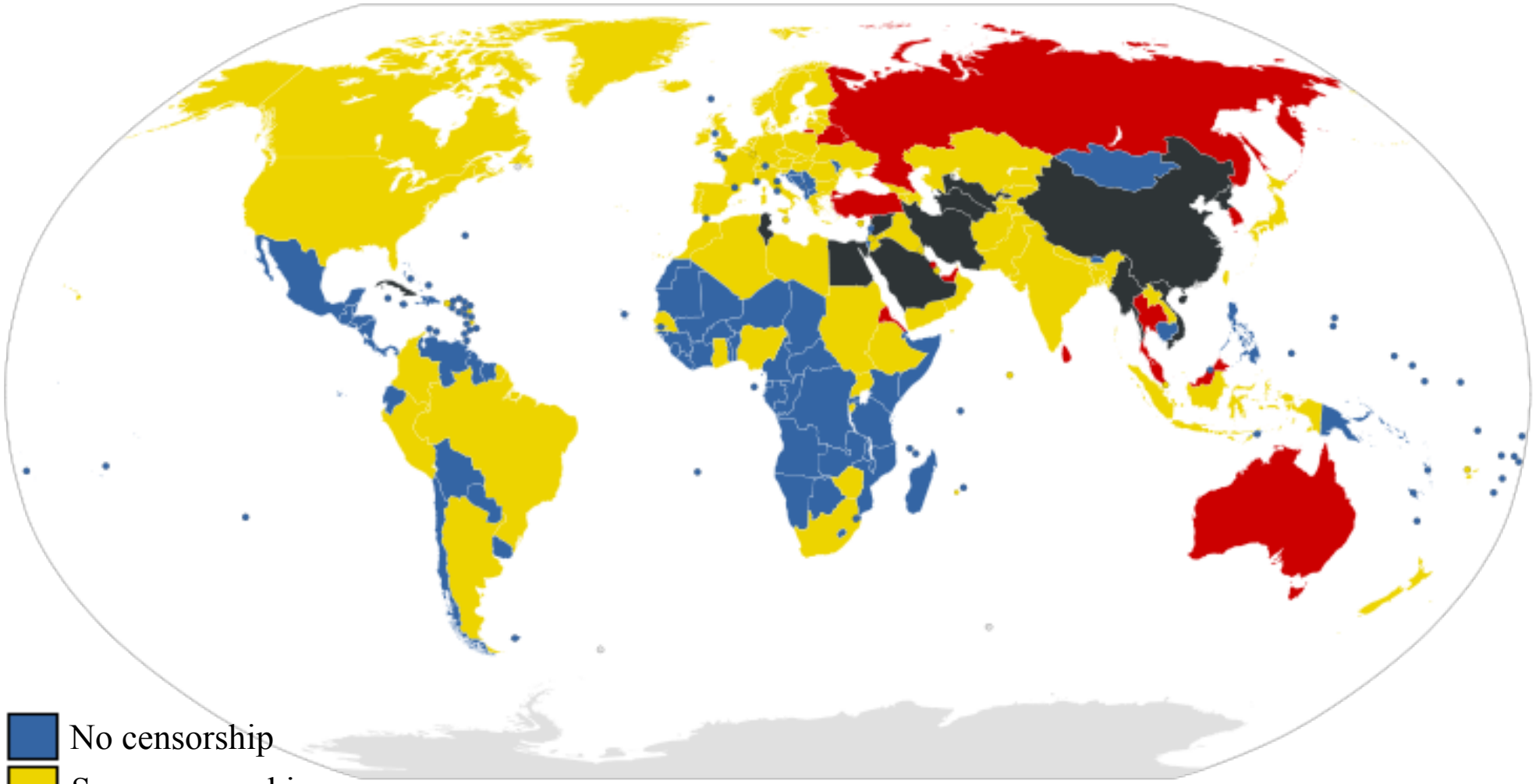
How to get Tor

- 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

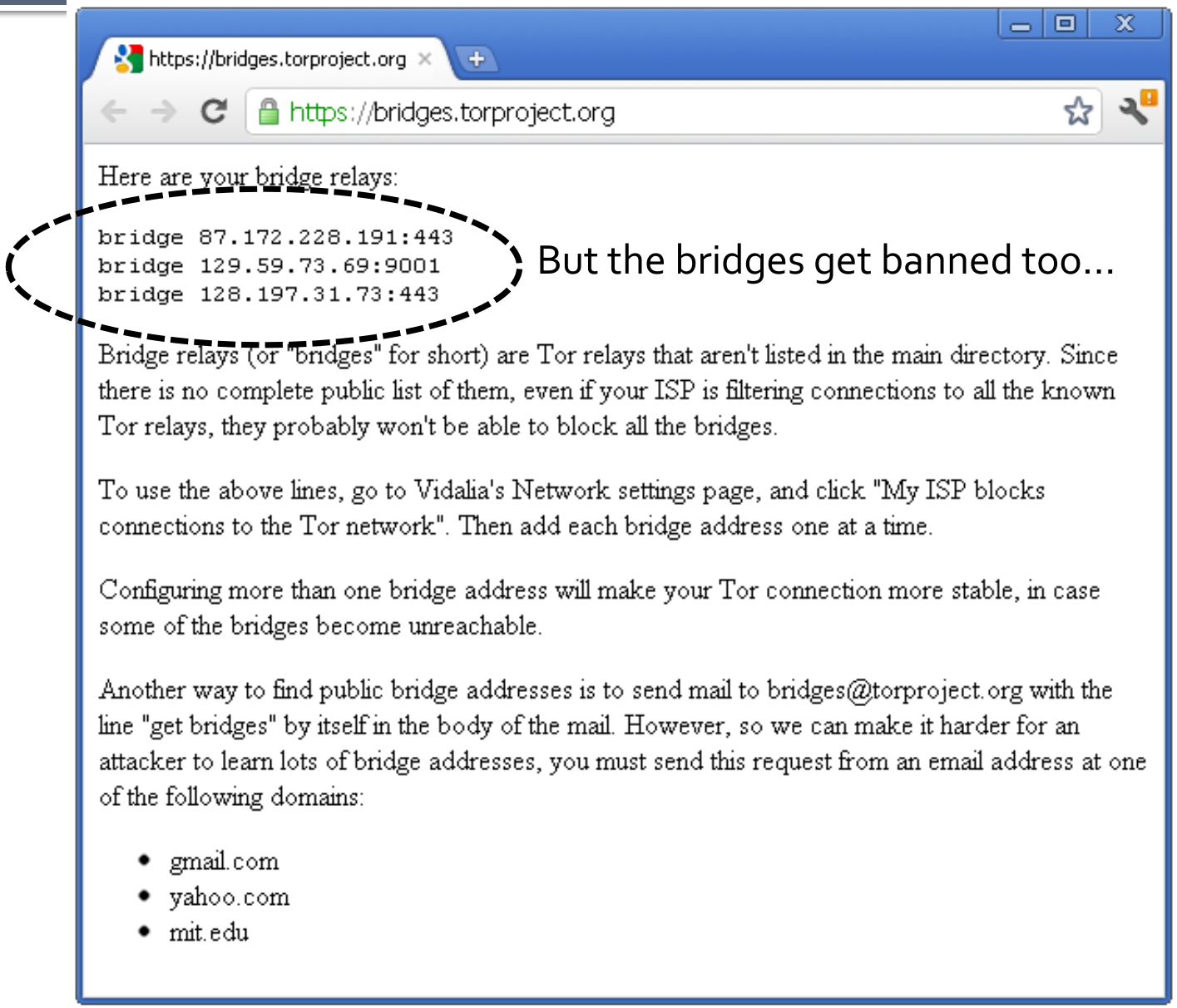
IP blocking, DNS blackholes, forged RST packets

Popular countermeasures

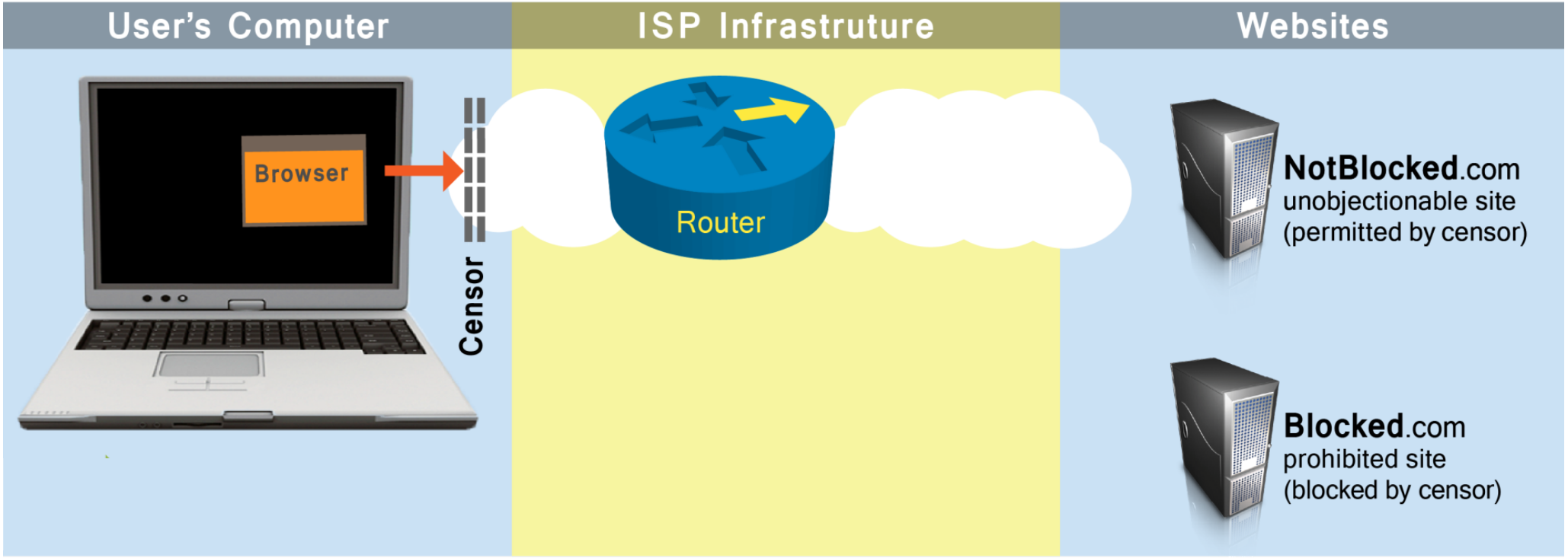
Mostly proxy based — Tor, Freenet, Ultrasurf, …

Problem: Cat-and-mouse game

Censorship Resistance: Tor Bridges



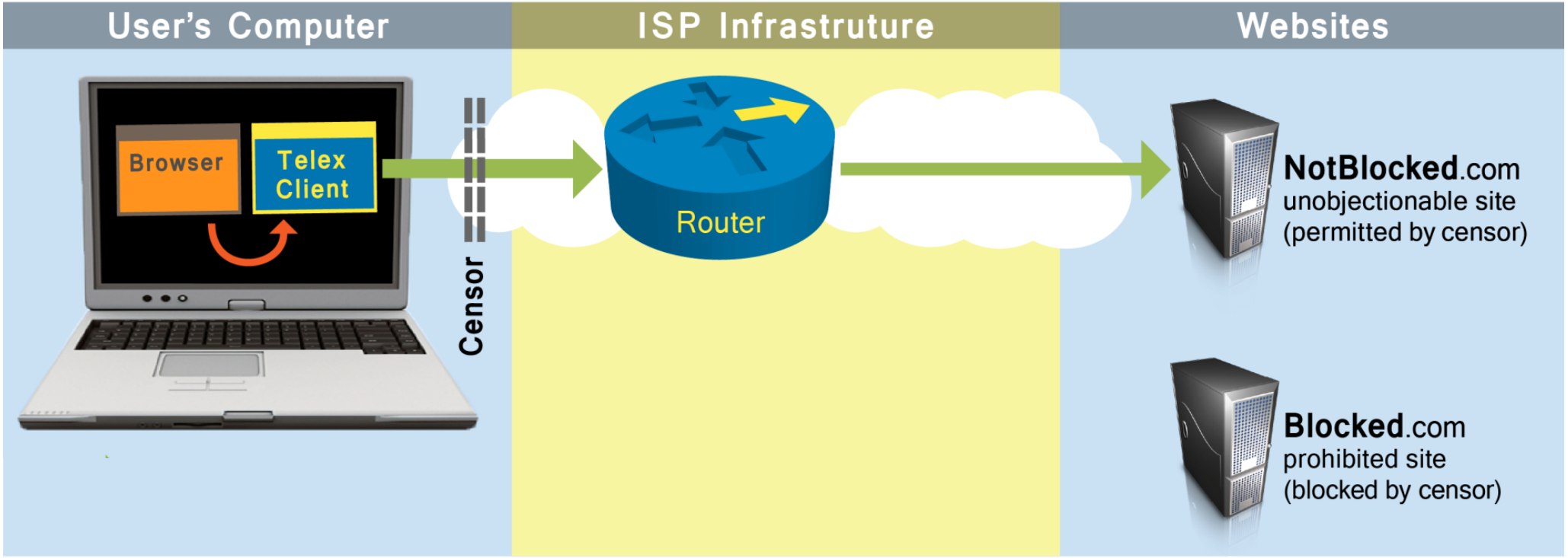
New Approach: Telex



Request for **permitted** site

Request for **prohibited** site

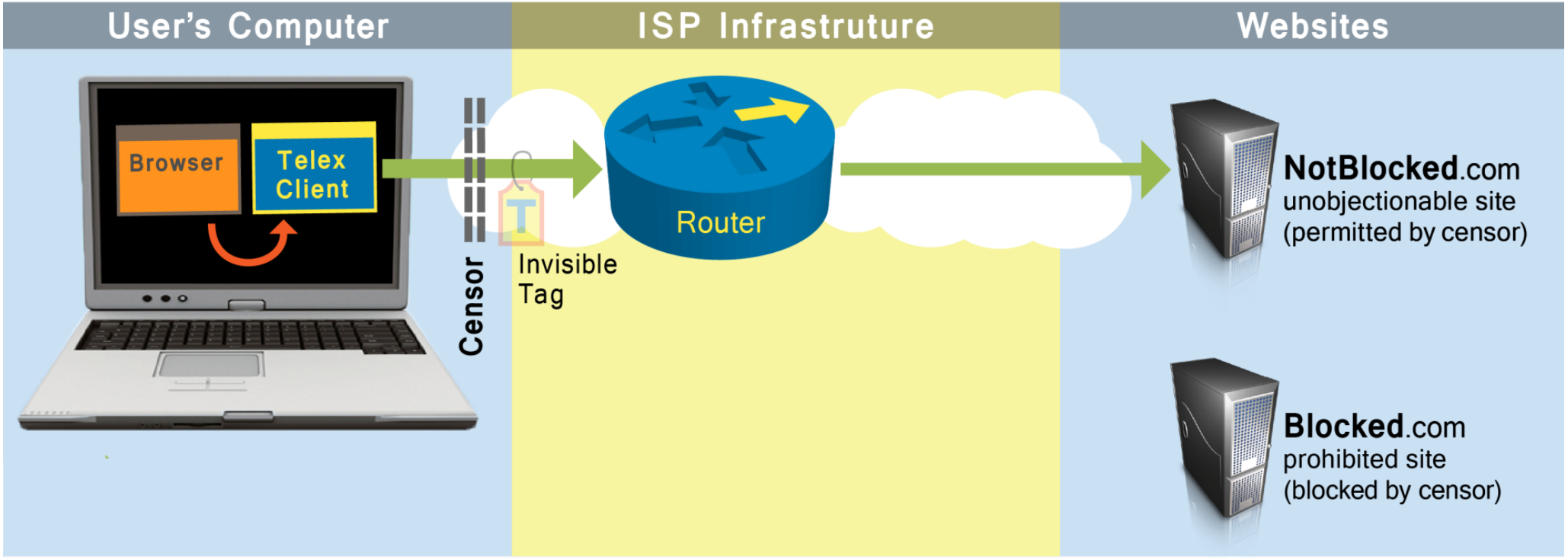
New Approach: Telex



Request for **permitted** site

Request for **prohibited** site

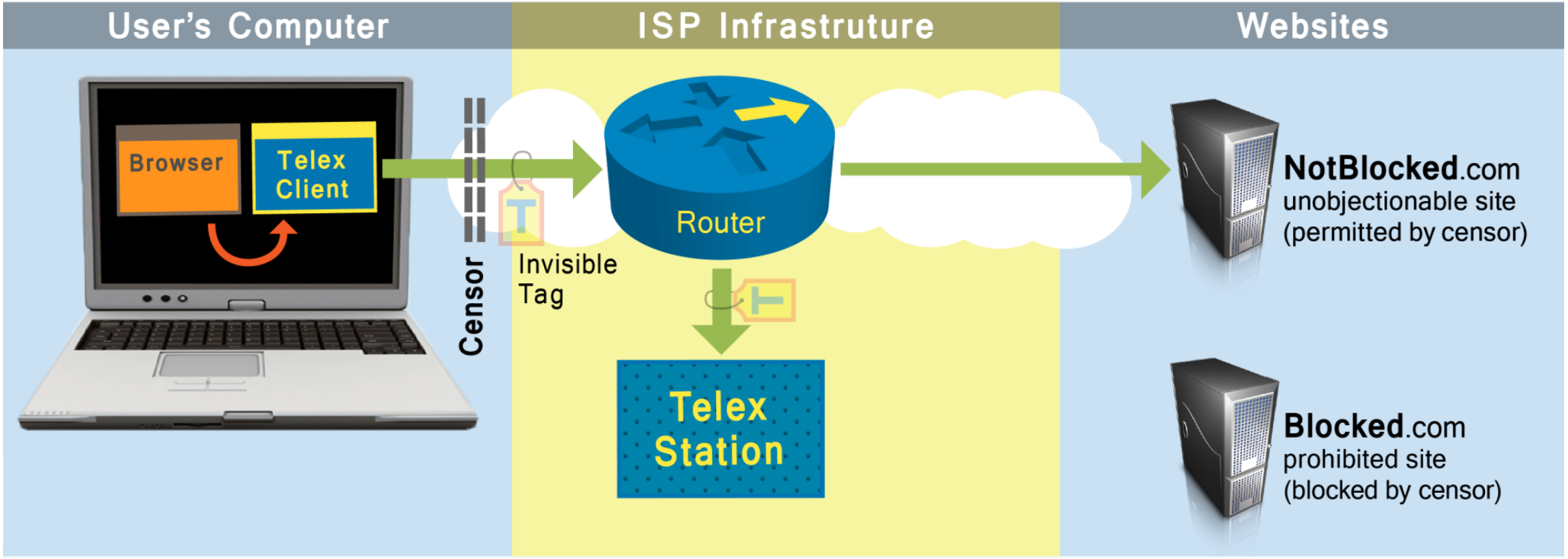
New Approach: Telex



Request for **permitted** site

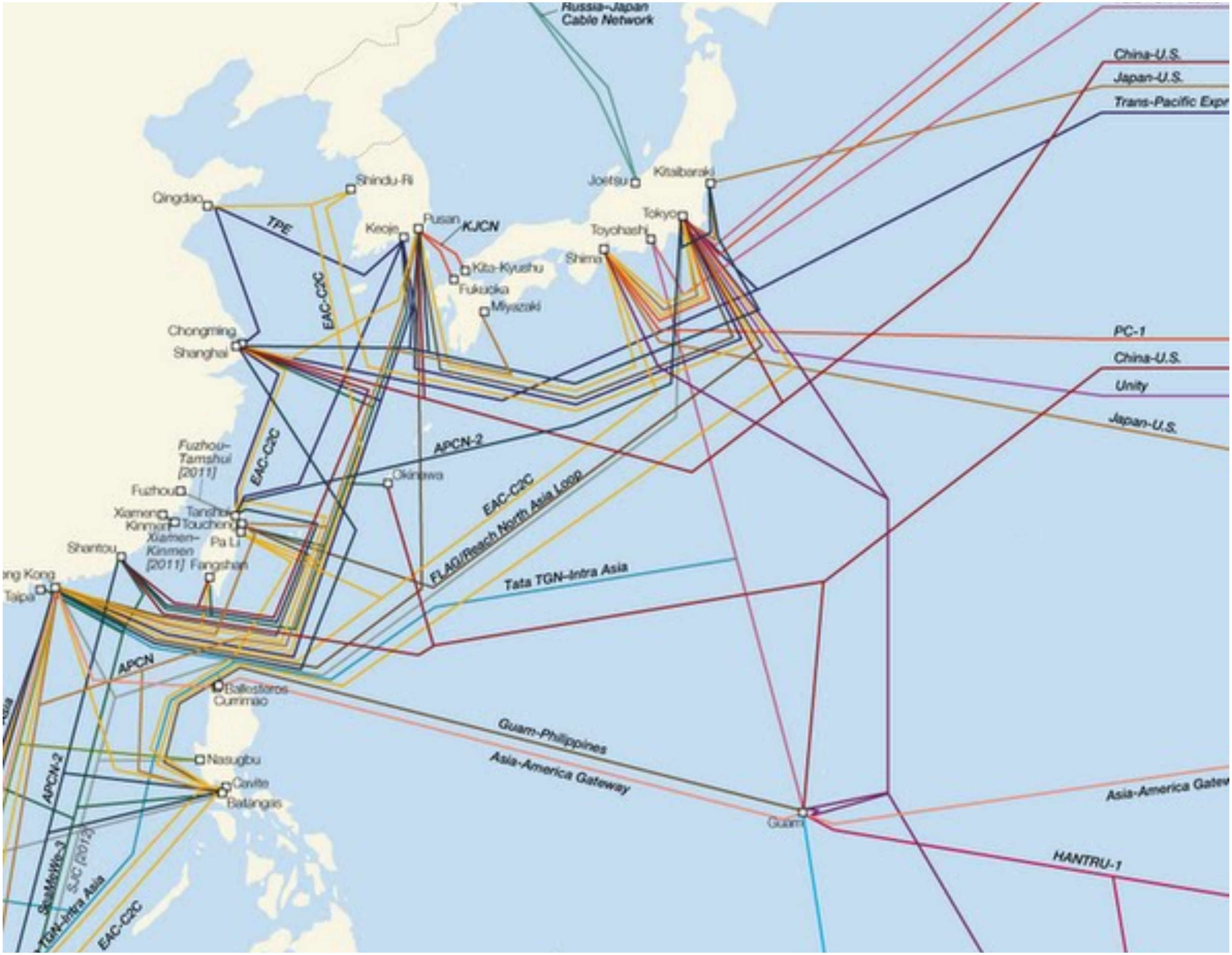
Request for **prohibited** site

New Approach: Telex

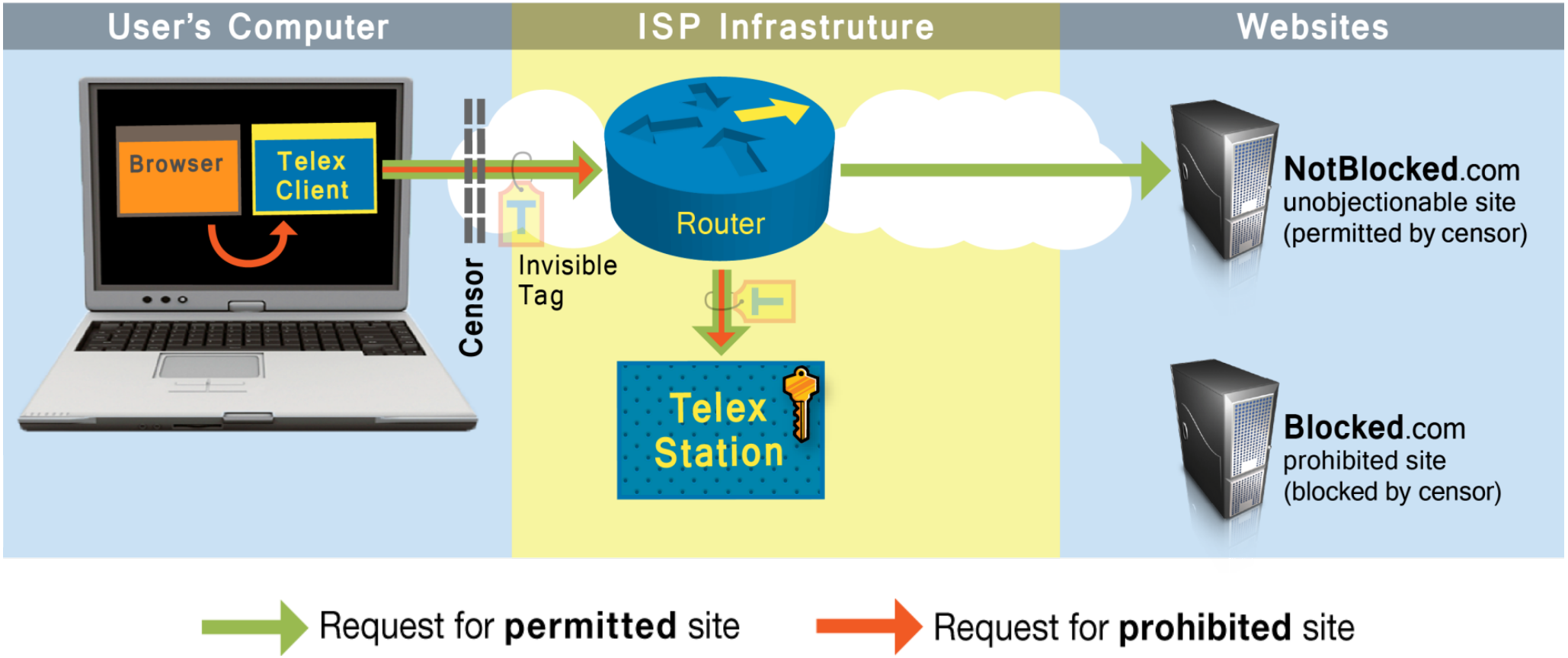


Request for **permitted** site

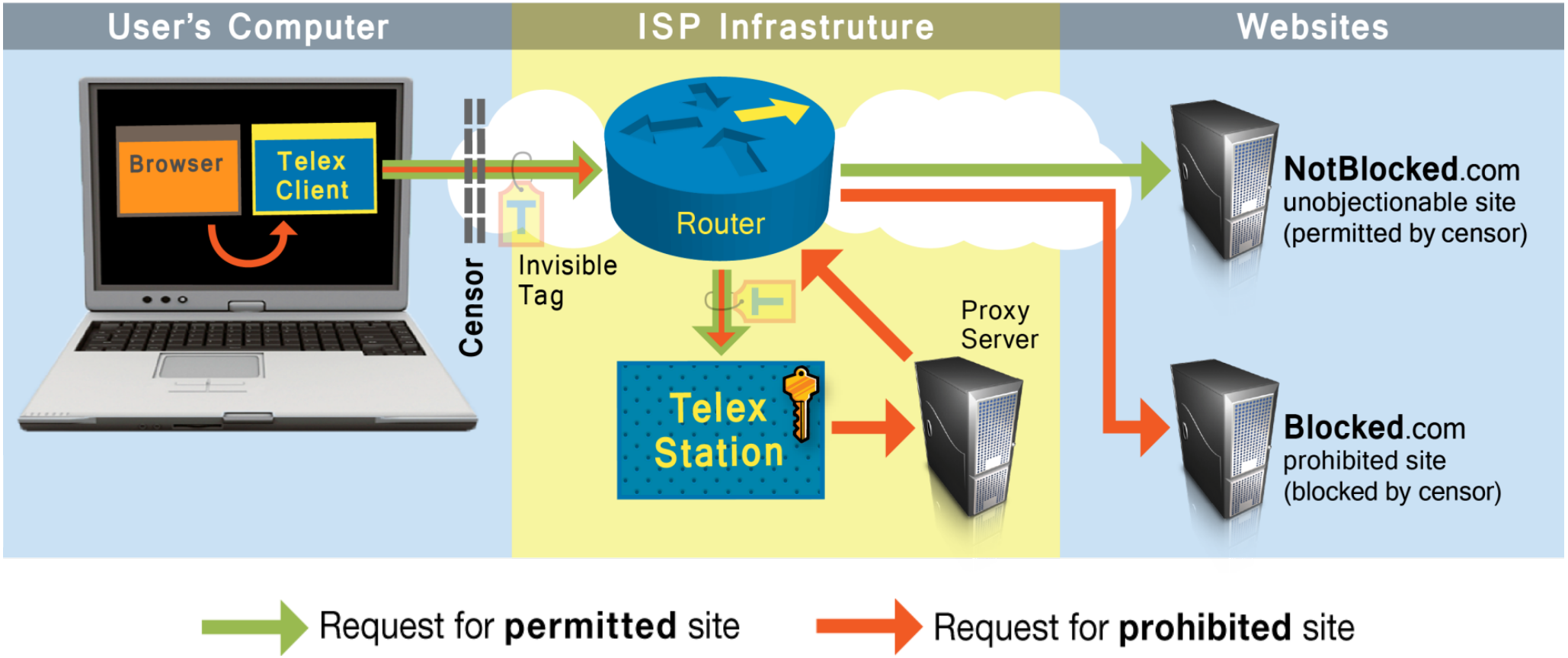
Request for **prohibited** site


Russia-Japan Cable Network
China-U.S.
Japan-U.S.
Trans-Pacific Expr
Shindu-Ri
Qingdao
TPE
Keoje
Pusan
KJCN
Joetsu
Kitaibaraki
Tokyo
Toyohashi
Shima
Kita-Kyushu
Fukuoka
Miyazaki
EAC-C2C
Chongming
Shanghai
PC-1
China-U.S.
Unity
Japan-U.S.
APCN-2
Fuzhou-Tamshui [2011]
EAC-C2C
Okinawa
Fuzhou
Xiamen
Kinmen
Tanshui
Toucheng
Pa Li
Xiamen-Kinmen [2011]
Fangshan
Shantou
EAC-C2C
FLAG/Reach North Asia Loop
Tata TGN-Intra Asia
Taipa
APCN
Ballesteros
Currimao
Guam-Philippines
Asia-America Gateway
Nasugbu
Cavite
Batangas
APCN-2
SJC [2012]
EAC-C2C
Guam
HANTRU-1

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.

https://www.eff.org/deeplinks/2013/06/why-metadata-matters

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)