Firewalls. Policies. Privacy. Anonymity. Economics.

CMPSC 403 Fall 2021

November 30 - December 2, 2021

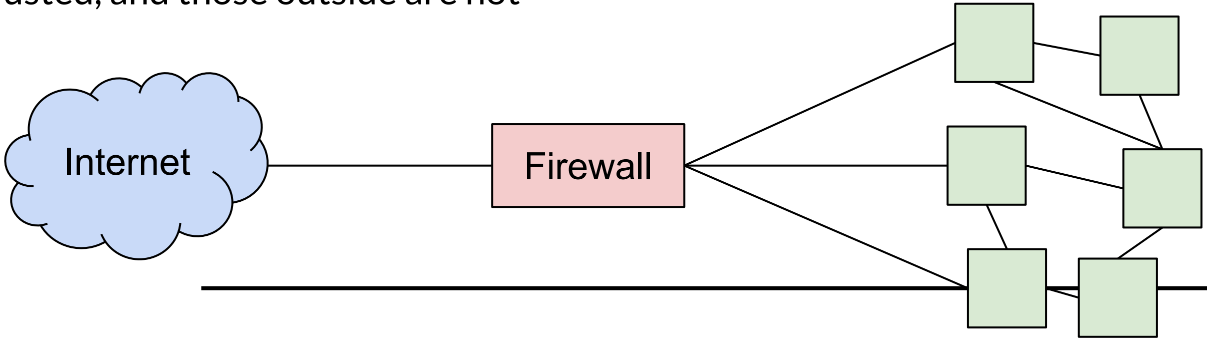
Firewalls

Motivation: Scalable Defenses

- How do you protect a set of systems against external attack?
  - Example: A company network with many servers and employee computers
- Observation: More network services = more risk
  - Each network connection creates more opportunities for attacks (greater attack surface)
  - Turning off all network services is often infeasible (print services, SSH services, etc.)
- Observation: More networked machines = more risk
  - What if you have to secure hundreds of systems?
  - What if the systems have different hardware, operating systems, and users?
  - What if there are some systems in the network that you aren’t aware of?
- Instead of securing individual machines, we want to secure the entire network!

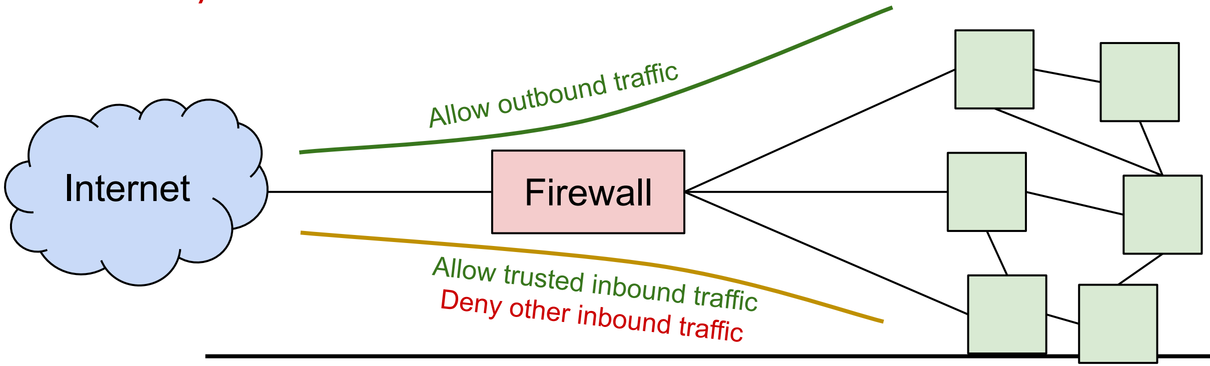
Firewalls and Security Policies

- Idea: Add a single point of access in and out of the network, with a monitor
  - "Ensure complete mediation"
  - Any traffic that could affect vulnerable systems must pass through the firewall
- Network access is controlled by a **policy**
  - Defines what traffic is allowed to exit the network (**outbound policy**)
  - Defines what traffic is allowed to enter the network (**inbound policy**)
  - Policy model based on our threat model: We usually assume users "inside" the network are trusted, and those outside are not



Firewalls and Security Policies

- What’s the policy of a standard home network?
  - Outbound policy: Allow outbound traffic
    - Users inside the network can connect to any service
  - Inbound policy: Only some traffic is able to enter the network
    - Allow inbound traffic in response an outbound connection
    - Allow inbound traffic to certain, trusted services (e.g. SSH), manually configured
    - Deny all other inbound traffic



Default Security Policies?

- How should we handle traffic that isn't explicitly allowed or denied?
    - **Default-allow policy**: Allow all traffic, but deny those on a specified **denylist**
        - As problems arise, add them to the denylist
    - **Default-deny policy**: Deny all traffic, but allow those on a specified **allowlist**
        - As needs arise (or users *complain*), add them to the allowlist?
        - Aside: user complaints are useful. Pay attention to them and try to make it so they don't complain, or if you can't fix the complaint, explain ***why***.
- Which default policy is best?
    - Default-allow is more flexible, but flaws are vulnerabilities and can be catastrophic
    - Default-deny is more conservative, but flaws are less painful
    - **Default-deny is generally accepted to be the best default policy ("consider fail-safe defaults")**

Stateless Packet Filters

- Firewalls are often **packet filters**, which inspect network packets and chooses what to do with them
  - Option #1: Allow the packet to pass through the firewall, forwarding it onwards
  - Option #2: Deny the packet from passing through the firewall, dropping it
- Stateless packet filters
  - Packet filters that have no history
  - All decisions must be made using only the information in the packet itself
  - Can have trouble implementing complex policies that require knowledge of history

Stateful Packet Filters

- A better idea: Keep state in the implementation of the packet filter
  - The filter keeps track of inbound/outbound connections
    - Notice: All connections have packets going in both directions, so a stateless filter could not do this
  - Rules define what connections are allowed or denied
  - Ultimately, packets are still either forwarded or dropped
- Example rules:
  - **`allow tcp connection 4.5.5.4:* -> 3.1.1.2:80`**
    - Allow connections from **`4.5.5.4`** to **`3.1.1.2`** with destination port 80
  - **`allow tcp connection *:*/int -> *:80/ext`**
    - Allow outbound connections with destination port 80
  - **`allow tcp connection *:*/int -> *:*/ext`**
    - Allow all outbound connections
  - **`allow tcp connection *:*/ext -> 1.2.2.3:80`**
    - Allow inbound connections to **`1.2.2.3`** with destination port 80

Think Along: Other Types of Firewalls

Investigate other types of firewalls:

- Proxy firewalls
- Virtual/cloud firewalls
- Next-generation firewalls (NGFW)
- Threat-focused NGFWs

Activity 16:
https://github.com/CMPSC403-AlleghenyCollege-Fall2021/community_notes/blob/main/firewalls.md

Firewall Pros and Cons

- Pros
  - Centralized management of security policies (single point of control)
  - Transparent operation to end users
  - Mitigates security vulnerabilities on end hosts (e.g. block anything that looks like shellcode)
- Cons
  - Reduced network connectivity
    - Some applications don’t work well inside a firewall
  - Vulnerability to “insiders”
    - Employees could be bribed or threatened
    - Devices are often brought from into the network outside (e.g. cell phones, laptops)
    - Once one device is compromised, attackers can quickly spread through the network
    - Could be mitigated by layering firewalls for more sensitive devices

Alternatives to Allowing Firewall Traffic

- **Virtual private network** (**VPN**): A set of protocols that allows direct access to an internal network via an external connection
    - Creates an encrypted tunnel to allow internal network traffic to be sent securely over the Internet
    - Intuition: The encrypted tunnel is an emulated Ethernet cable that allows you to connect “inside” the network
    - The firewall allows VPN traffic, which allows arbitrary traffic to be tunneled inside

Privacy

What is Privacy?

- Privacy is control over your own information. Freedom from intrusion into personal matters

- Privacy is a person's right or expectation to control the disclosure of his/her personal information, including activity metadata

- Privacy is the "right to be let alone" — Louis Brandeis

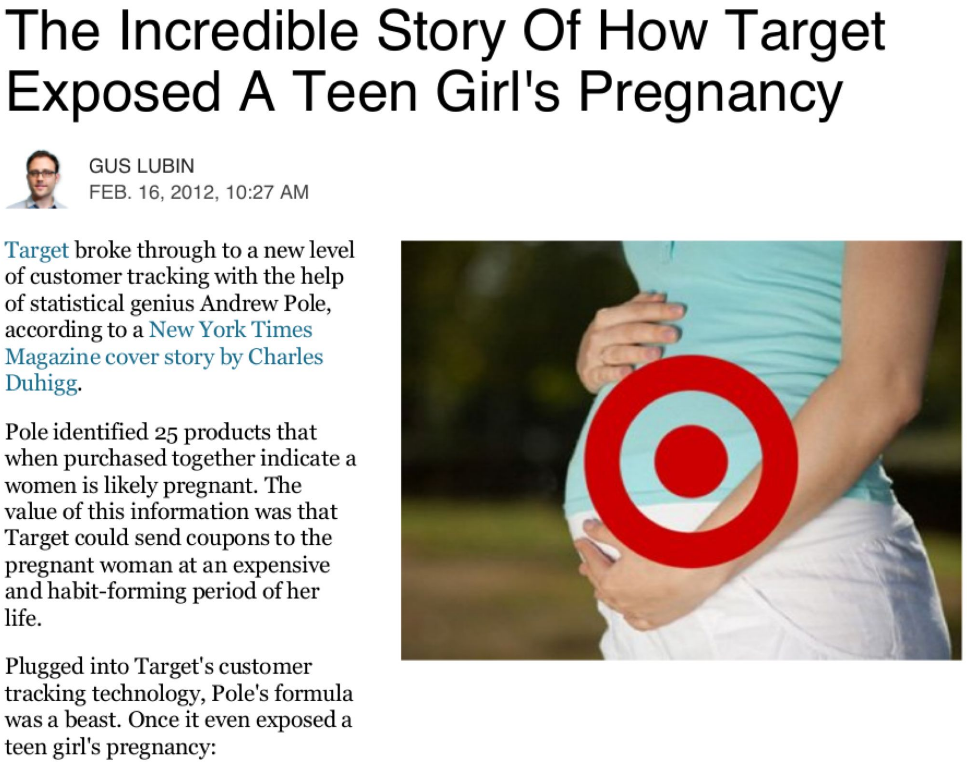
- Privacy means something like what the Founders meant by "liberty"
  Free speech, free association, autonomy, …
  freedom from censorship and constant surveillance

- Privacy-motivating examples in U.S. History
  - Martin Luther King Jr. "blackmailed" by FBI
  - McCarthyism witch-hunt for communists

Think Along!

- Give one example of :
    - **violation of privacy online**

Direct Sharing



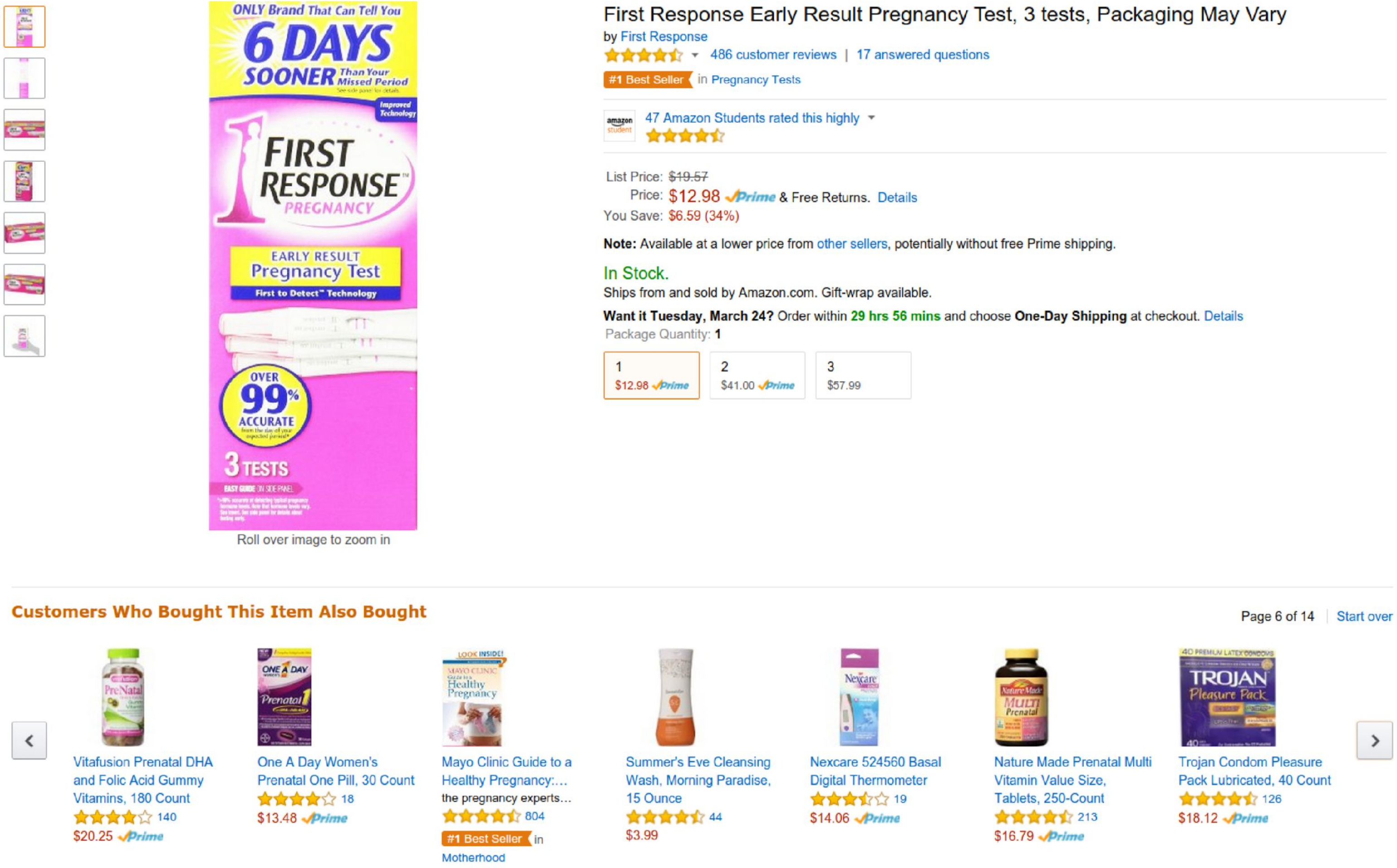
The Incredible Story Of How Target Exposed A Teen Girl's Pregnancy

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:


ONLY Brand That Can Tell You
6 DAYS SOONER Than Your Missed Period
Improved Technology
FIRST RESPONSE PREGNANCY
EARLY RESULT Pregnancy Test
First to Detect™ Technology
OVER 99% ACCURATE
3 TESTS
EASY GUIDE ON SIDE PANEL

Roll over image to zoom in

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

by First Response

★★★★☆ 486 customer reviews | 17 answered questions

#1 Best Seller in Pregnancy Tests

47 Amazon Students rated this highly

★★★★☆

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**

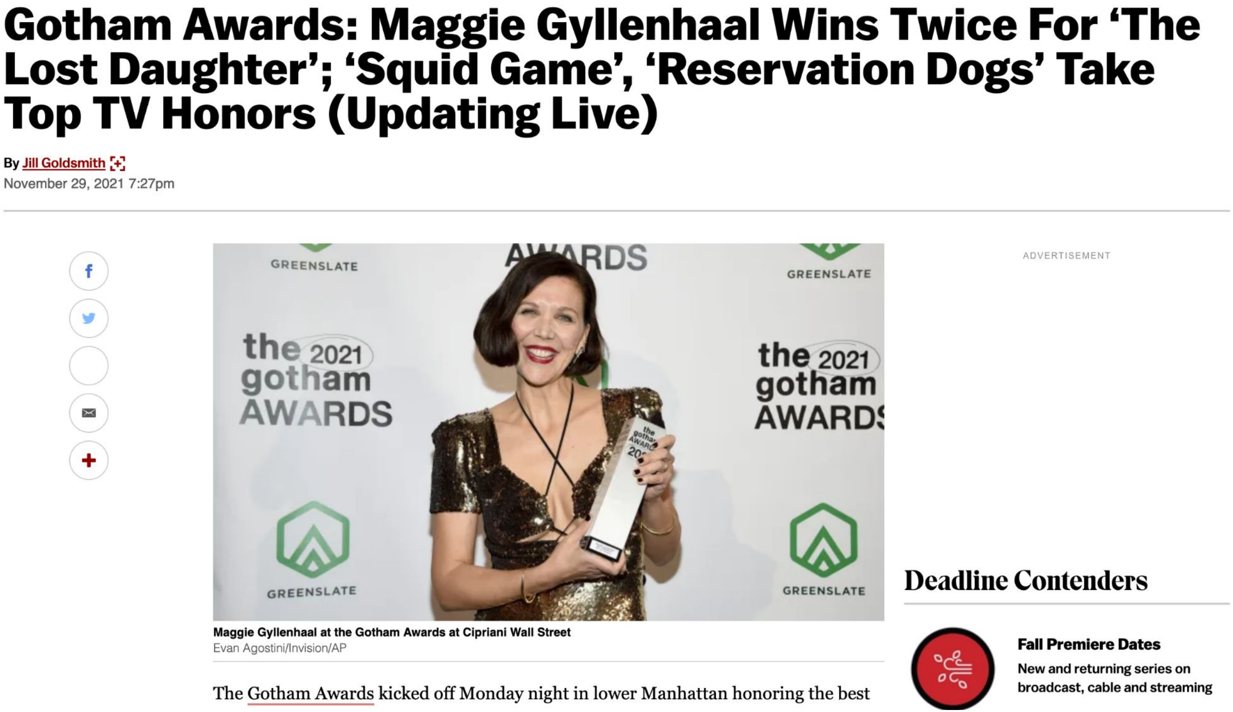
1	2	3
$12.98 ✓Prime	$41.00 ✓Prime	$57.99

Customers Who Bought This Item Also Bought

Page 6 of 14 | Start over

Vitafusion Prenatal DHA and Folic Acid Gummy Vitamins, 180 Count	One A Day Women's Prenatal One Pill, 30 Count	Mayo Clinic Guide to a Healthy Pregnancy:…	Summer's Eve Cleansing Wash, Morning Paradise, 15 Ounce	Nexcare 524560 Basal Digital Thermometer	Nature Made Prenatal Multi Vitamin Value Size, Tablets, 250-Count	Trojan Condom Pleasure Pack Lubricated, 40 Count
★★★★☆ 140	★★★★☆ 18	the pregnancy experts…	★★★★☆ 44	★★★☆☆ 19	★★★★☆ 213	★★★★☆ 126
$20.25 ✓Prime	$13.48 ✓Prime	★★★★☆ 804	$3.99	$14.06 ✓Prime	$16.79 ✓Prime	$18.12 ✓Prime
		#1 Best Seller in Motherhood				

Third Party Tracking



Gotham Awards: Maggie Gyllenhaal Wins Twice For 'The Lost Daughter'; 'Squid Game', 'Reservation Dogs' Take Top TV Honors (Updating Live)

By Jill Goldsmith

November 29, 2021 7:27pm

Maggie Gyllenhaal at the Gotham Awards at Cipriani Wall Street

Evan Agostini/Invision/AP

The Gotham Awards kicked off Monday night in lower Manhattan honoring the best

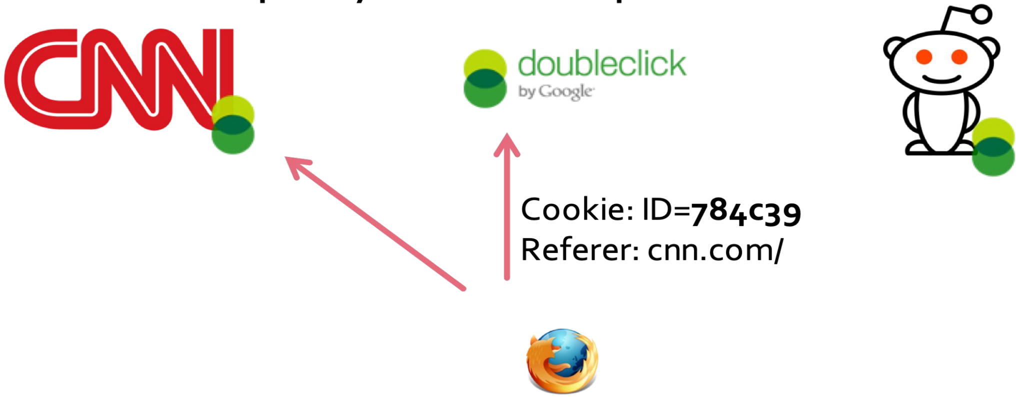
Deadline Contenders

Fall Premiere Dates

New and returning series on broadcast, cable and streaming

Third Party Cookies

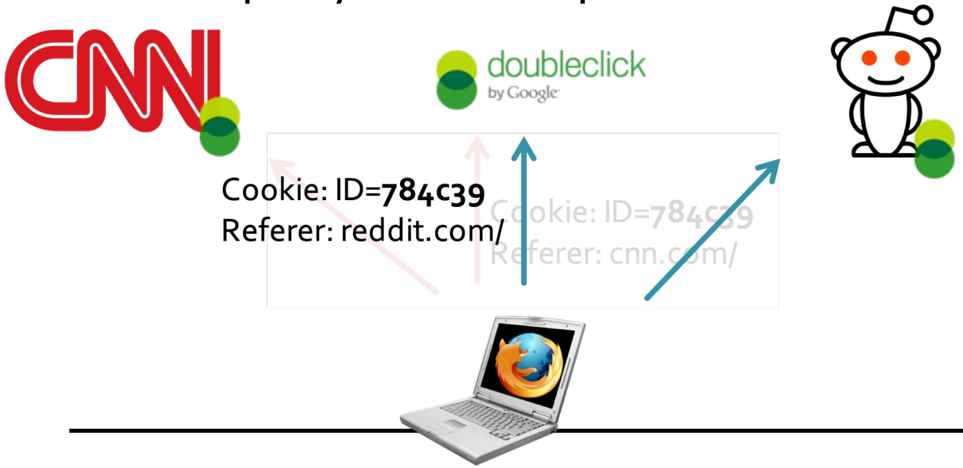
- Site A’s page requests a third-party resource (image, script, iframe)
  - Normally, browser sends cookie associated with that third-party in that request



Cookie: ID=**784c39**
Referer: 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

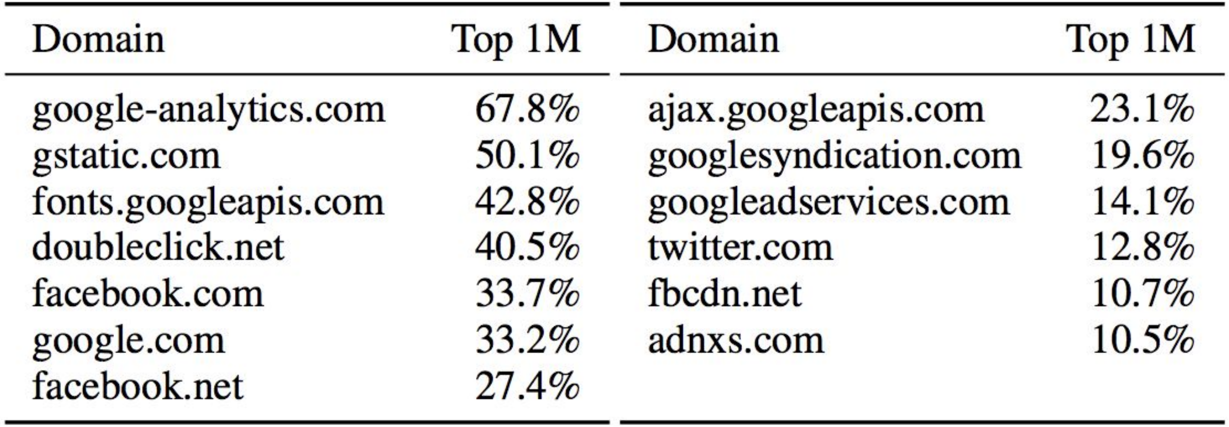


Cookie: ID=**784c39**
Referer: reddit.com/

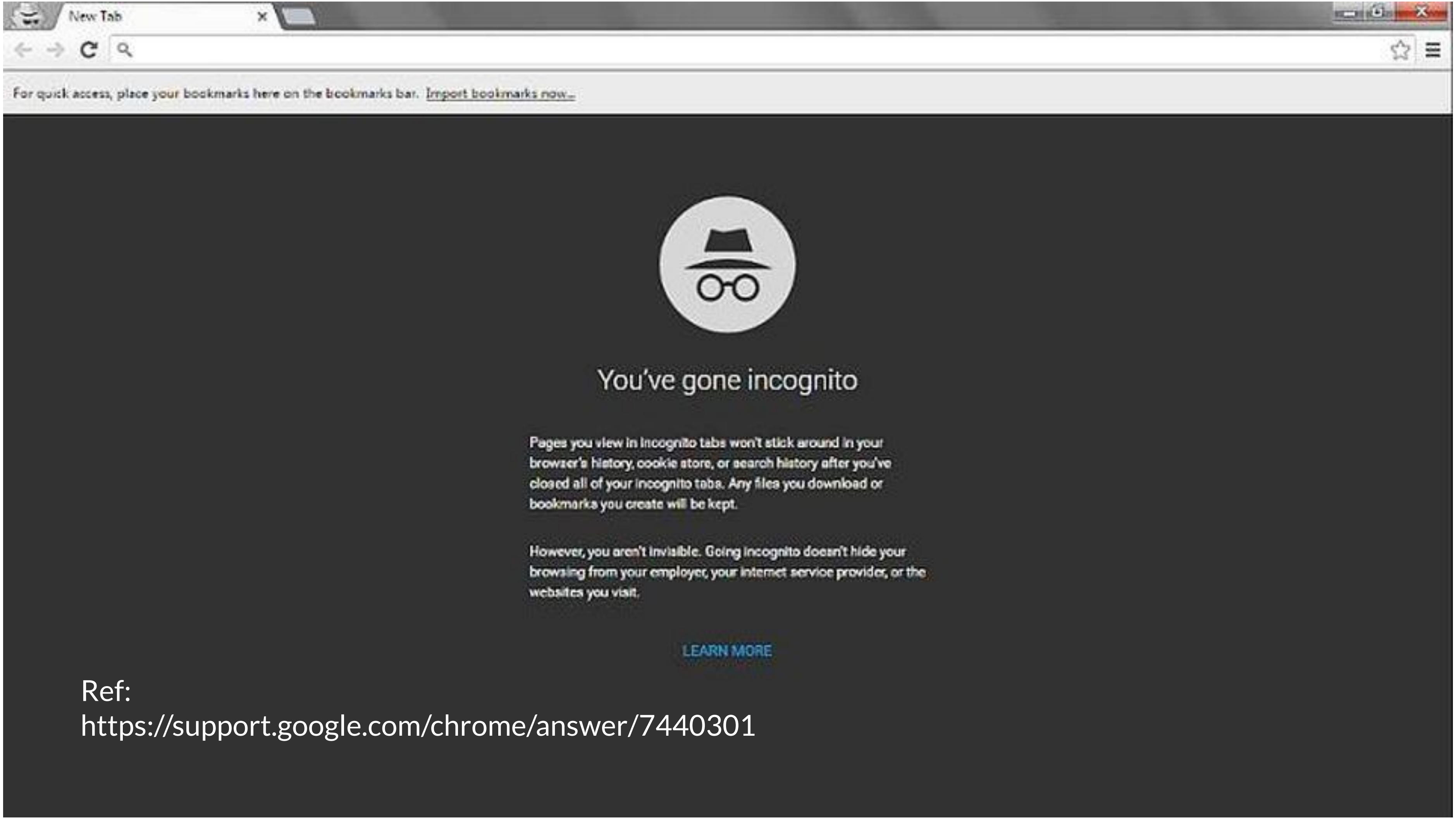
Cookie: ID=**784c39**
Referer: cnn.com/

Third Party Cookies

Facebook, DoubleClick, etc. know much more about you than actual website does because they can track you across websites.



Domain	Top 1M	Domain	Top 1M
google-analytics.com	67.8%	ajax.googleapis.com	23.1%
gstatic.com	50.1%	googlesyndication.com	19.6%
fonts.googleapis.com	42.8%	googleadservices.com	14.1%
doubleclick.net	40.5%	twitter.com	12.8%
facebook.com	33.7%	fbcdn.net	10.7%
google.com	33.2%	adnxs.com	10.5%
facebook.net	27.4%		



For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

You've gone incognito

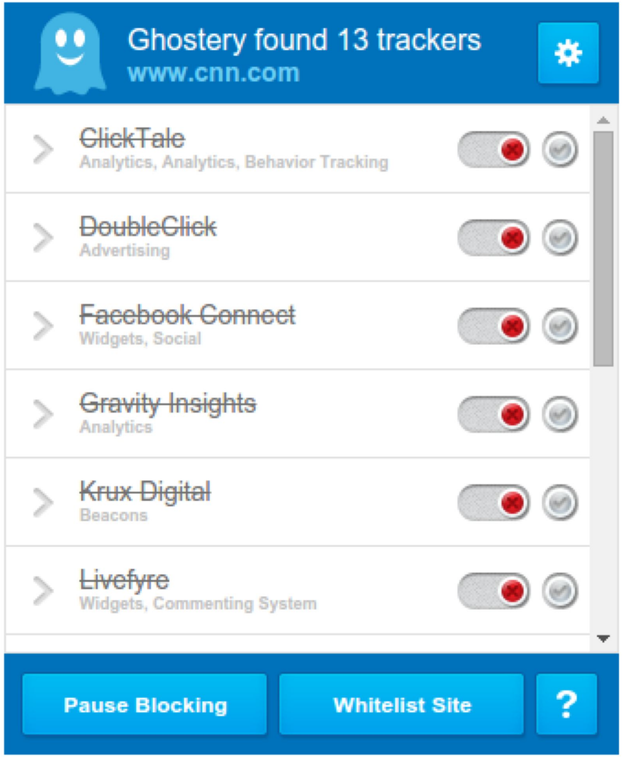
Pages you view in incognito tabs won't stick around in your browser's history, cookie store, or search history after you've closed all of your incognito tabs. Any files you download or bookmarks you create will be kept.

However, you aren't invisible. Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit.

Ref:
https://support.google.com/chrome/answer/7440301

Ghostery

https://www.ghostery.com/



Ghostery found 13 trackers
www.cnn.com

~~ClickTale~~
Analytics, Analytics, Behavior Tracking

~~DoubleClick~~
Advertising

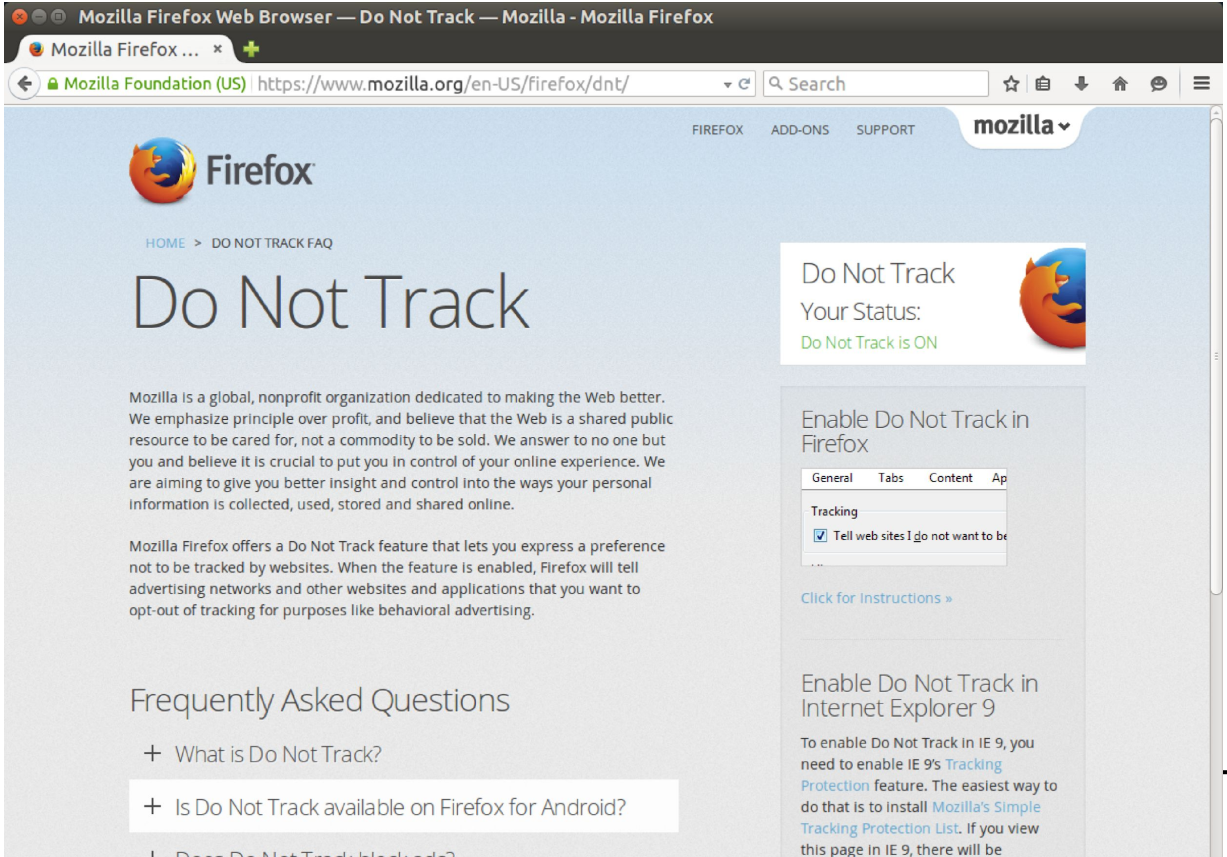
~~Facebook Connect~~
Widgets, Social

~~Gravity Insights~~
Analytics

~~Krux Digital~~
Beacons

~~Livefyre~~
Widgets, Commenting System

DNT



Do Not Track

Mozilla is a global, nonprofit organization dedicated to making the Web better. We emphasize principle over profit, and believe that the Web is a shared public resource to be cared for, not a commodity to be sold. We answer to no one but you and believe it is crucial to put you in control of your online experience. We are aiming to give you better insight and control into the ways your personal information is collected, used, stored and shared online.

Mozilla Firefox offers a Do Not Track feature that lets you express a preference not to be tracked by websites. When the feature is enabled, Firefox will tell advertising networks and other websites and applications that you want to opt-out of tracking for purposes like behavioral advertising.

Frequently Asked Questions

+ What is Do Not Track?

+ Is Do Not Track available on Firefox for Android?

Do Not Track

Your Status:

Do Not Track is ON

Enable Do Not Track in Firefox

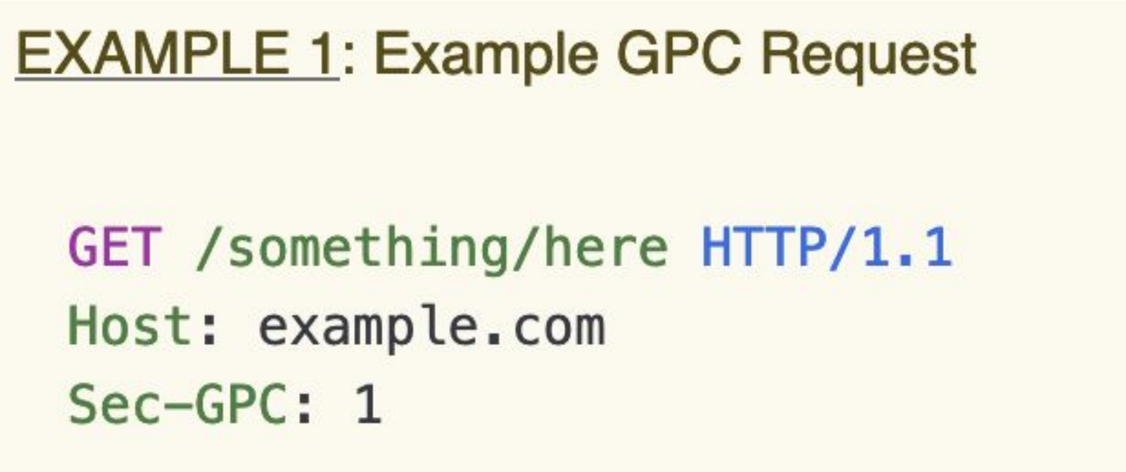
☑ Tell web sites I do not want to be

Click for Instructions »

Enable Do Not Track in Internet Explorer 9

To enable Do Not Track in IE 9, you need to enable IE 9's Tracking Protection feature. The easiest way to do that is to install Mozilla's Simple Tracking Protection List. If you view this page in IE 9, there will be

Global Privacy Control (GPC)



EXAMPLE 1: Example GPC Request

```
GET /something/here HTTP/1.1
Host: example.com
Sec-GPC: 1
```

https://globalprivacycontrol.github.io/gpc-spec/
https://globalprivacycontrol.org/

Chrome Third Party Cookies

March 2021 — Google began to block third-party cookies in Chrome

Suggesting alternative — "**FLoC**" — Federated Learning of Cohorts

- Idea: Let advertisers track semi-anonymous groups of thousands of people
- Large number of “cohorts,” groups of people that share interests
    - SimHash of domains visited in the last week
- Each flock is assigned an ID — up to advertiser to make sense of what the ID

Think Along!

- Give one example of :
    - **Benefit of FLoC**
    - **Downside of FLoC**

Privacy Enhancing Technologies

Methods for protecting personal data

Most Common/Successful? TLS.

TLS is **a cryptographic protocol designed to provide end-to-end security of data sent between applications over the network**.

- Comes with browser. Also used for protecting email. It just works, without you having to configure anything. Protects *contents* of communication from passive eavesdroppers and active MITM attacks.

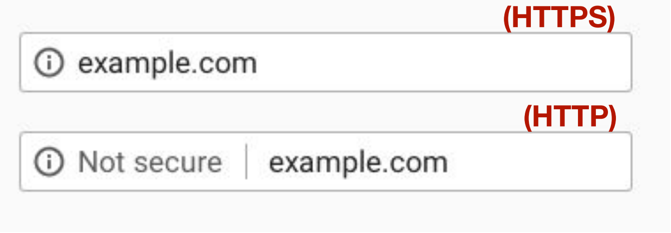
- Tools that provide confidentiality also provide some privacy. You probably don't want your landlord or coffee shop customers to learn things about you.

Encouraging HTTPS Adoption

2014: HTTPS used as a page rank indicator

Early 2018: Mozilla announces that new features will require HTTPS

Late 2018: New Chrome HTTPS indicators



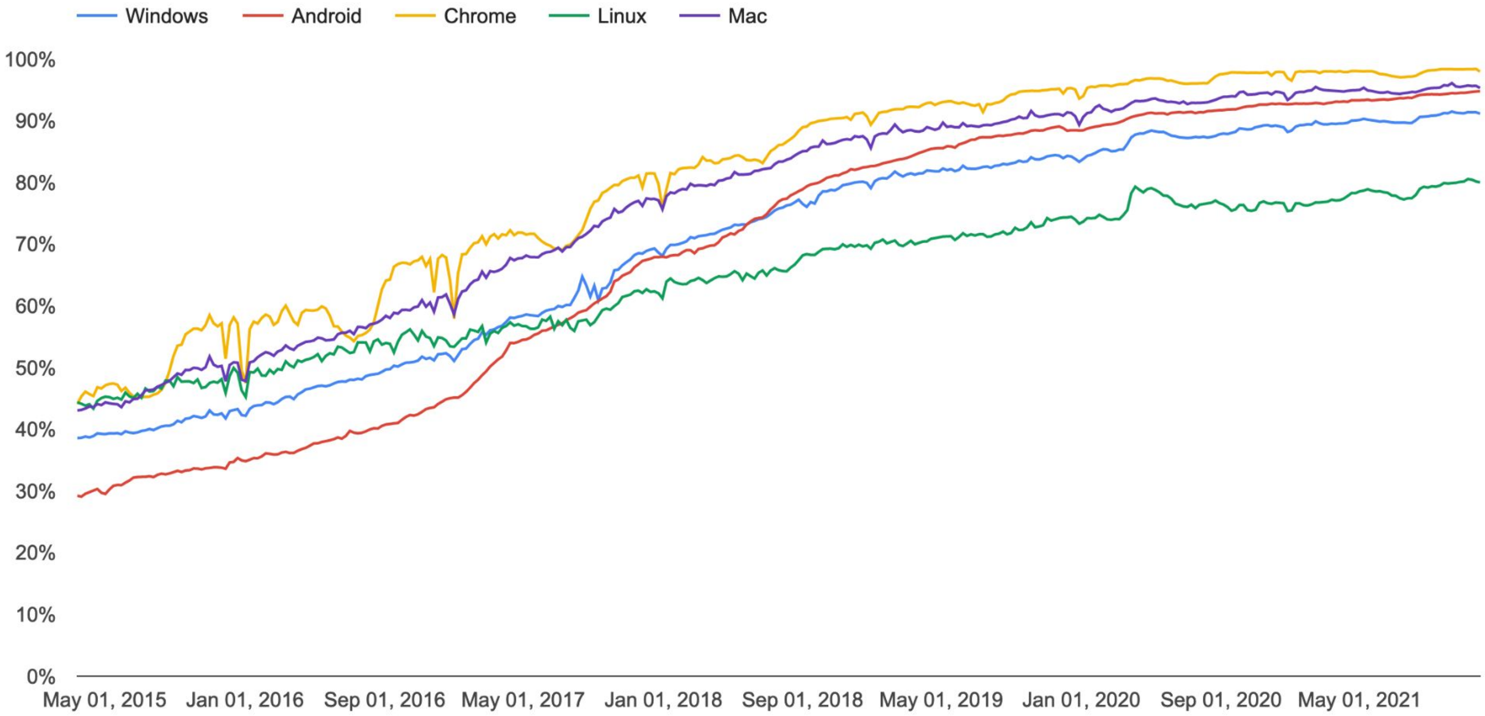
(HTTPS)

ⓘ example.com

(HTTP)

ⓘ Not secure | example.com

Chrome Page Loads over HTTPS



Google Transparency Report https://transparencyreport.google.com/?hl=en

Protecting Metadata

TLS only protects content. What doesn't TLS protect against?

We may want to protect metadata:

- Who is visiting what websites? Who is sending messages to whom?
- Government might not like that you are visiting Human Rights Watch website
- Government might not be amused that you are sending messages to Human Rights Watch
- We may want to hide the existence of the message (maybe sending an encrypted message at all is going to cause you problems)

Anonymity

Anonymity

- **Anonymity**: Concealing your identity
  - Anonymous communication on the Internet: The identity of the source and/or destination are concealed
- Anonymity is not confidentiality
  - Confidentiality hides the contents of the communication
  - Anonymity hides the identities of who is communicating with whom

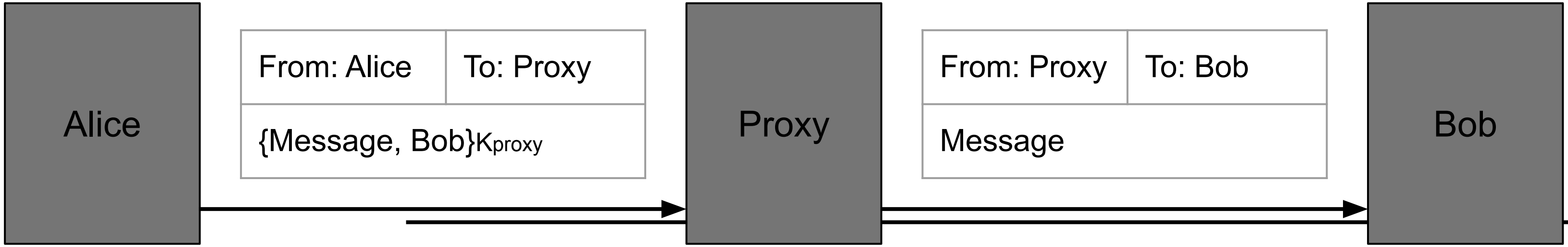
Anonymity on the Internet

- Anonymity on the Internet is hard
  - Difficult, if not impossible, to achieve on your own
  - Packets contain the source IP address and destination IP address
- Anonymity is easier for attackers
  - An attacker can hack into someone else’s computer and send communications from that computer
  - We assume honest users won’t hack into other computers
- **State of the art technique:** Ask someone else to send messages for you

Proxies and VPNs

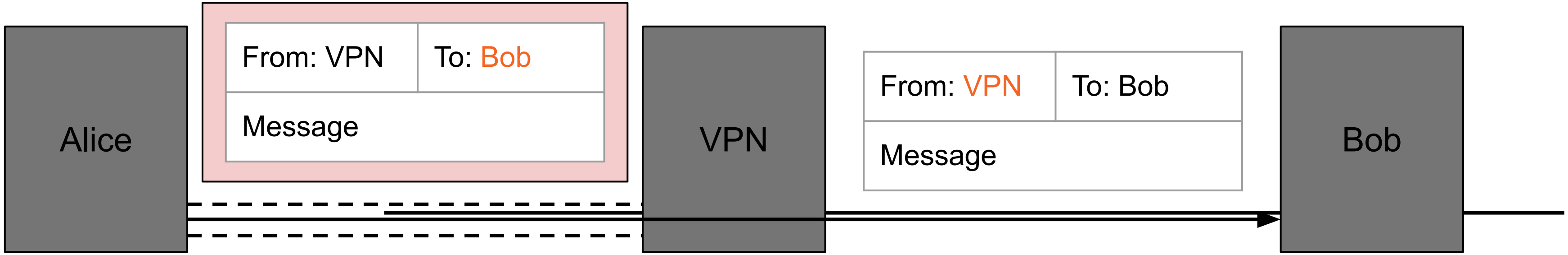
Proxies

- Alice wants to send a message to Bob
  - Bob shouldn't know the message is from Alice
  - An eavesdropper (Eve) cannot deduce that Alice is talking to Bob
- **Proxy**: A third party that relays our Internet traffic
  - Alice sends the message and the recipient (Bob) to the proxy, and the proxy forwards the message to Bob
    - The recipient's name (and optionally the message) is encrypted, so an eavesdropper does not see a packet with both Alice and Bob's identities in plaintext
  - Bob receives the message from the proxy, with no indication it came from Alice



Virtual Private Networks (VPNs)

- Recall VPNs: A virtual connection to an internal network
  - Allows access to an internal network through an encrypted tunnel
  - Creates an alternative use case: Appear as though you are coming from the virtually connected network instead of your real network!
    - Similar concept to proxies, but Alice directly sends packets as though coming from the VPN, wrapped in the VPN's layer of encryption
    - Proxies operate at the application layer, while VPNs operate at the network layer



Proxies and VPNs: Issues

- Performance
  - Sending a packet requires additional hops across the network
- Cost
  - VPNs can cost $80 to $200 per year
- Trusting the proxy
  - The proxy can see the sender and recipient’s identities
  - Attackers might convince the proxy to tell them about your identity

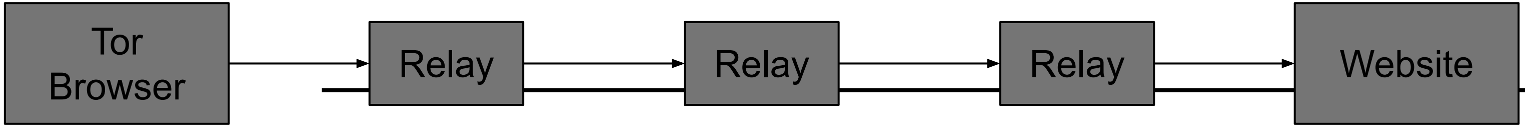
Real Use for VPNs

- Evading censorship
  - A local adversary can't see your traffic…
    - But the censor could just block VPN traffic instead
- Access control
  - Systems that only allow "internal" access or access from known networks…
  - The campus VPN is about solving this problem
- Separating idiots from their money
  - Commercial VPN services:
    Scare people into subscribing (and make it easy to do so)
    Make it almost impossible to cancel!

Tor

Tor

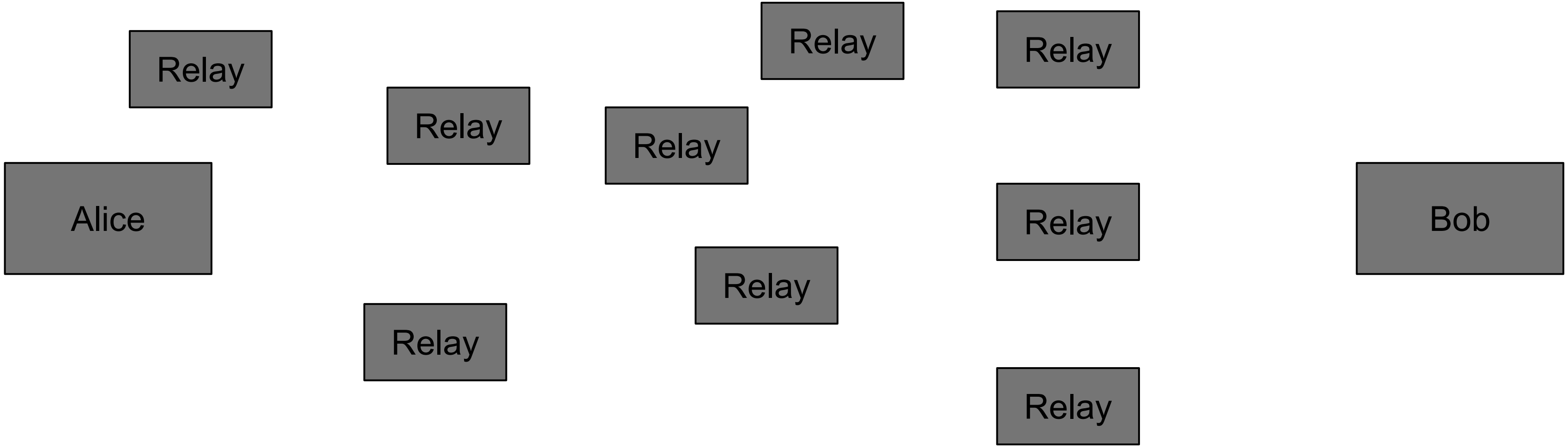
- Idea: Send the packet through multiple proxies instead of just one proxy
- **Tor**: A network that uses multiple proxies (relays) to enable anonymous communications
    - Stands for **T**he **O**nion **R**outer
- Components of Tor
    - Tor network: A network of many **Tor relays** (proxies) for forwarding packets
    - Directory server: Lists all Tor relays and their public keys
    - Tor Browser: A web browser configured to connect to the Tor network (based on Firefox)
    - Tor onion services: Servers that can only be reached through the Tor network
    - Tor bridges: Tor relays that try to hide the fact that a user is connecting to the Tor network



Tor Threat Model

- Security: Client anonymity and censorship resistance
  - Optional: Server anonymity with onion services
- Performance: Low(ish) latency (communication should be fast)
- Tor preserves anonymity against local adversaries
  - Example: An on-path attacker sees Alice send a message to a Tor relay, but not the final destination of the message
  - Example: The server should not know the identity of the client

Tor Circuits

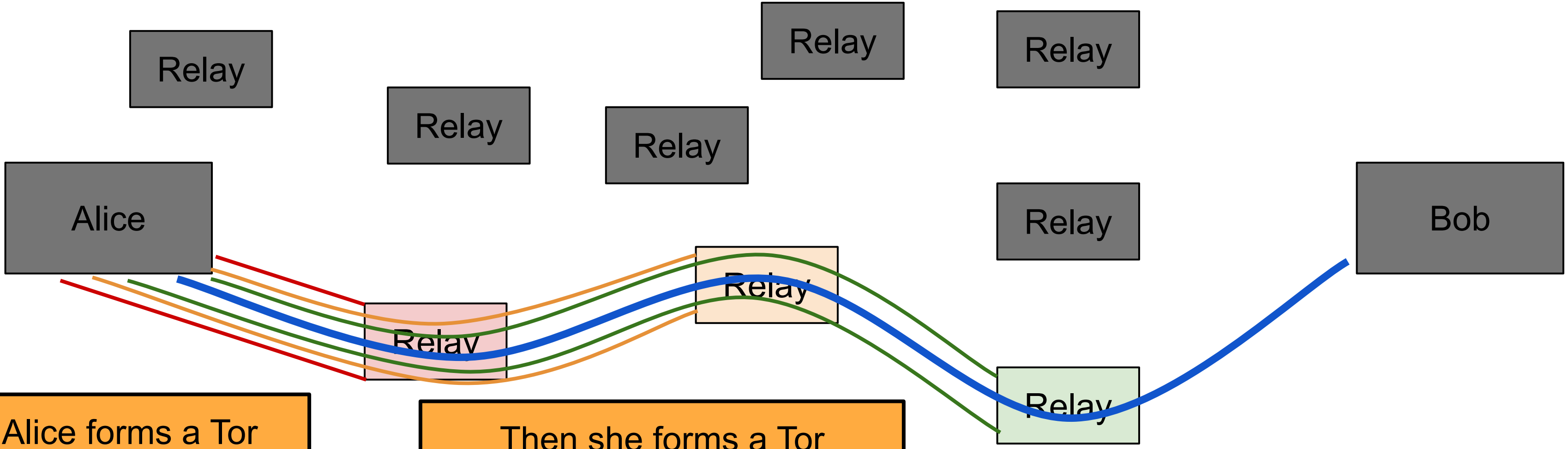


Suppose Alice wants to talk to Bob anonymously.

Alice queries the directory server and chooses 3 relays

Tor Circuits

TLS is **a cryptographic protocol designed to provide end-to-end security of data sent between applications over the network**.



Alice forms a Tor connection with the entry node

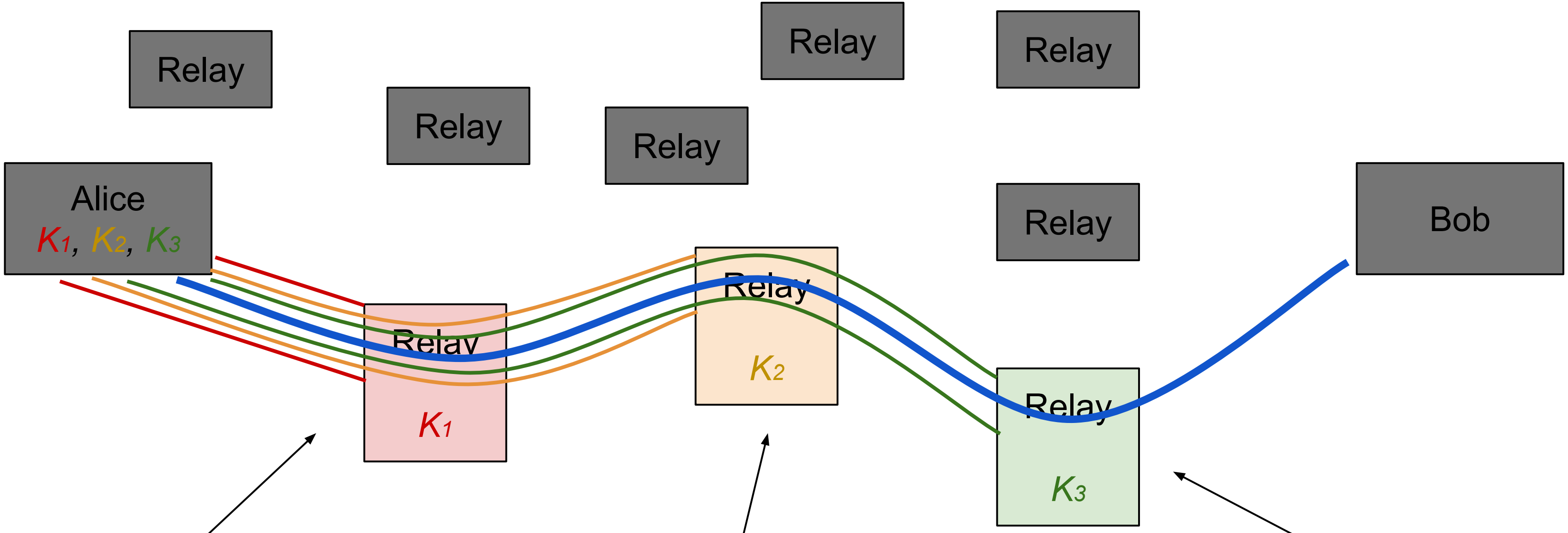
Then she forms a Tor connection with the second node, through the first node

Notice: Relay 1 is only relaying Tor cells. It doesn't know the contents of the cells!

Then she forms a Tor connection with the exit node, through the second node

Finally, she connects to Bob (optionally forming a TLS connection with Bob)

Tor Circuits



Relay 1 knows that Alice is using Tor but *not* who Alice is talking to

Relay 2 knows nothing (other than that someone is using Tor)

Relay 3 knows that someone is talking to Bob, but not who

Tor Exit Nodes

- Notice: The exit node can see the message and the recipient
  - Without collusion, the exit node doesn't know the sender
- The exit node is a man-in-the-middle attacker
  - If the user is not using TLS to connect to the end host (using HTTP), the exit node can see and modify the traffic
  - If the user is using TLS (using HTTPS), the exit node cannot see or tamper with the contents of the traffic

Tor Weaknesses

- Timing Attacks
    - Observe when Alice sends a message, when Bob receives a message, and link the two together
- Collusion
    - Multiple nodes working together and sharing information
    - Defense: Guard nodes (must have high reputation and must have existed for a long time)
- Distinguishable traffic
    - Does not hide you are using Tor

Who uses anonymity systems?

“If you’re not doing anything wrong, you shouldn’t have anything to hide.”

- Implies that anonymous communication is for criminals

The truth: who uses Tor?

- Journalists, Law Enforcement, Human Rights Activists, Business Executives, Intelligence/Military, Normal People

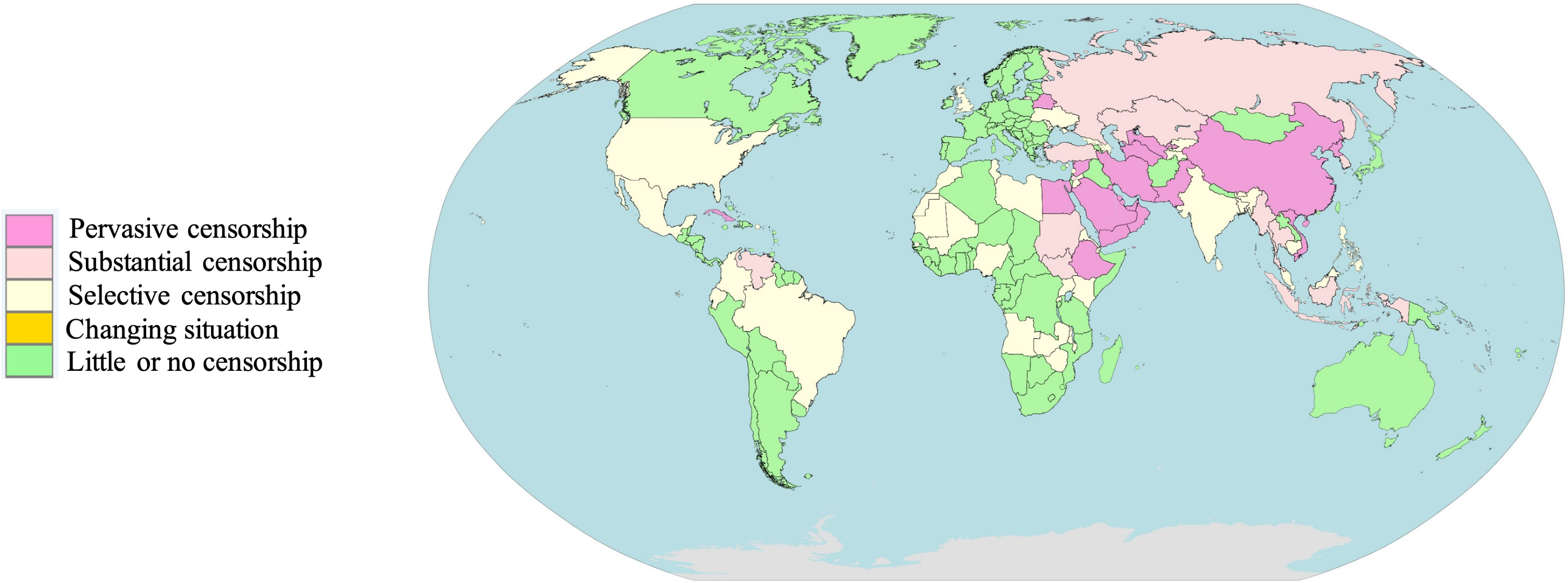
Internet Censorship

- **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

Internet Censorship



Ethics

General Principles

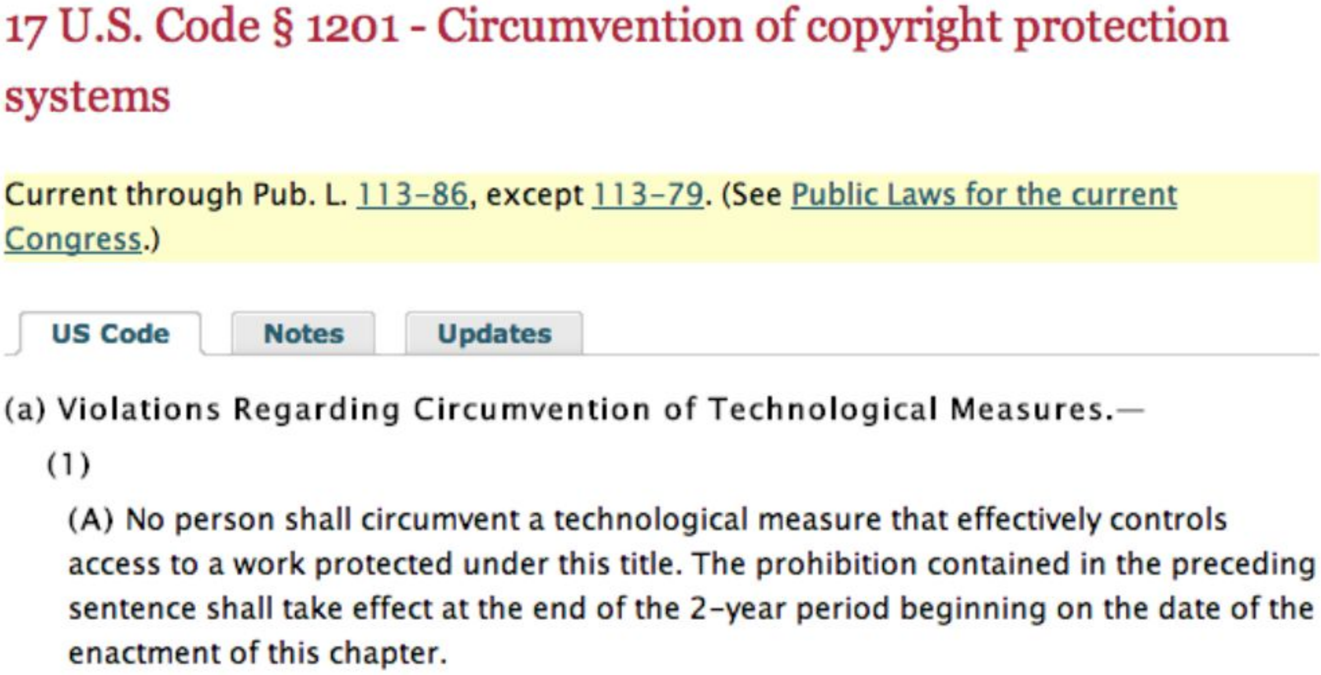
- Ethics:
    - Try to be a good person.
    - Be thoughtful about your actions and their effects on yourself and others.
- Legal issues:
    - Don’t violate laws.
    - If lawyers or law enforcement are involved, you have already lost. It doesn’t matter if you could in theory win the case in the end.

Computer Fraud and Abuse Act (CFAA)

18U.S.CODE §1030-FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS

Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer ...

Digital Millennium Copyright Act (DMCA)



17 U.S. Code § 1201 - Circumvention of copyright protection systems

Current through Pub. L. 113-86, except 113-79. (See Public Laws for the current Congress.)

(a) Violations Regarding Circumvention of Technological Measures.—

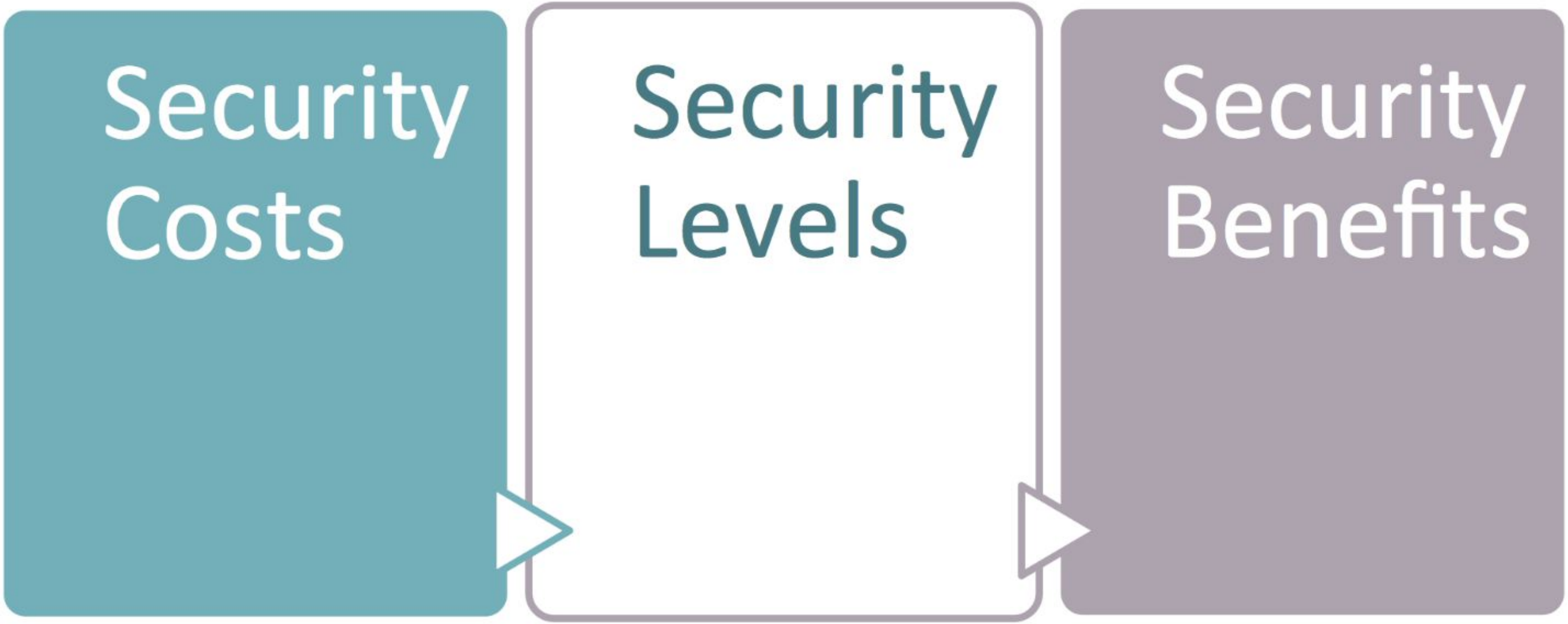
(1)

(A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter.

Economics of (cyber) security

security
computer
guard
fraud
risk
hang
perform
night
data
safe
geeks
using
meets
cyberpeace
like
keep
decision-making
policy/internet
approaches
great
zeros
scientist
subjects
break
administrator
economics
support
cybersecurity
bums
ph.d
human
internet
ones
protecting
statistical
cybercrime
governance
evangelist
network
information
teach
help
abuse
work
technical
guys
prism
scourges
candidate
research
analytical
banks
reality
systems
science
cyber
privacy
excellent
around
bad

Costs, benefits, and levels of security



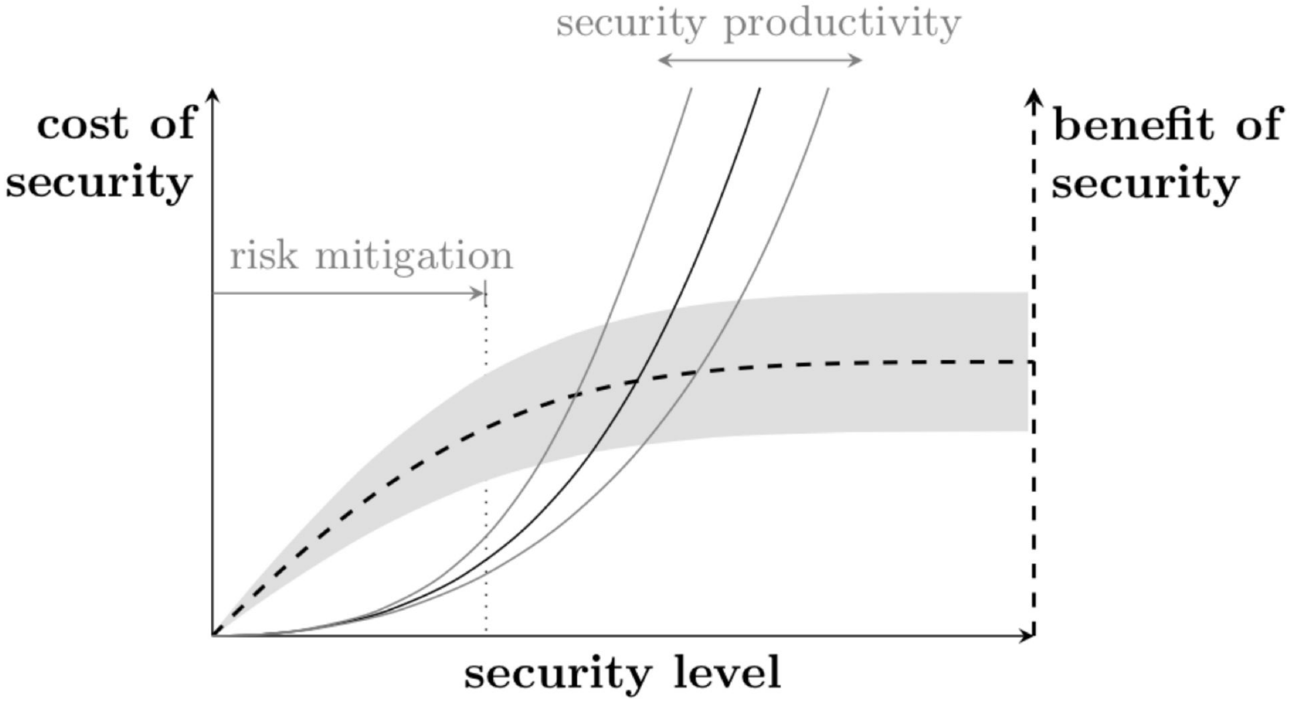
Security Costs

Security Levels

Security Benefits

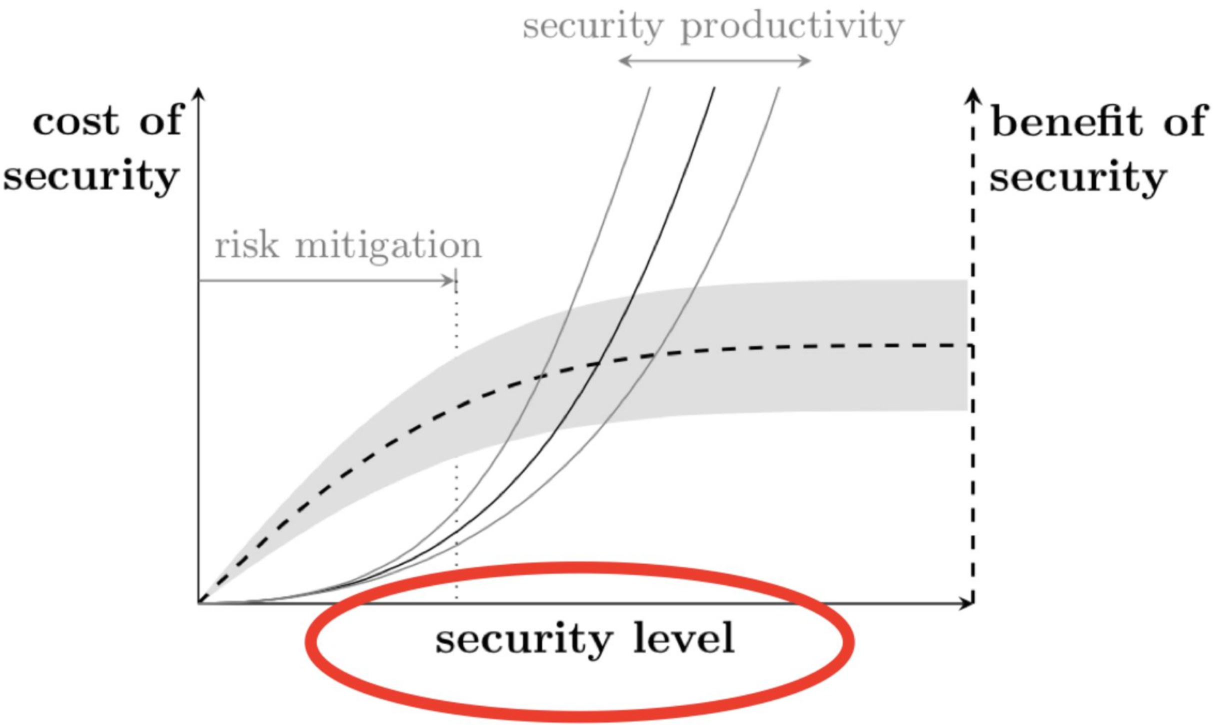
Source: “Economics of Cyber security: What to measure?”

Costs, benefits, and levels of security



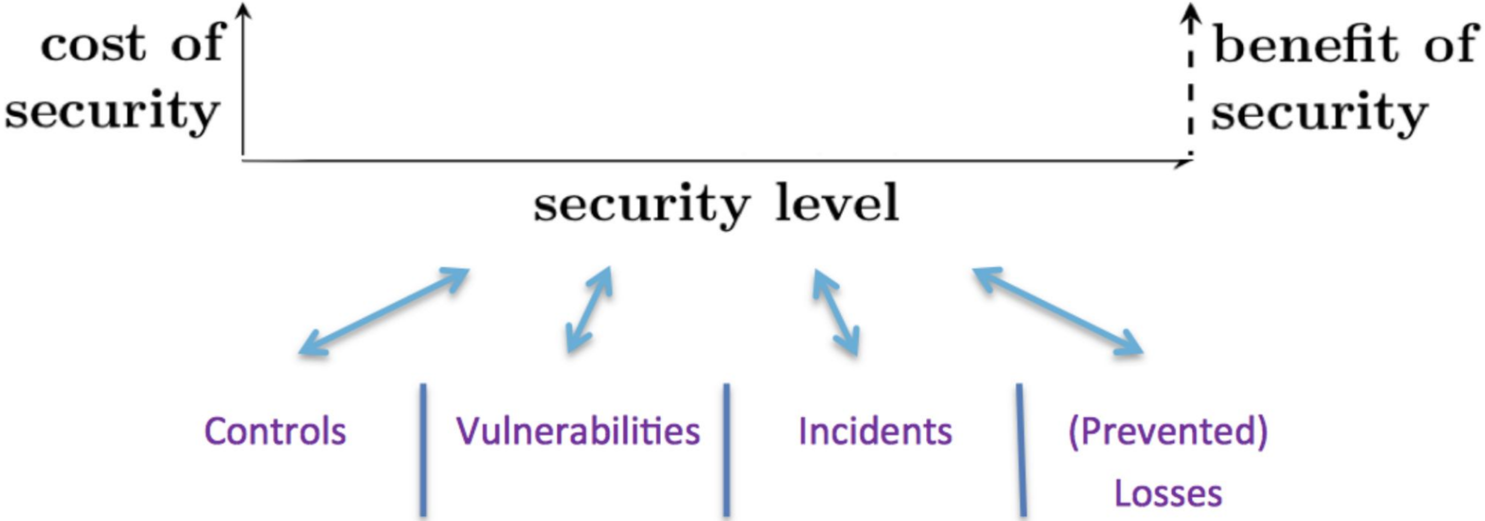
Source: "Economics of Cyber security: What to measure?"

Security Level



Source: "Economics of Cyber security: What to measure?"

Security Level Metrics


cost of security
benefit of security
security level
Controls
Vulnerabilities
Incidents
(Prevented) Losses