

# CSE 127: Introduction to Security

## Lecture 17: Privacy and Anonymity

**Nadia Heninger and Deian Stefan**

UCSD

Fall 2019

# Lecture outline

- Foundations of privacy
- Historical and current “crypto wars” in the US
- Privacy-enhancing technologies
  - PGP and modern encrypted messaging
  - Tor and anonymous communication
  - Privacy-respecting browsers (Tor, Firefox, Brave)

# What is privacy and why do we care?

Various definitions of privacy:

- Secrecy
- Anonymity
- Solitude

Human rights and values:

- Human dignity
- Mental health
- Intimacy/relationships

Political and democratic values:

- Liberty of action
- Moral autonomy

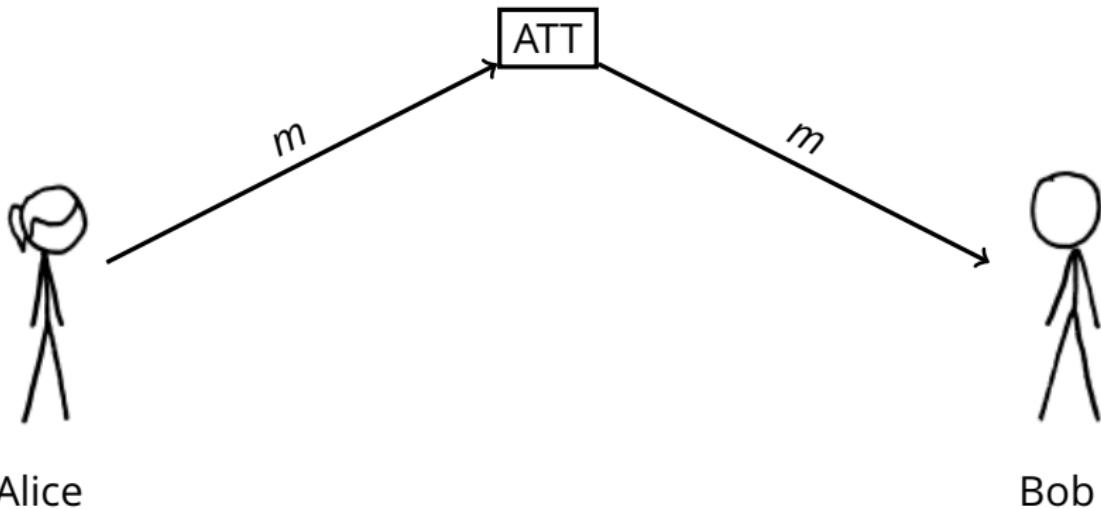
# The “crypto wars”: a historical look

- Crypto wars 1.0
  - Late 1970s,
  - US government threatened legal sanctions on researchers who published papers about cryptography.
  - Threats to retroactively classify cryptography research.
- Crypto wars 2.0
  - 1990s
  - Main issues: Export control and key escrow
  - Several legal challenges
- Crypto wars 3.0
  - Now
  - Snowden
  - Apple v. FBI
  - ...?
  - Calls for “balance”

## Reminder: US export controls on cryptography

- Pre-1994: Encryption software requires individual export license as a munition.
- 1994: US State Department amends ITAR regulations to allow export of approved software to approved countries without individual licenses. 40-bit symmetric cryptography was understood to be approved.
- 1995: Netscape develops initial SSL protocol. Includes weakened “export” cipher suites.
- 1996: Bernstein v. United States; California judge rules ITAR regulations are unconstitutional because “code is speech”
- 1996: Cryptography regulation moved to Department of Commerce.
- 1999: TLS 1.0 standardized. Includes weakened “export” cipher suites.
- 2000: Department of Commerce loosens regulations on mass-market and open source software.

# Third-Party Service Providers

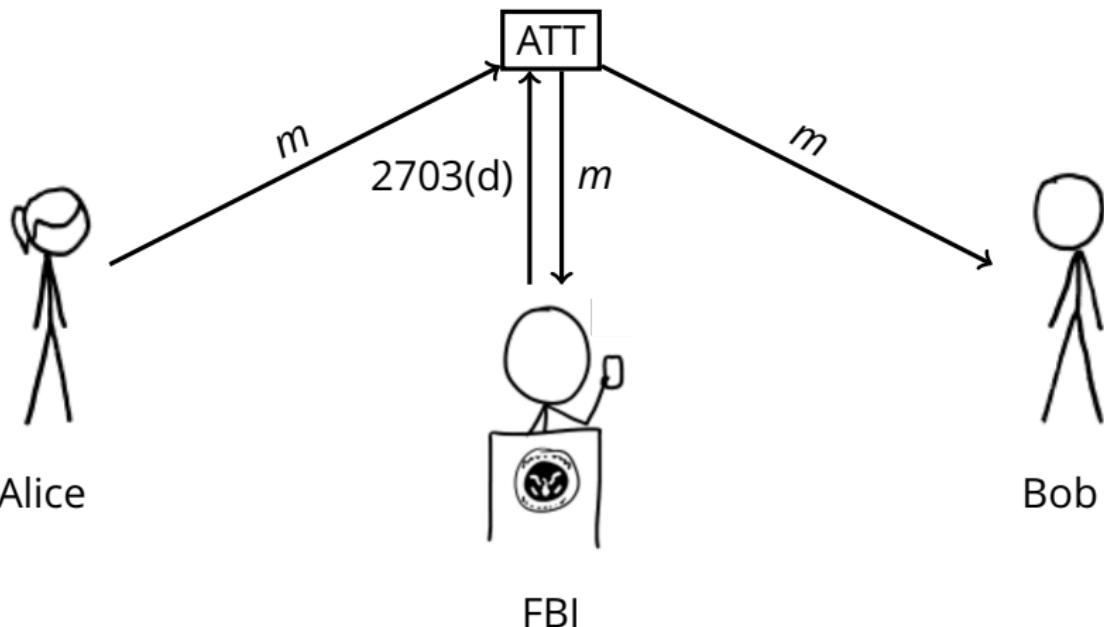


Alice

Bob

Communications/network service providers (ISPs, Google, Facebook, etc.) can generally see all traffic or communications they handle.

# Legal Requests to Service Providers



Under the Stored Communications Act (1986), the US government can compel service providers to turn over customer communications. Only requires a subpoena for "storage" or communications held longer than 180 days.

## Bavarian raids

4 Jul, 2018

On June 20th, in order to gather data on a Riseup user, our fiscal sponsor in the EU was raided by the Bavarian police. This extreme overreach included raids on several homes, a hackerspace, a social center, and a lawyer's office. The police took all the computers, cell phones, disks, and records that they could. Several people were arrested and are now out and safe. However, as a consequence of these raids, the police have filed a number of unrelated charges.

What caused the police-state to raise up its ugly head? In this case, the justification was a website created to organize against a rally of an extreme right political party. It seems in Bavaria, you cannot make a website that tries to get people to come protest neo-fascists without also offending the police. The website had a riseup.net email address listed for a contact, and knowing they cannot get information from Riseup, the police looked at Riseup's donate page and found we accept donations in Europe through a non-profit organization ("Verein") based in Germany called Zwiebelfreunde. They decided this meant that Riseup was run by this organization (it is not), and so aggressively targeted this organization.

What does this mean for you, dear Riseup user?

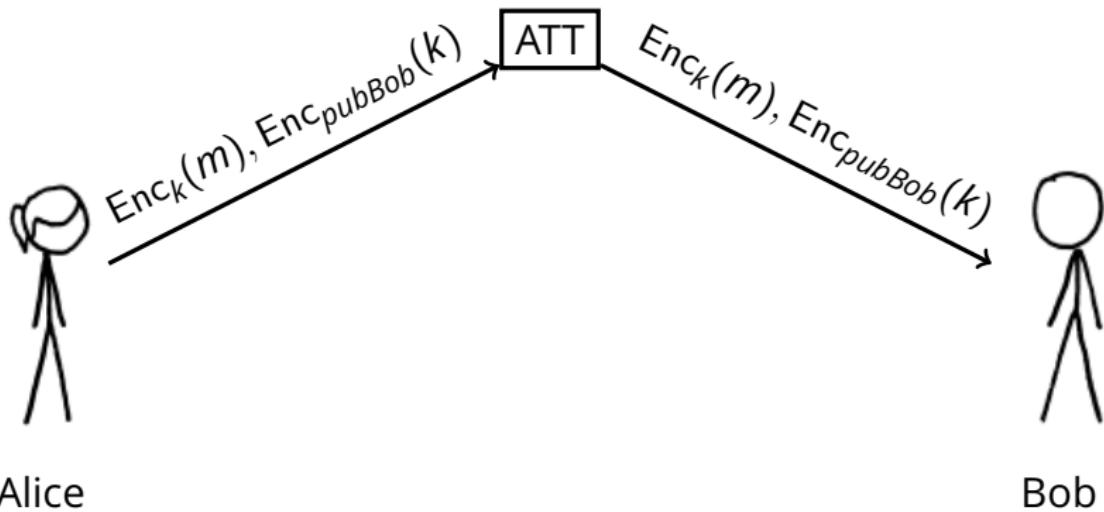
First, don't panic. All your data stored by Riseup is still secure.

Second, if you donated to Riseup via our European IBAN mechanism then there is a good chance the German police now have a record of your bank account number, name, amount you donated, and the date of the donation.

Third, please join us in supporting our friends and allies at Zwiebelfreunde<sup>1</sup>. They are amazing and need your support. In the coming weeks, information will be posted to their website detailing ways that you can help.

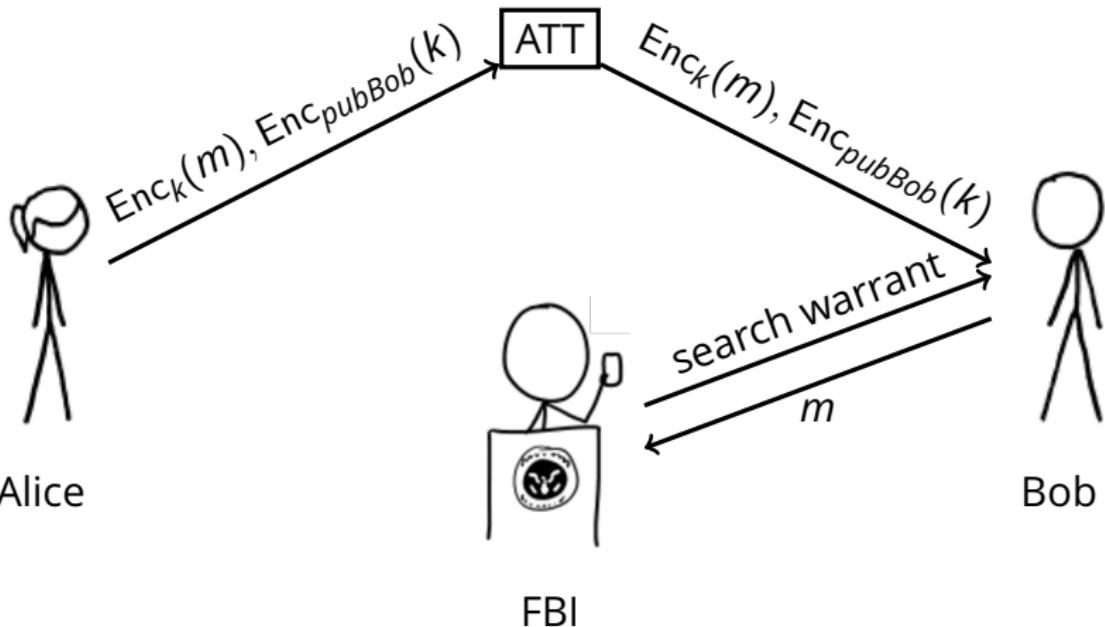
In solidarity,  
The Riseup Birds

# End-to-end encryption and service providers



If a message is end-to-end encrypted, the service provider may not have the plaintext.

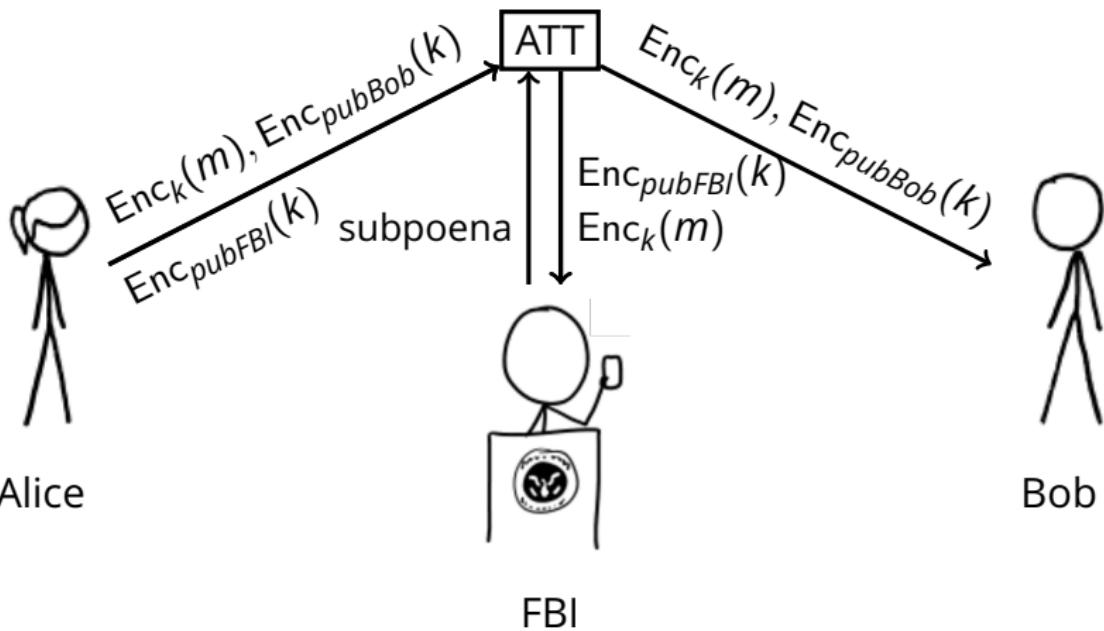
# End-to-end encryption and service providers



Law enforcement can always serve the customer with a search warrant for the decrypted communications.

# End-to-end encryption and service providers

"Key escrow" or "backdoored encryption"



The US government has been asking service providers to design ways to overcome encryption for decades. Most reasonable proposals work something like this.

# Pretty Good Privacy (PGP)

- Written by Phil Zimmermann in 1991
  - Response to US Senate bill requiring crypto backdoors (didn't pass)
- Public key email encryption "for the masses"
  - Signatures, public key encryption, or sign+encrypt
- Key management
  - Public keyservers
  - Web of trust: users sign other users' keys
- Grand jury investigated Zimmermann 1993–1996
  - No indictment issued, but was a subject for violating export controls
- Fundamental insight: Knowledge about cryptography is public. In theory citizens can circumvent government-mandated key escrow by implementing cryptography themselves.

Type	bits/keyID	cr. time	exp time	key	expir
<hr/>					
pub	1024D/ <a href="#">B2D7795E</a>	2001-01-04			
sig	dirct <a href="#">B2D7795E</a>	2001-01-04			<a href="#">[selfsig]</a>
	Revocation key fingerprint:	<a href="#">3FC7 3204 1D23 E9EA 66DD</a>	<a href="#">B500 9C9D BC21 DF74 DC61</a>		
uid	<a href="#">Philip R. Zimmermann &lt;prz@mit.edu&gt;</a>				
sig	sig <a href="#">B2D7795E</a>	2001-01-04			<a href="#">[selfsig]</a>
sig	sig <a href="#">B2D7795E</a>	2001-01-04			<a href="#">[selfsig]</a>
sig	sig <a href="#">FAEBD5FC</a>	2001-01-04			<a href="#">Philip R. Zimmermann &lt;prz@acm.org&gt;</a>
sig	sig <a href="#">B2D7795E</a>	2001-01-06			<a href="#">[selfsig]</a>
sig	exp <a href="#">FAEBD5FC</a>	2001-01-06	2010-01-06		<a href="#">Philip R. Zimmermann &lt;prz@acm.org&gt;</a>
sig	sig <a href="#">66A74B31</a>	2001-01-06			<a href="#">Teun Nijsen &lt;teun.nijsen@uvt.nl&gt;</a>
sig	sig <a href="#">66A74B31</a>	2001-01-06			<a href="#">Teun Nijsen &lt;teun.nijsen@uvt.nl&gt;</a>
sig	sig <a href="#">CF73EC4C</a>	2001-01-06			<a href="#">Will Price &lt;wprice@pgp.com&gt;</a>
sig	sig <a href="#">CF73EC4C</a>	2001-01-06			<a href="#">Will Price &lt;wprice@pgp.com&gt;</a>
sig	sig <a href="#">EEB63AB1</a>	2001-01-06			<a href="#">Ron &amp; Bes Vantreese &lt;ron-bes@usa.net&gt;</a>
sig	sig <a href="#">F414952B</a>	2001-01-07			<a href="#">Jeffrey I. Schiller &lt;jis@gvv.net&gt;</a>
sig	sig <a href="#">F414952B</a>	2001-01-07			<a href="#">Jeffrey I. Schiller &lt;jis@gvv.net&gt;</a>
sig	sig <a href="#">0A791610</a>	2001-01-09			<a href="#">Stale Schumacher Ytteborg &lt;stale@hypnotech.com&gt;</a>
sig	sig <a href="#">0A791610</a>	2001-01-09			<a href="#">Stale Schumacher Ytteborg &lt;stale@hypnotech.com&gt;</a>
sig	sig <a href="#">4793C529</a>	2001-02-02			<a href="#">Hugh Miller &lt;hmiller@luc.edu&gt;</a>
sig	sig <a href="#">EE881DEC</a>	2001-03-03			<a href="#">h3xx &lt;h3x.x@phreaker.net&gt;</a>
sig	sig <a href="#">D7C776BF</a>	2001-03-03			<a href="#">h3xx Secure Data</a>
sig	sig <a href="#">EEB63AB1</a>	2001-03-05			<a href="#">Ron &amp; Bes Vantreese &lt;ron-bes@usa.net&gt;</a>
sig	sig <a href="#">EEB63AB1</a>	2001-03-05			<a href="#">Ron &amp; Bes Vantreese &lt;ron-bes@usa.net&gt;</a>
sig	sig <a href="#">BF67D2EB</a>	2001-03-10			<a href="#">Michael A. Haisley Jr. &lt;mikehaisley@home.com&gt;</a>
sig	sig <a href="#">BF67D2EB</a>	2001-03-10			<a href="#">Michael A. Haisley Jr. &lt;mikehaisley@home.com&gt;</a>
sig	sig <a href="#">F491BD21</a>	2001-04-13			<a href="#">Ben Paul Wise &lt;bwise@sito.saic.com&gt;</a>
sig	sig <a href="#">251F35C1</a>	2001-04-20			<a href="#">Marco Balmer &lt;marco.balmer@calculus.ch&gt;</a>



<https://xkcd.com/364/>

"Never bring tequila to a key-signing party."

# PGP in the modern era

- PGP was built before modern cryptographic protocol design was properly understood.
- Numerous vulnerabilities
  - Outdated cipher choices
  - Doesn't authenticate encryption with a MAC or authenticated encryption mode
- Commercialized in the 90s, most recently developed by Symantec
- GnuPG and libgcrypt open source and quite widely used
- 2005 paper on usability issues: "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0" by Whitten and Tygar
  - Most experts unable to use PGP properly

## HOW TO USE PGP TO VERIFY THAT AN EMAIL IS AUTHENTIC:



<https://xkcd.com/1181/>

"If you want to be extra safe, check that there's a big block of jumbled characters at the bottom."

# Message Encryption since PGP

- For messaging, Signal, WhatsApp, or iMessage offer modern end-to-end encryption.
- Modern protocols typically:
  - Use Diffie-Hellman to negotiate ephemeral keys
  - Use long-term authentication keys with out-of-band fingerprint verification
  - Offer “forward secrecy”:
    - In theory, protects against key compromise at time  $t$  revealing plaintext of previous messages
    - If sender or recipient store plaintext, this is more likely point of compromise
  - Offer “deniability”:
    - Message recipient can verify message integrity without a third party being able to “cryptographically prove” that sender sent the message.
    - Cryptographically interesting, but likely legally irrelevant.

# Crypto Wars 2.0

In the current debates about government-mandated weakening of cryptography, there are two scenarios of interest:

- Message encryption.
  - This is what we've talked about so far in lecture.
- Storage encryption.
  - For example, unlocking iPhones.
  - This is what the Apple v. FBI case was about.

In Apple v. FBI, the question was whether the government could compel Apple to break their own encryption mechanism with the All Writs Act. The government backed down and reportedly used a specialty consulting firm to unlock the phone.

5 the following three important functions: (1) it will bypass or  
6 disable the auto-erase function whether or not it has been enabled;  
7 (2) it will enable the FBI to submit passcodes to the SUBJECT DEVICE  
8 for testing electronically via the physical device port, Bluetooth,  
9 Wi-Fi, or other protocol available on the SUBJECT DEVICE; and (3) it  
10 will ensure that when the FBI submits passcodes to the SUBJECT  
11 DEVICE, software running on the device will not purposefully  
12 introduce any additional delay between passcode attempts beyond what  
13 is incurred by Apple hardware.

14       3. Apple's reasonable technical assistance may include, but is  
15 not limited to: providing the FBI with a signed iPhone Software  
16 file, recovery bundle, or other Software Image File ("SIF") that can  
17 be loaded onto the SUBJECT DEVICE. The SIF will load and run from  
18 Random Access Memory ("RAM") and will not modify the iOS on the  
19 actual phone, the user data partition or system partition on the  
20 device's flash memory. The SIF will be coded by Apple with a unique  
21 identifier of the phone so that the SIF would only load and execute  
22 on the SUBJECT DEVICE. The SIF will be loaded via Device Firmware  
23 Upgrade ("DFU") mode, recovery mode, or other applicable mode

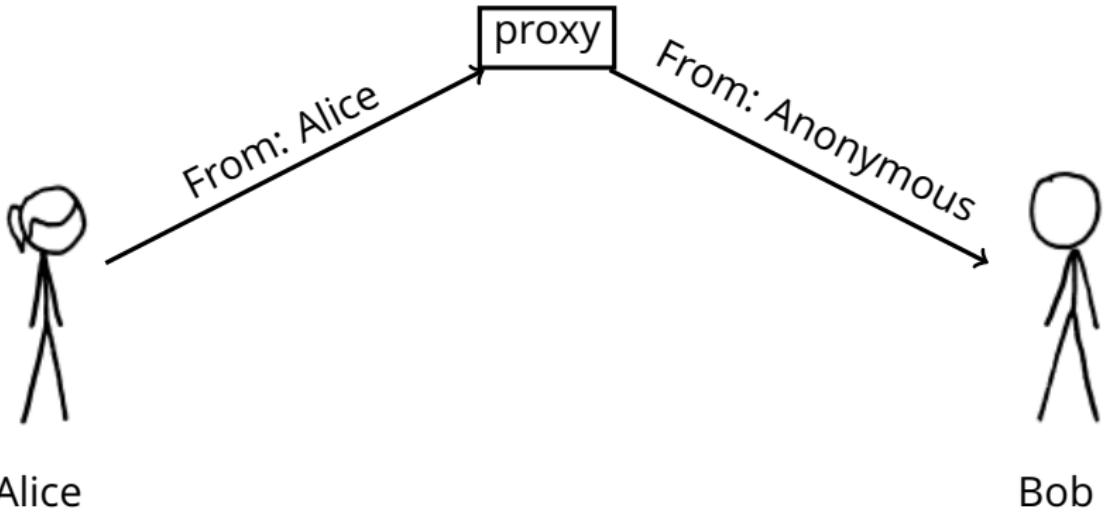
# Anonymity

Michael Hayden, former NSA director: "We kill people based on metadata."

- Long history of anonymous communication in US democracy
- e.g. Revolutionary war anonymous political pamphlets

**Technical question:** Is anonymous communication still feasible on the internet?

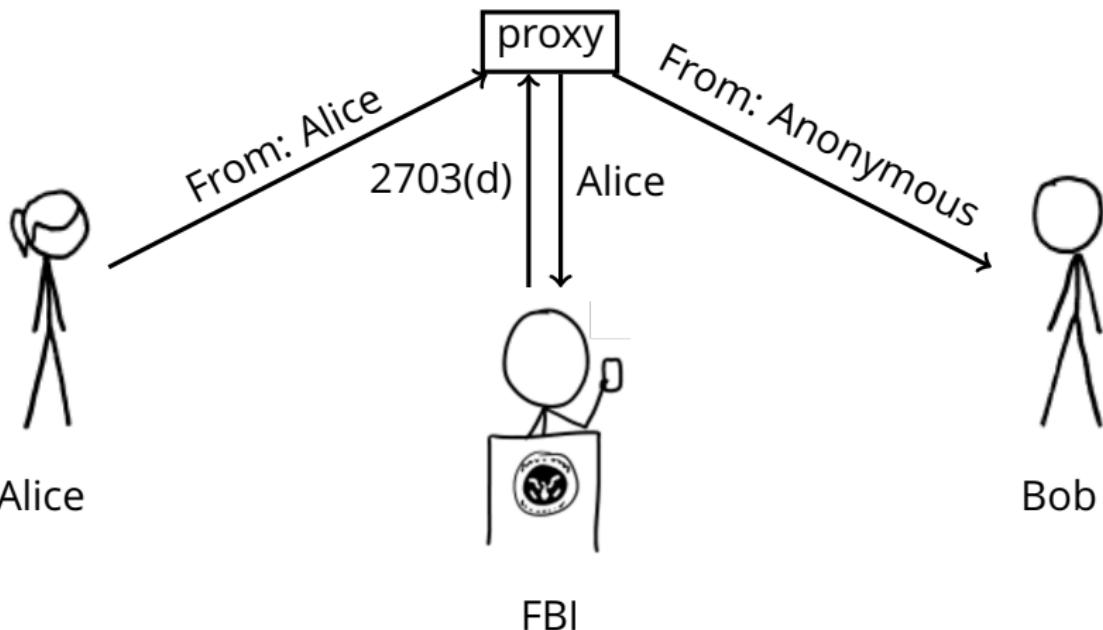
## “Anonymity” via tunneling or proxies



A proxy can rewrite metadata. Examples:

- Early “anonymous remailers” forwarded email.
- VPN services allow users to tunnel traffic

## "Anonymity" via tunneling or proxies



One-hop proxies have a single point of failure, must see both sides of communication.

# Attempt to fix: Anonymous bulletin boards

Post message encrypted to recipient in public; recipient tries to decrypt all messages.

The screenshot shows a web browser window with the URL <https://groups.google.com/forum/#!forum/alt.anonymous.messages>. The page is a Google Groups forum. The title of the forum is "alt.anonymous.messages". There are 30 topics listed. The first post is highlighted with a blue border. The posts are as follows:

Post ID	Author	Content	Timestamp
e3f830a750e86cc02d6ca9d9085e6584b9dea671201b4354	By Anonymous	1 post - 0 views	3:26 PM
23dbc30573b09ffff978fb828bcc652aa08ec35bfff960b34	By Nobody	1 post - 0 views	3:25 PM
2cf6a2383a8eb1f0d2030e9481c34427af0b/46a58cb51fe	By Anonymous	1 post - 0 views	3:25 PM
9e6bcd1268ecd042e583e8c3a8eff4104717bf1934085470	By Anonymous	1 post - 0 views	3:12 PM
860aae78a0e2bf0e7294a73f0c2299f69e413ba9556d4b8ab	By Anonymous	1 post - 0 views	3:11 PM
A8RLUhD0egA7UXEJfZFFXhvry9dtBoi/APnmsq3bHC8	By Anonymous	6 posts - 0 views	3:02 PM
6de94aae75cae14475792bb0b8d42fcfd6267d6c1509c157	By Nomen Nescio	1 post - 0 views	2:49 PM
850251801c5e6fc1460bc994a2e3e49f639e72e3ea0c55d8	By Nobody	1 post - 0 views	2:48 PM
72ca49dfde614c21beb1a52a8df45b4383b002945220/da5			

Bulletin board host still has metadata from visitors.

# Tor: Anonymous communication for TCP sessions

Desired properties:

- Network attacker watching client traffic can't see destination.
- Destination server does not see client IP address.
- Network nodes can't link client and server.
- Fast enough to support TCP streams and network applications.

Current state: A nonprofit organization, active academic research, deployed around the world.

Not perfect, but a building block.

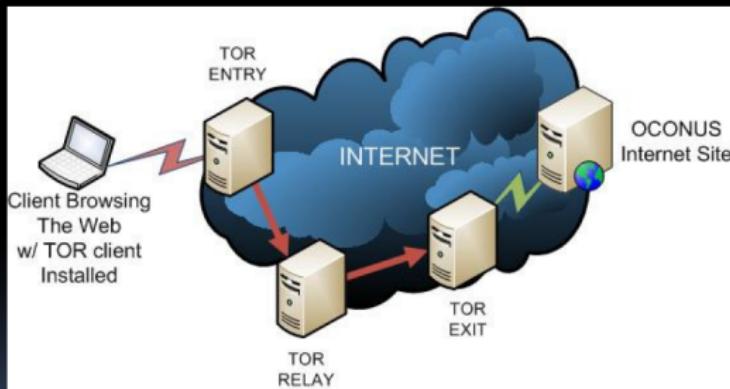


## (U) What is TOR?

- (U) “The Onion Router”
- (U) Enables anonymous internet activity
  - General privacy
  - Non-attribution
  - Circumvention of nation state internet policies
- (U) Hundreds of thousands of users
  - Dissidents (Iran, China, etc)
  - (S//SI//REL) **Terrorists!**
  - (S//SI//REL) Other targets too!

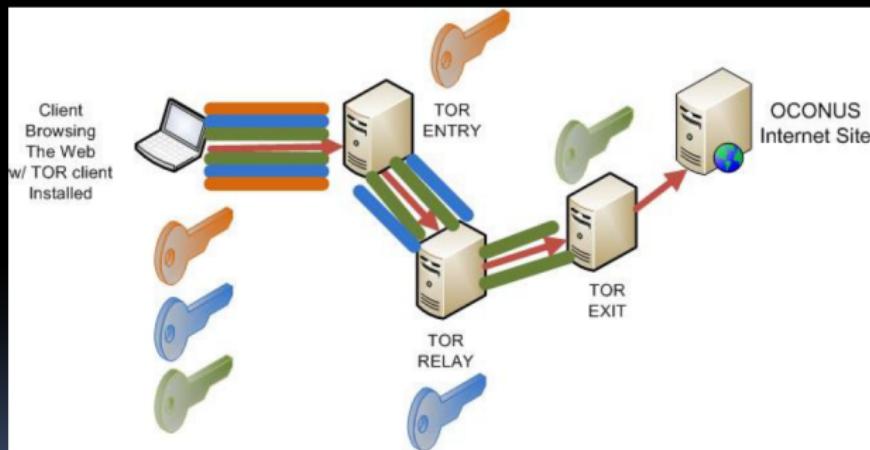


# (U) What is TOR?





# (U) What is TOR?





# (U) What is TOR?

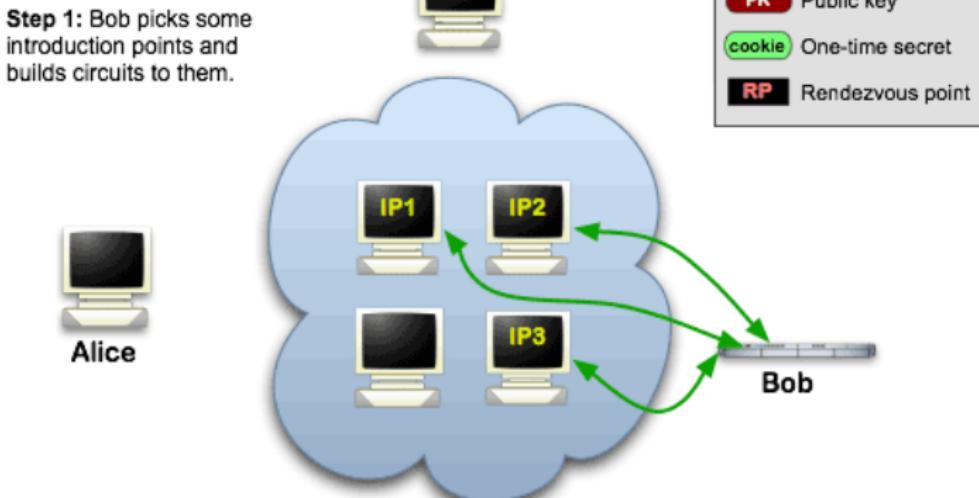
- (U) TOR Browser Bundle
  - Portable Firefox 10 ESR (tbb-firefox.exe)
  - Vidalia
  - Polipo
  - TorButton
  - TOR
  - “Idiot-proof”

# Tor also allows “anonymous” servers



## Onion Services: Step 1

Step 1: Bob picks some introduction points and builds circuits to them.

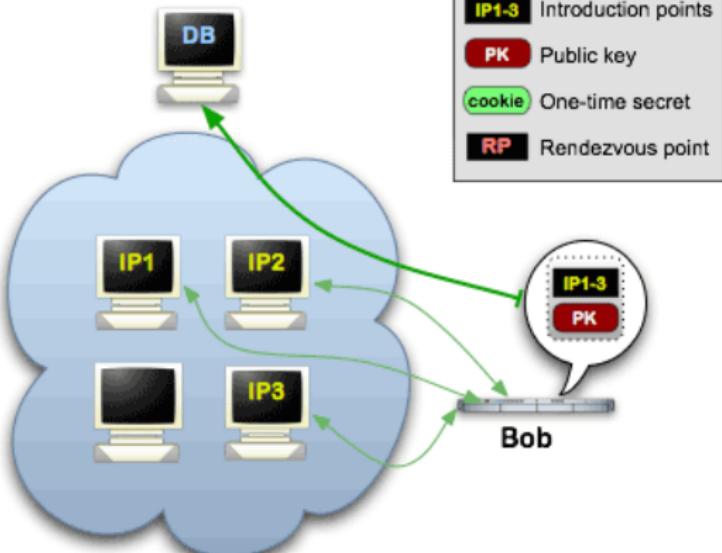


# Tor also allows “anonymous” servers



## Onion Services: Step 2

Step 2: Bob advertises his service -- XYZ.onion -- at the database.

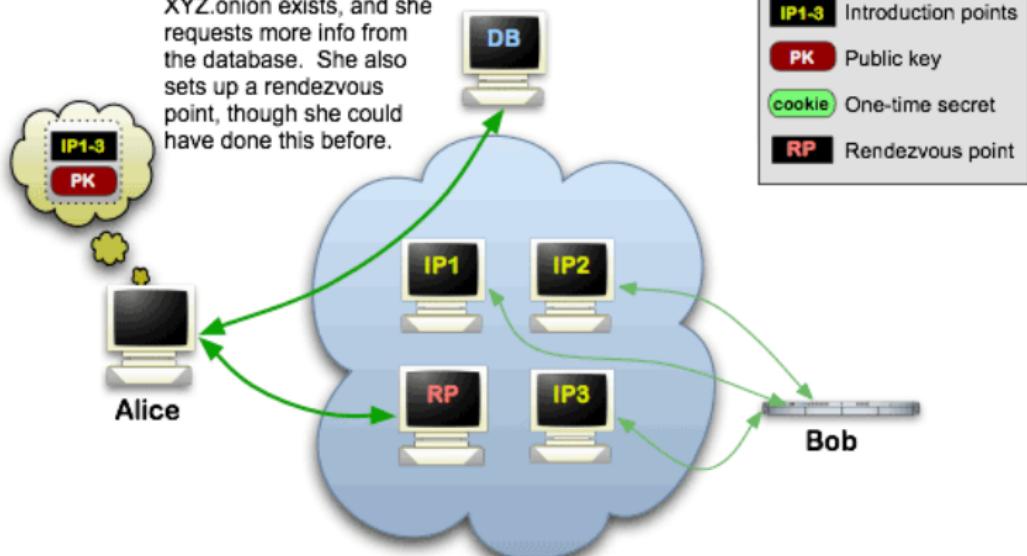


# Tor also allows “anonymous” servers



## Onion Services: Step 3

**Step 3:** Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.

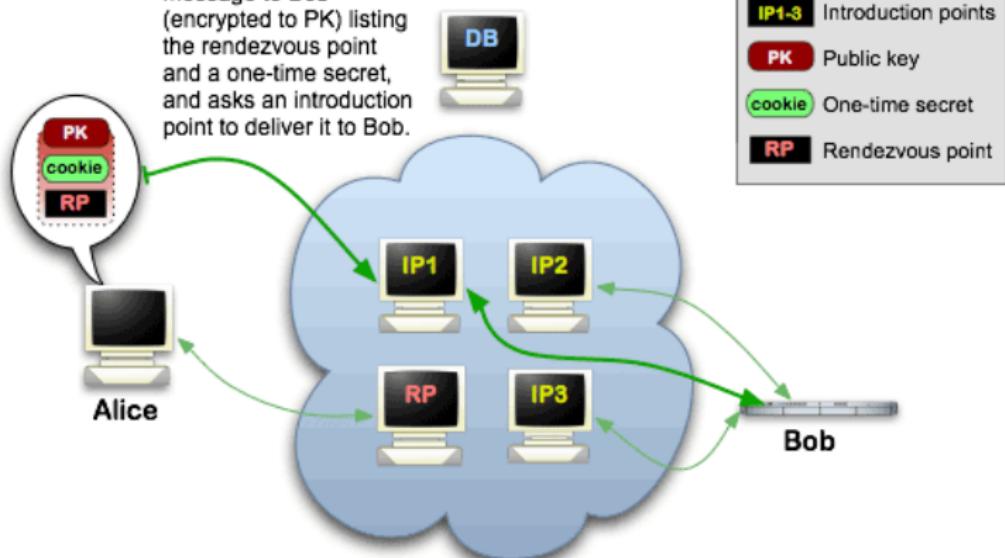


# Tor also allows “anonymous” servers



## Onion Services: Step 4

**Step 4:** Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.



# Tor also allows “anonymous” servers

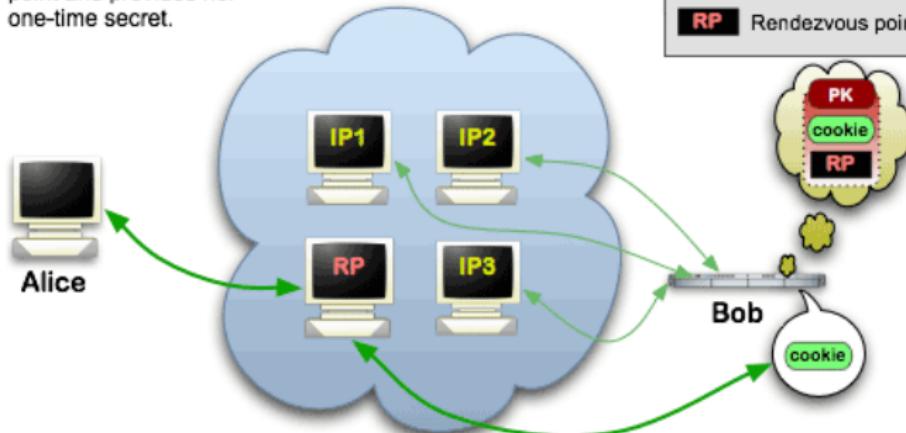


## Onion Services: Step 5

**Step 5:** Bob connects to the Alice's rendezvous point and provides her one-time secret.



	Tor cloud
	Tor circuit
	Introduction points
	Public key
	One-time secret
	Rendezvous point



# Tor also allows “anonymous” servers

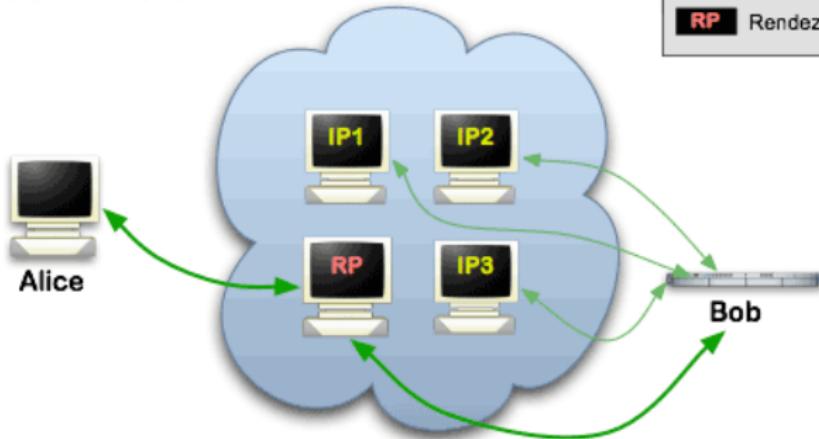


## Onion Services: Step 6

**Step 6:** Bob and Alice proceed to use their Tor circuits like normal.



	Tor cloud
	Tor circuit
	IP1-3 Introduction points
	PK Public key
	cookie One-time secret
	RP Rendezvous point



# Tor also allows “anonymous” servers

The screenshot shows the Silk Road anonymous marketplace homepage. At the top, there's a navigation bar with links like "Welcome! | Silk Road", "Most Visited", "Learn more about Tor", "The Tor Blog", "TORDIR - Link List", and "Welcome! | Silk Road". Below the header, the Silk Road logo is displayed with the text "Silk Road" and "anonymous marketplace". To the right, there are links for "Welcome", "messages(0)", "orders(0)", "account(\$0)", "settings", "log out", and a shopping cart icon showing "(0)".  
  
On the left, there's a sidebar titled "Shop by category:" with links to various drug categories: Cannabis(203), Ecstasy(35), Psychedelics(127), Opioids(39), Stimulants(68), Dissociatives(9), Other(197), and Benzos(43).  
  
The main content area features three product cards: "1 hit of LSD (blotter)" for \$0.58, "1/8 oz high quality cannabis" for \$2.05, and "1 g pure MDMA (white)" for \$1.28. Each card includes an image of the product.  
  
To the right of the products, there's a "Step-by-step:" guide with three steps: "Get anonymous money", "Buy something here", and "Enjoy it when it arrives!". Below this, a note says "Vacation mode. Important info for sellers...".  
  
At the bottom, there's a section titled "recent feedback:" showing reviews from sellers like "1UP of Canada(97)", "CaliforniaSunrise", "Rook", "illy", "somatik", "gamely54", "mellowyellow", and "dirtysouf(100)". Each review includes a rating (e.g., 4 of 5) and a short comment. The "item" link at the end of each row likely leads to the seller's profile.

vice.com

In practice, prominent “hidden services” deanonymized through real-world metadata, browser 0days, misconfigured servers.



Stinks (U)

[REDACTED]  
[REDACTED]  
CT SIGDEV  
[REDACTED]

JUN 2012

Derived From: NSA/CSSM 1-52  
Dated: 20070108  
Declassify On: 20370101

# Tor Stinks... (U)

- We will never be able to de-anonymize all Tor users all the time.
- With manual analysis we can de-anonymize a **very small fraction** of Tor users, however, **no** success de-anonymizing a user in response to a TOPI request/on demand.

b. On March 1, 2012, at approximately 5:03 p.m. CST, HAMMOND was seen leaving the CHICAGO RESIDENCE. Almost immediately after, CW-1 (in New York) contacted me to report that the defendant was offline. Pen/Trap data also reflected that TOR network activity and Internet activity from the CHICAGO RESIDENCE stopped at approximately the same time.

c. Later, also on March 1, 2012, at approximately 6:23 p.m. CST, HAMMOND was observed returning to the CHICAGO RESIDENCE. TOR network traffic resumed from the CHICAGO RESIDENCE approximately a minute or so later. Moreover, CW-1 reported to me that the defendant, using the online alias "yohoho," was back online at approximately the same time as physical surveillance in Chicago showed HAMMOND had returned to the CHICAGO RESIDENCE. New York FBI, through a program that remotely monitors the Internet activity of the buddy list on CW-1's jabber program, including when a "buddy" signs on and off, corroborated CW-1's report that the defendant, using "yohoho," was back online. Pen/Trap data reflected extensive TOR-related activity through the night.

8. In the course of this investigation, I have learned that the person who sent the e-mail messages described above took steps to disguise his identity. Specifically, Harvard received the e-mail messages from a service called Guerrilla Mail, an Internet application that creates temporary and anonymous e-mail addresses available free of charge. Further investigation yielded information that the person who sent the e-mail messages accessed Guerrilla Mail by using a product called TOR, which is also available free of charge on the Internet and which automatically assigns an anonymous Internet Protocol ("IP") address that can be used for a limited period of time. Every computer attached to the Internet uses an IP address, which is a unique numerical identifier, to identify itself to other computers on the Internet and direct the orderly flow of electronic information between them. IP addresses typically consist of four numbers between 0 and 255 separated by periods (*e.g.*, 216.239.51.99). Both TOR and Guerrilla Mail are commonly used by Internet users seeking to communicate anonymously and in a manner that makes it difficult to trace the IP address of the computer being used.

9. Harvard University was able to determine that, in the several hours leading up to the receipt of the e-mail messages described above, ELDOKIM accessed TOR using Harvard's wireless network.

# Privacy on the web

- Companies like Google, Facebook, Twitter, Microsoft, Amazon, Target, Walmart, ... make a lot of money from tracking users.
- For some of these companies you are the product. So tracking you is their business.

# Privacy on the web

- Companies like Google, Facebook, Twitter, Microsoft, Amazon, Target, Walmart, ... make a lot of money from tracking users.
- For some of these companies you are the product. So tracking you is their business.
- How do websites track users?

# Privacy on the web

- Companies like Google, Facebook, Twitter, Microsoft, Amazon, Target, Walmart, ... make a lot of money from tracking users.
- For some of these companies you are the product. So tracking you is their business.
- How do websites track users?
  - Third-party cookies: recall that cookies for `trackme.com` are sent with any request to `trackme.com`, even if you're on `cnn.com`.

# Privacy on the web

- Companies like Google, Facebook, Twitter, Microsoft, Amazon, Target, Walmart, ... make a lot of money from tracking users.
- For some of these companies you are the product. So tracking you is their business.
- How do websites track users?
  - Third-party cookies: recall that cookies for `trackme.com` are sent with any request to `trackme.com`, even if you're on `cnn.com`.
  - Tracking content: Sites include tracking code into URLs (e.g., advertisements, videos, marketing emails, etc.)

# Privacy on the web

- Companies like Google, Facebook, Twitter, Microsoft, Amazon, Target, Walmart, ... make a lot of money from tracking users.
- For some of these companies you are the product. So tracking you is their business.
- How do websites track users?
  - Third-party cookies: recall that cookies for `trackme.com` are sent with any request to `trackme.com`, even if you're on `cnn.com`.
  - Tracking content: Sites include tracking code into URLs (e.g., advertisements, videos, marketing emails, etc.)
  - Fingerprinting: sites profile your browser, extensions, OS, hardware, screen resolution, fonts you have installed, etc.

## What can you do about this?

- Can't really avoid these platforms (e.g., Facebook profiles you even if you don't have an account).
- Use a browser that cares about your privacy (e.g., Firefox, The Tor Browser, Brave, Safari)
- Use privacy-enhancing browser extensions

# Privacy-enhanced browsing (Firefox)

Standard  
Balanced for protection and performance. Pages will load normally.

Strict  
Stronger protection, but may cause some sites or content to break.

Custom  
Choose which trackers and scripts to block.

Cookies All third-party cookies (may cause websites to break)  
Cross-site and social media trackers  
Cookies from unvisited websites  
All third-party cookies (may cause websites to break)  
All cookies (will cause websites to break)

Tracking cookies

Cryptominers

Fingerprinters

 You will need to reload your tabs to apply these changes. [Reload All Tabs](#)

 Heads up!  
Blocking trackers could impact the functionality of some sites. Reload a page with trackers to load all content. [Learn how](#)

Send websites a "Do Not Track" signal that you don't want to be tracked [Learn more](#)

- Always
- Only when Firefox is set to block known trackers

# Privacy-enhanced browsing (Tor)

## Security

### Security Level

Disable certain web features that can be used to attack your security and anonymity.

[Learn more](#)

**Standard**

All Tor Browser and website features are enabled.

**Safer**

Disables website features that are often dangerous, causing some sites to lose functionality.

JavaScript is disabled on non-HTTPS sites.

Some fonts and math symbols are disabled.

Audio and video (HTML5 media), and WebGL are click-to-play.

**Safest**

Only allows website features required for static sites and basic services. These changes affect images, media, and scripts.

JavaScript is disabled by default on all sites.

Some fonts, icons, math symbols, and images are disabled.

Audio and video (HTML5 media), and WebGL are click-to-play.

# Privacy-enhanced browsing (Brave & Safari)

The image shows two screenshots side-by-side comparing privacy settings in the Brave browser and the Safari browser on iOS.

**Brave Browser Privacy Report (Left):**

- Shields:** Enabled (purple switch).
- cnn.com Blocking Monitor:**
  - 55 Ads and Trackers blocked.
  - 1 HTTPS Upgrades.
  - 0 Scripts Blocked.
  - 0 Fingerprinting Methods.
- Individual Controls:**
  - Block Ads & Tracking: Enabled (purple switch).
  - HTTPS Everywhere: Enabled (purple switch).
  - Block Phishing: Enabled (purple switch).
  - Block Scripts: Disabled (gray switch).
  - Fingerprinting Protection: Enabled (purple switch).

**Safari Settings (Right):**

- Block Pop-ups:** Enabled (green switch).
- Content Blockers:** Enabled (green switch).
- Downloads:** iCloud Drive selected.
- TABS:**
  - Show Tab Bar: Enabled (green switch).
  - Show Icons in Tabs: Disabled (gray switch).
- Open Links:** In New Tab selected.
- Close Tabs:** Manually selected.
- PRIVACY & SECURITY:**
  - Allow Safari to automatically close tabs that haven't recently been viewed.
  - Prevent Cross-Site Tracking: Enabled (green switch).
  - Block All Cookies: Disabled (gray switch).
  - Fraudulent Website Warning: Enabled (green switch).
  - Check for Apple Pay: Enabled (green switch).

# Privacy-enchanting extensions

- Privacy Badger blocks trackers; uBlock Origin blocks ads; many others

The screenshot shows a web browser window displaying a CNN article about Donald Trump. The Privacy Badger extension is active, overlaying the page with its interface. The main content of the page includes a headline "Trump will not" and a large image of Donald Trump's ear. The Privacy Badger interface lists several tracking domains with their status: avm.dunns.com (red), ib.adnxs.com (red), c.amazon-adsystem.com (red), bat.bing.com (red), cdnjs.cloudflare.com (yellow), and dpm.demdex.net (red). Below this list are three buttons: "Disable Privacy Badger for This Site", "Did Privacy Badger break this site? Let us know!", and "Donate to EFF". A small note at the bottom states "version 2019.11.18".

TRENDING: New Orleans shooting | London

## Trump will not

Neither the President

Wednesday's impeachment hearing, the White House has told the House Judiciary Committee

Privacy Badger detected 15 potential [trackers](#) on this page. You shouldn't need to adjust the sliders unless something is broken.

Domain	Status
avm.dunns.com	Red
ib.adnxs.com	Red
c.amazon-adsystem.com	Red
bat.bing.com	Red
cdnjs.cloudflare.com	Yellow
dpm.demdex.net	Red

[Disable Privacy Badger for This Site](#)

[Did Privacy Badger break this site? Let us know!](#)

[Donate to EFF](#)

version 2019.11.18

# Privacy-enchanting extensions

- Privacy Badger blocks trackers; uBlock Origin blocks ads; many others

