CS5331: Web Security

Lecture 10: Web Privacy

Privacy in Web

Reference:

Cybersecurity 101: Protect your privacy from hackers, spies, and the government
https://www.zdnet.com/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-government/

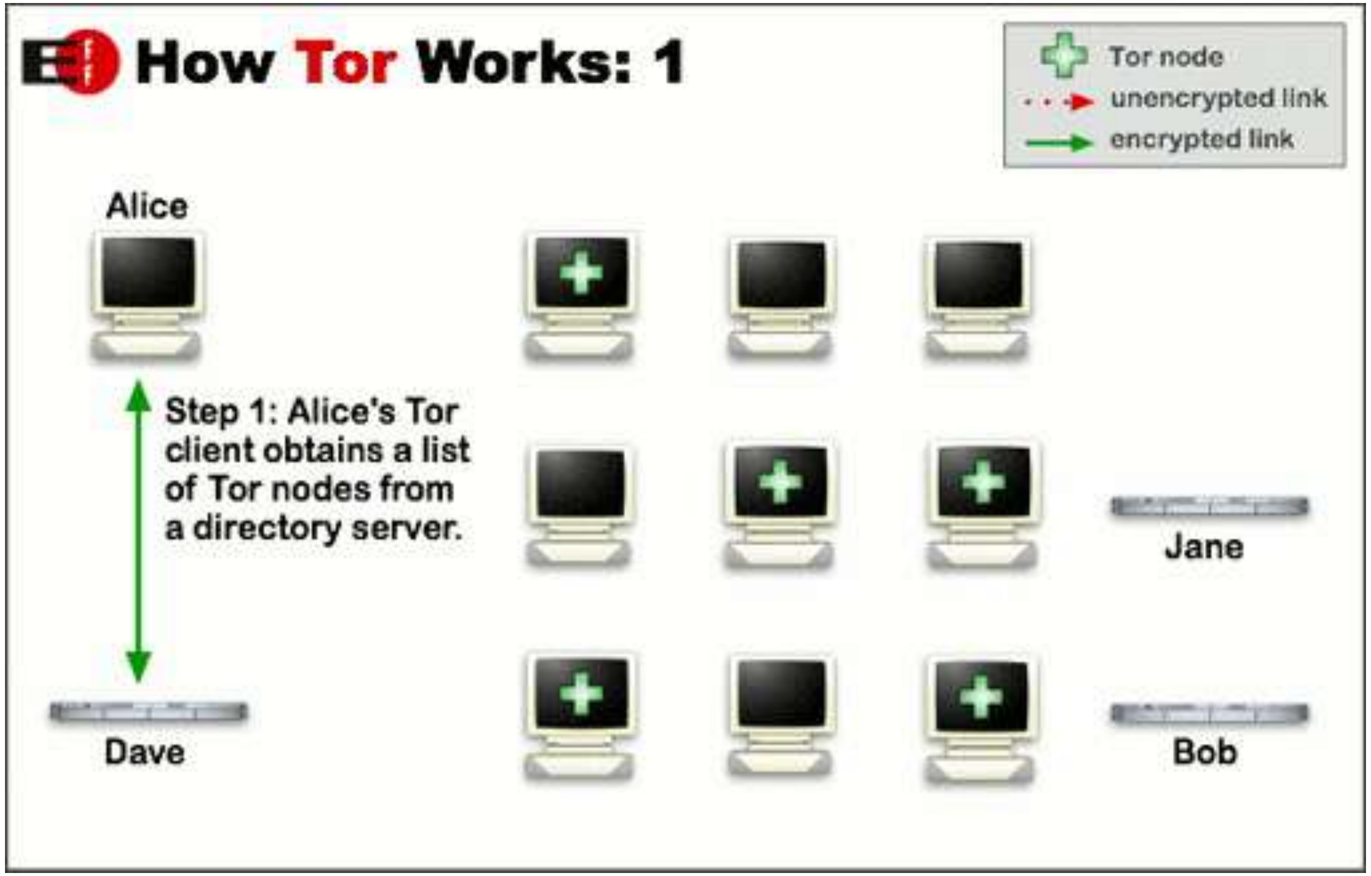
Definition of Internet Privacy

- **Internet privacy** involves the right or mandate of personal privacy concerning the storing, repurposing, provision to third parties, and displaying of information pertaining to oneself via the Internet*. -- Wikipedia*
- Security vs. Privacy
  - Security is about who can access data.
  - Privacy is about who, *at what time, for which purpose,* can have access data.

Scope of Privacy and Data Management

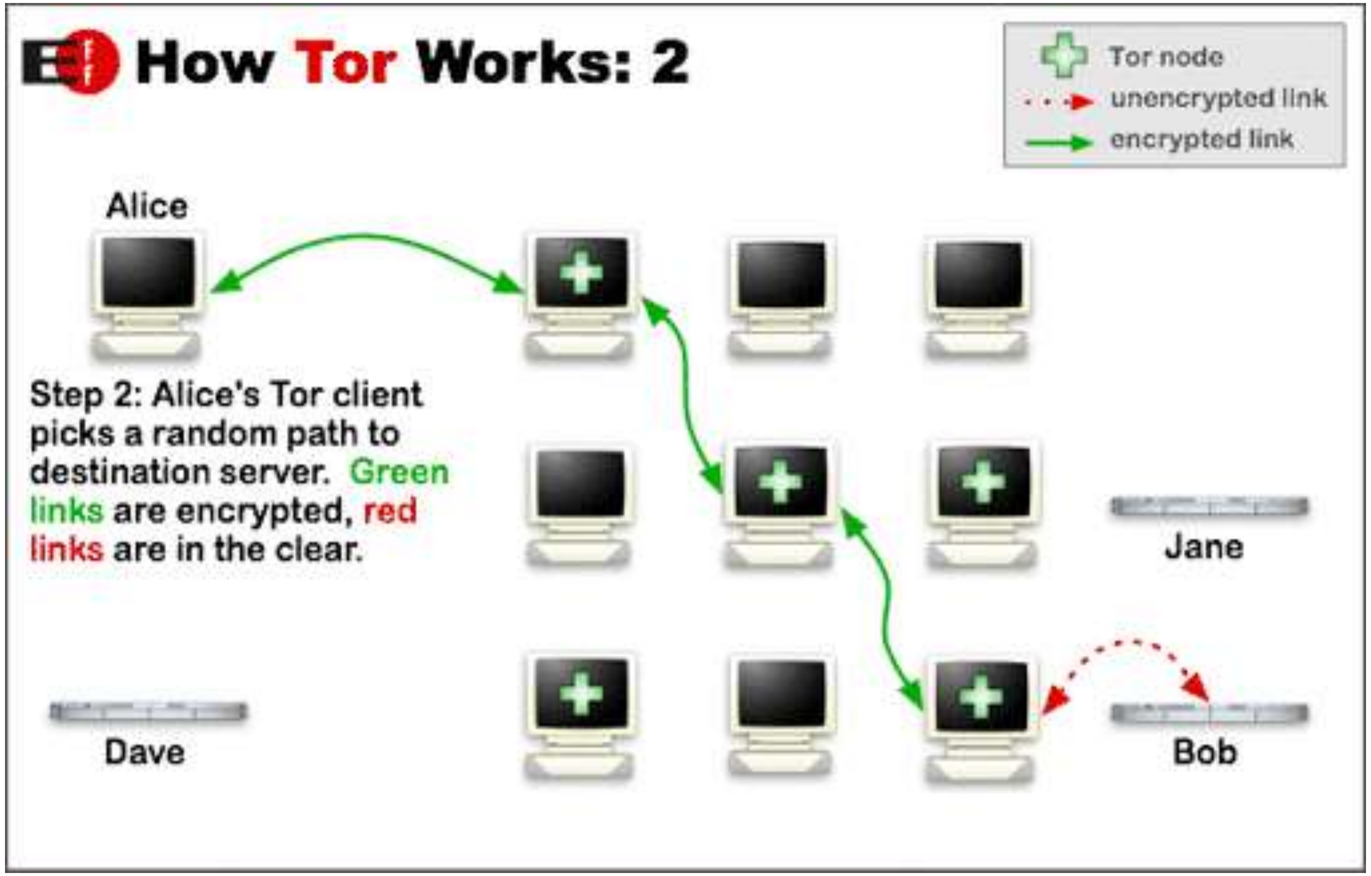
- Types of data relevant to privacy
  - Personally Identifiable Information (PII)
  - Browsing habits and web visits
  - Messages, Emails, etc.
  - Shopping and financial information
  - Medical information
- Data management is at the heart

Tor Anonymity Network


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

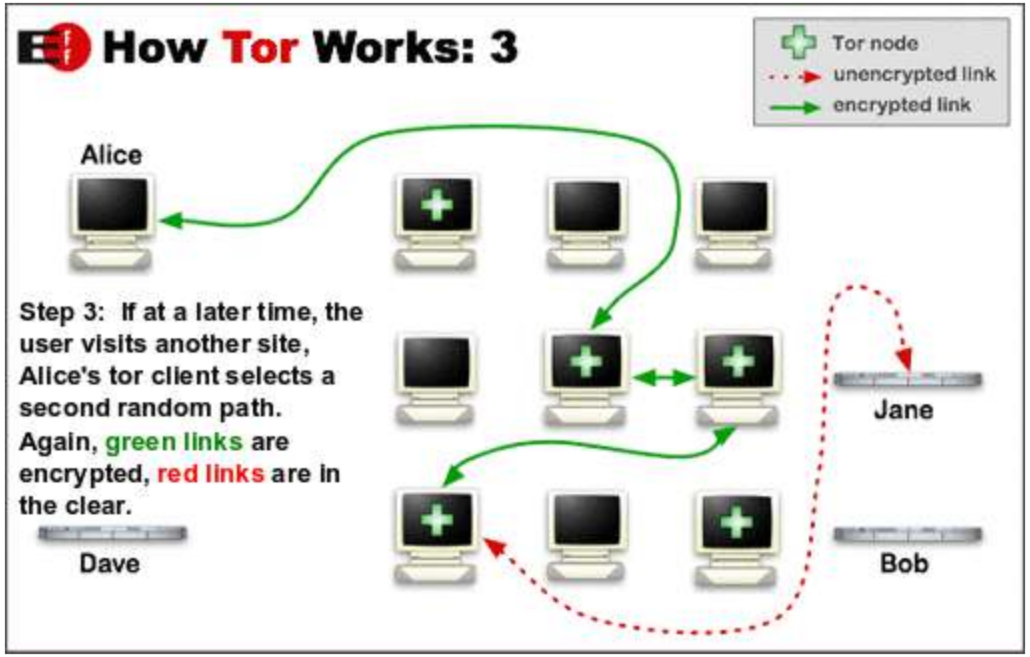
https://2019.www.torproject.org/about/overview.html.en

Tor Anonymity Network



Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

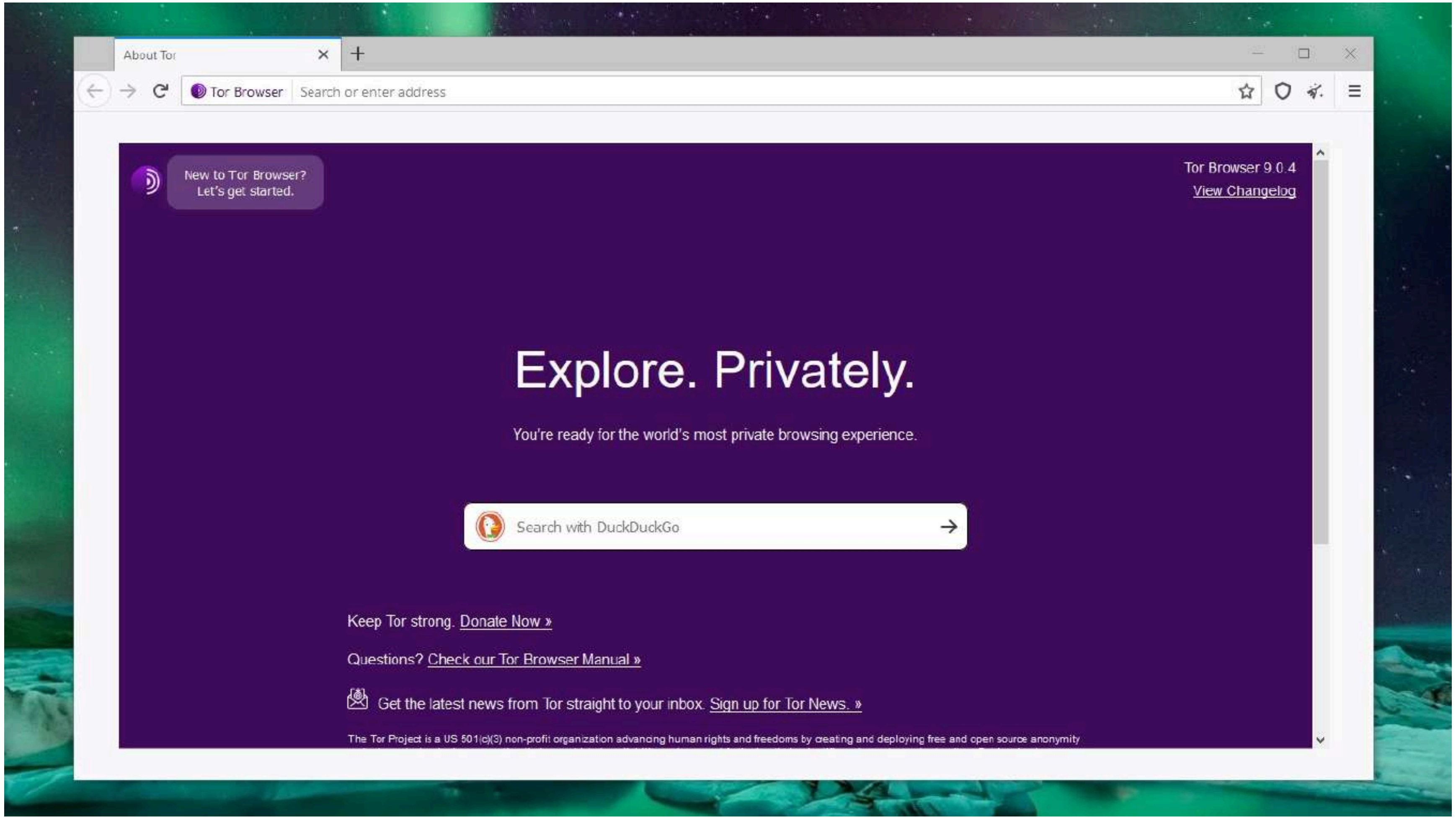
Tor Anonymity Network



How Tor Works: 3

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.

Tor Browser



Tor Browser 9.0.4
View Changelog

Explore. Privately.

You're ready for the world's most private browsing experience.

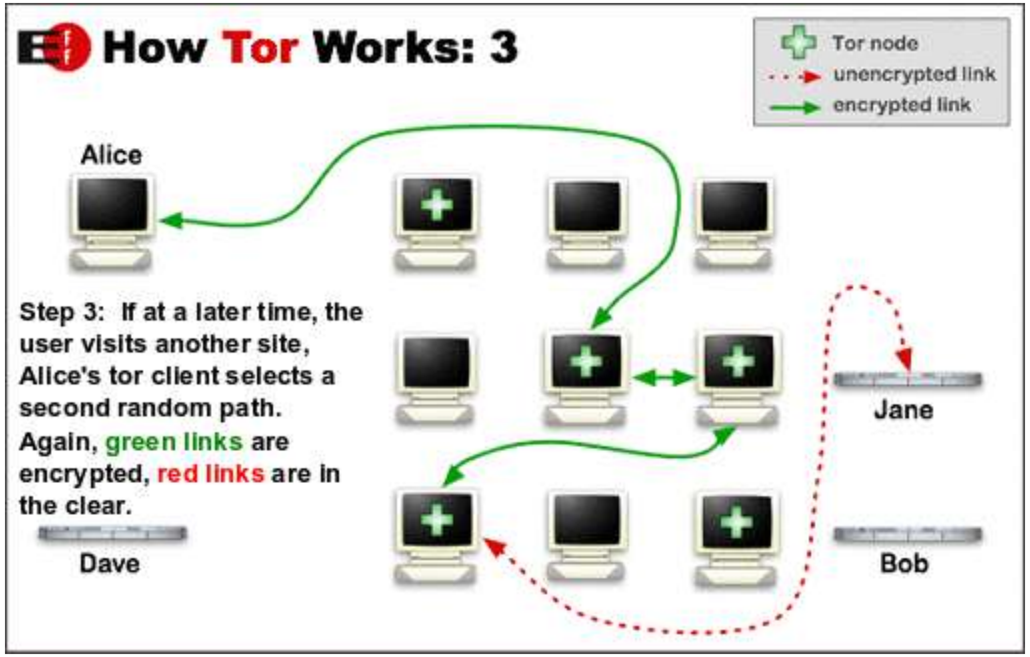
Keep Tor strong. Donate Now »

Questions? Check our Tor Browser Manual »

Get the latest news from Tor straight to your inbox. Sign up for Tor News. »

The Tor Project is a US 501(c)(3) non-profit organization advancing human rights and freedoms by creating and deploying free and open source anonymity

Tor: Leakage from DNS Request



How Tor Works: 3

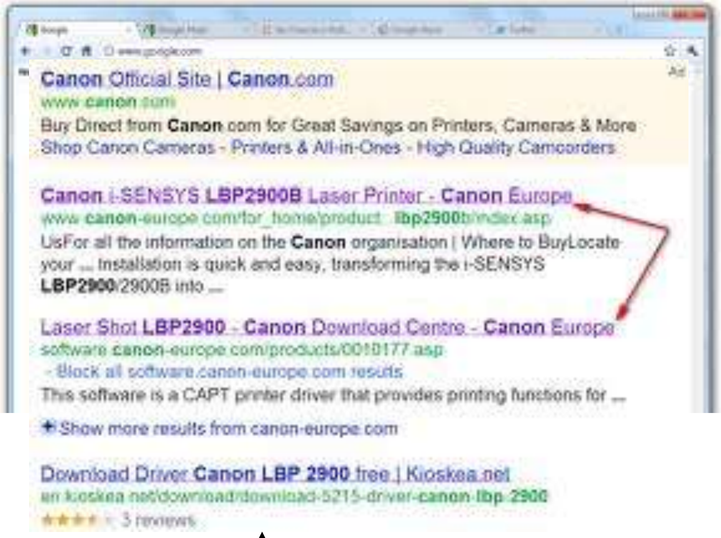
Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

VPN and Public Wifi

- What are the threat model?
  - What data is visible to whom?
  - Encryption vs. plain text
- Learn to trace the data through the life cycle in the web infrastructure to have a clear understanding of the threat model.

Browser History Sniffing

- Stealing browsing history



www.google.com

Ad

Canon Official Site | Canon.com
www.canon.com
Buy Direct from Canon.com for Great Savings on Printers, Cameras & More
Shop Canon Cameras - Printers & All-in-Ones - High Quality Camcorders

Canon i-SENSYS LBP2900B Laser Printer - Canon Europe
www.canon-europe.com/for_home/product...lbp2900b/index.asp
UsFor all the information on the Canon organisation | Where to BuyLocate your ... Installation is quick and easy, transforming the i-SENSYS LBP2900/2900B into ...

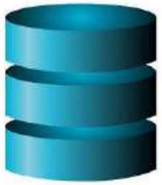
Laser Shot LBP2900 - Canon Download Centre - Canon Europe
software.canon-europe.com/products/0010177.asp
- Block all software.canon-europe.com results
This software is a CAPT printer driver that provides printing functions for ...

Show more results from canon-europe.com

Download Driver Canon LBP 2900 free | Kioskea.net
en.kioskea.net/download/download-5215-driver-canon-lbp-2900
★★★★ 3 reviews

getComputedStyle()

X

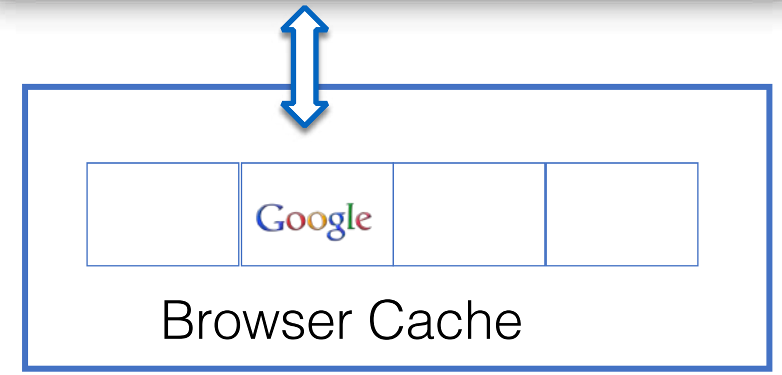


Browsing History

https://blog.mozilla.org/security/2010/03/31/plugging-the-css-history-leak/

Benefits of Browser Cache

https://www.google.com.sg
+You
Gmail
Images
Sign in
Google
Singapore
Google Search
I'm Feeling Lucky
Google.com.sg offered in: 中文(简体) Bahasa Melayu தமிழ்



Browser Cache

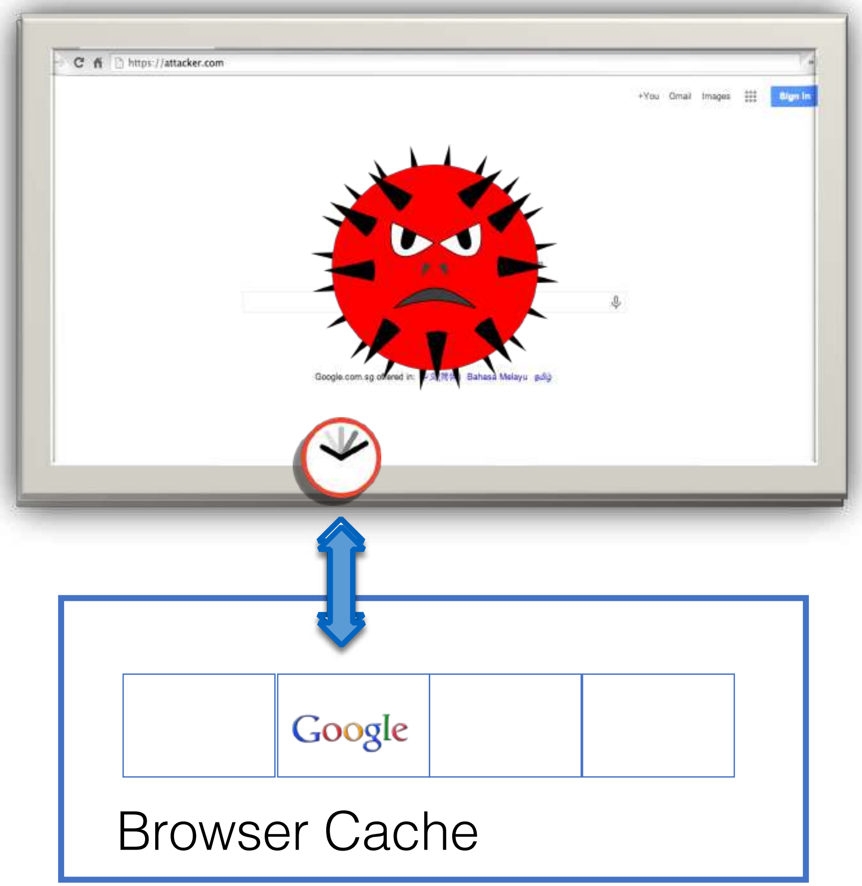
1st: 1360ms

2nd: 320ms

3rd: 350ms

Save Time

Timing Channels via the Browser Cache


https://attacker.com
+You Gmail Images Sign in
Google.com.sg offered in Bahasa Melayu
Google

Browser Cache

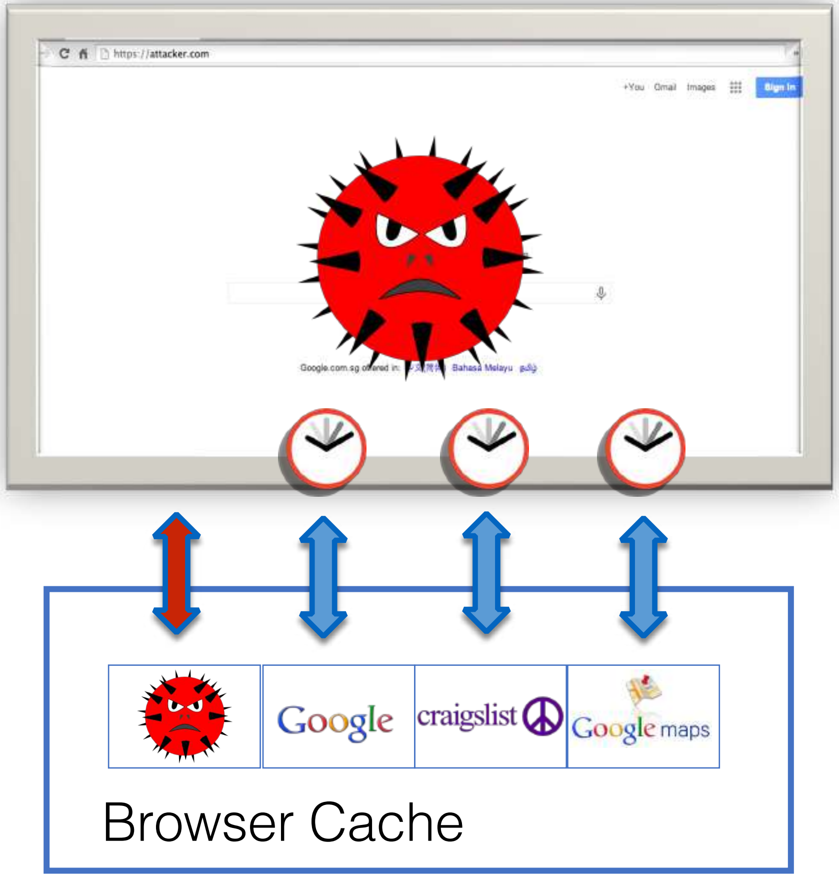
1st: 1360ms

2nd: 320ms

3rd: 350ms

Geo-Inference Attacks via the Browser Cache

Browser cache
is shared
across all sites



Browser Cache

Infer users'
geo-locations!

geo-oriented resources

Measuring Image Load Time

Before Loading

img.onload Fires

```
var image = document.createElement(`img');
image.setAttribute(`startTime', (new
Date().getTime()));
image.onload = function()
{
    var endTime = new Date().getTime();
    var loadTime = endTime -
parseInt(this.getAttribute(`startTime'));
    ......
}
```

attacker.com

How to Infer a User’s Neighborhood?

Google maps

https://www.google.com.sg/maps/vt/pb=
!1m5!1m4!1i15!2i12627!3i23720!4i128!2m1!1e0!3m3!5e1105!12m1!1e47!4e0

Predictable URLs

(12627, 23720)

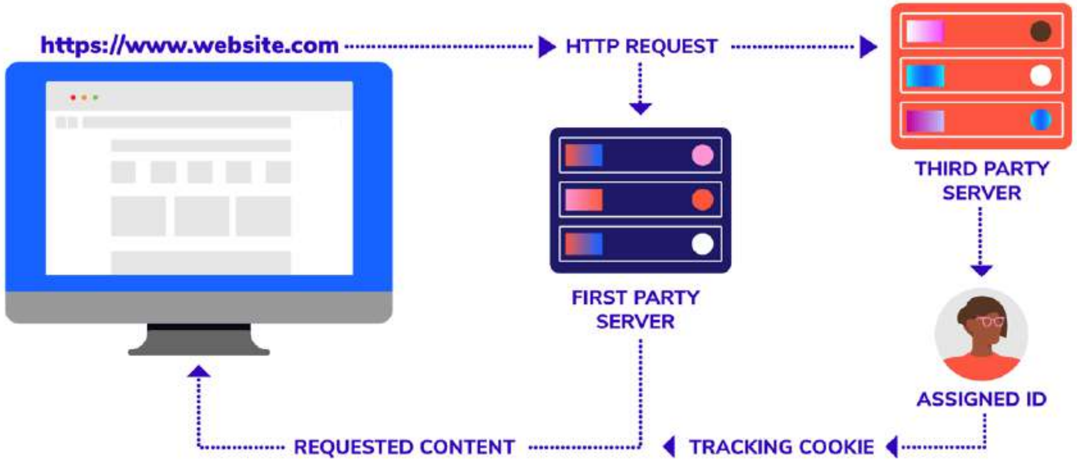
Grand Loop Rd, Yellowstone National Park, WY
82190, USA

Map
Tiles

Kent Ridge Rd
National University
of Singapore School
of Computing
NUS Faculty of Arts
and Social Sciences
Research Link
NUS Department
of Engineering
Kent Ridge Dr
NUS
Business
School
Institute Of
Materials R

Web Tracking

- Web tracking is based on third-party cookie



- Mobile tracking can use more device information

Private Browsing Mode

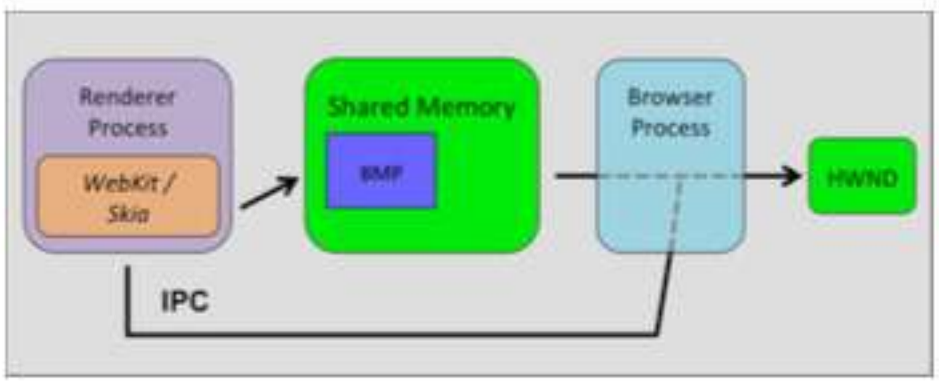
- Clear cookies when browser starts
  - Disable tracking by cookies
- Tracking is to identify users
  - Can users be directly identified?
  - Browser fingerprinting
    - Browser size, extra fonts, extensions/plugins, hardware information

Browser Fingerprinting

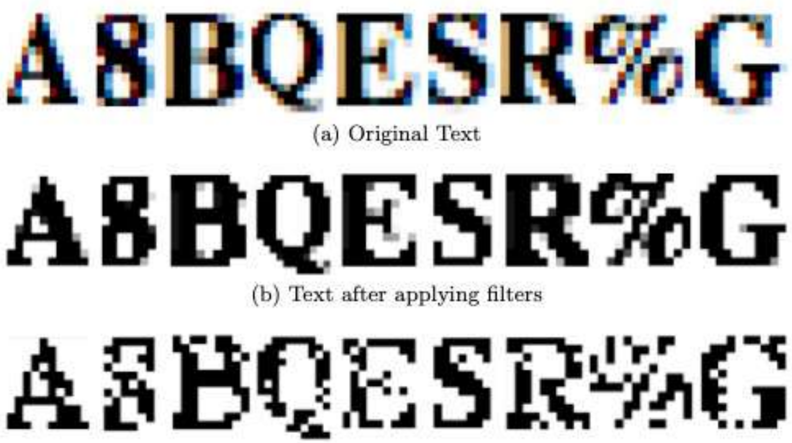
- Guest lecture by Brave
  - Fingerprinting and Privacy on the Web https://web.stanford.edu/class/cs253/lectures/Lecture%2008.pdf

Side-Channel Probing in Browsers

- CSS blur filter can be applied to web images
  - Different timing!



- Text can be stolen by pages in other origins.



(a) Original Text

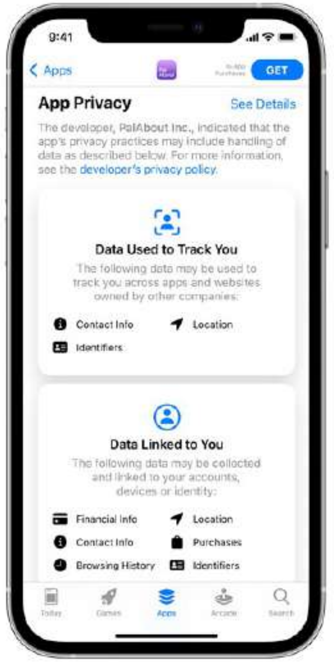
(b) Text after applying filters

(c) Stolen Text

Resources Control on Mobile

- Resources
  - Files
  - Photos
  - Camera/Microphone
  - Location
  - Sensors
  - …
- Apple's privacy updates
  - Explicit confirmation on tracking
  - Privacy labels for apps

- Major pushback from Internet companies



App Privacy See Details

The developer, PalAbout Inc., indicated that the app's privacy practices may include handling of data as described below. For more information, see the developer's privacy policy.

Data Used to Track You

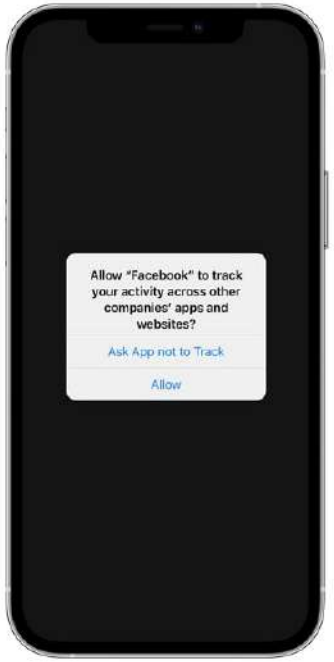
The following data may be used to track you across apps and websites owned by other companies:

Contact Info
Location
Identifiers

Data Linked to You

The following data may be collected and linked to your accounts, devices or identity:

Financial Info
Location
Contact Info
Purchases
Browsing History
Identifiers

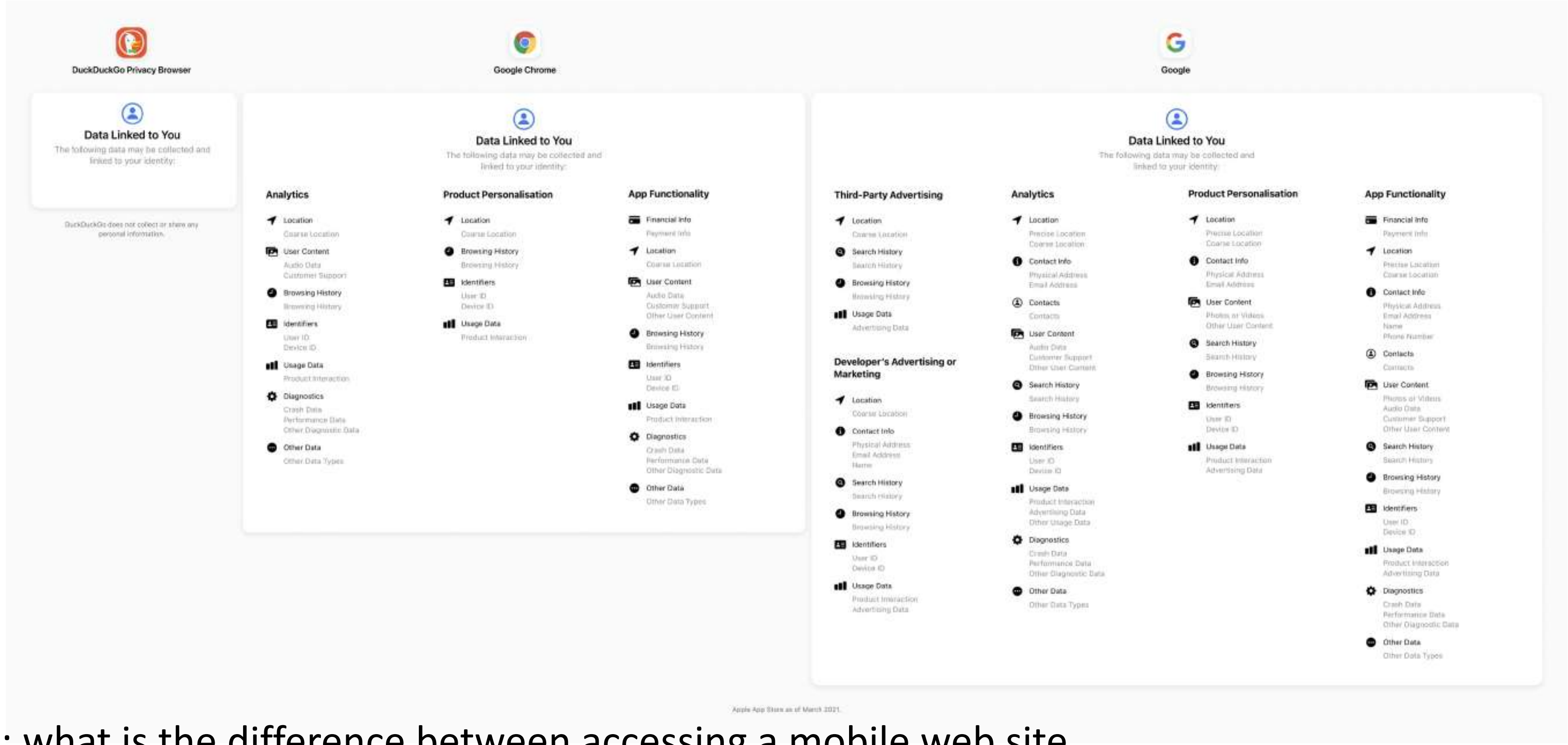


Allow "Facebook" to track your activity across other companies' apps and websites?

Ask App not to Track

Allow

Mobile App Privacy Labels



DuckDuckGo Privacy Browser

Data Linked to You

The following data may be collected and linked to your identity:

DuckDuckGo does not collect or share any personal information.

Google Chrome

Data Linked to You

The following data may be collected and linked to your identity:

Analytics

- Location
  - Coarse Location
- User Content
  - Audio Data
  - Customer Support
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
- Diagnostics
  - Crash Data
  - Performance Data
  - Other Diagnostic Data
- Other Data
  - Other Data Types

Product Personalisation

- Location
  - Coarse Location
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction

App Functionality

- Financial Info
  - Payment Info
- Location
  - Coarse Location
- User Content
  - Audio Data
  - Customer Support
  - Other User Content
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
- Diagnostics
  - Crash Data
  - Performance Data
  - Other Diagnostic Data
- Other Data
  - Other Data Types

Google

Data Linked to You

The following data may be collected and linked to your identity:

Third-Party Advertising

- Location
  - Coarse Location
- Search History
  - Search History
- Browsing History
  - Browsing History
- Usage Data
  - Advertising Data

Developer's Advertising or Marketing

- Location
  - Coarse Location
- Contact Info
  - Physical Address
  - Email Address
  - Name
- Search History
  - Search History
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
  - Advertising Data

Analytics

- Location
  - Precise Location
  - Coarse Location
- Contact Info
  - Physical Address
  - Email Address
- Contacts
  - Contacts
- User Content
  - Audio Data
  - Customer Support
  - Other User Content
- Search History
  - Search History
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
  - Advertising Data
  - Other Usage Data
- Diagnostics
  - Crash Data
  - Performance Data
  - Other Diagnostic Data
- Other Data
  - Other Data Types

Product Personalisation

- Location
  - Precise Location
  - Coarse Location
- Contact Info
  - Physical Address
  - Email Address
- User Content
  - Photos or Videos
  - Other User Content
- Search History
  - Search History
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
  - Advertising Data

App Functionality

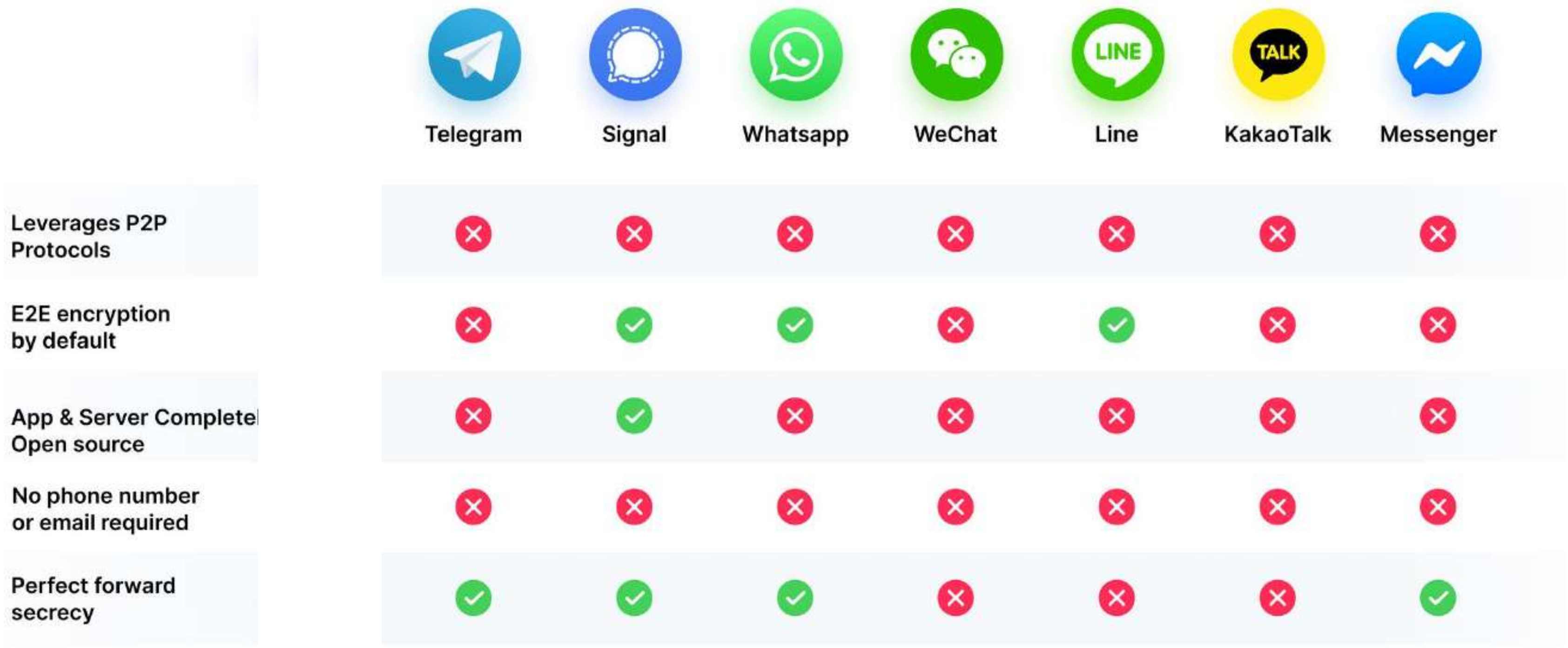
- Financial Info
  - Payment Info
- Location
  - Precise Location
  - Coarse Location
- Contact Info
  - Physical Address
  - Email Address
  - Name
  - Phone Number
- Contacts
  - Contacts
- User Content
  - Photos or Videos
  - Audio Data
  - Customer Support
  - Other User Content
- Search History
  - Search History
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
  - Advertising Data
- Diagnostics
  - Crash Data
  - Performance Data
  - Other Diagoodic Data
- Other Data
  - Other Data Types

Apple App Store as of March 2021.

Question: what is the difference between accessing a mobile web site and running its app on phones.

Source: https://twitter.com/DuckDuckGo/status/1371509053613084679

Messenger App Privacy



	Telegram	Signal	Whatsapp	WeChat	Line	KakaoTalk	Messenger
Leverages P2P Protocols	✗	✗	✗	✗	✗	✗	✗
E2E encryption by default	✗	✓	✓	✗	✓	✗	✗
App & Server Completel Open source	✗	✓	✗	✗	✗	✗	✗
No phone number or email required	✗	✗	✗	✗	✗	✗	✗
Perfect forward secrecy	✓	✓	✓	✗	✗	✗	✓

Identifying User Accounts

- If I know your twitted at a few time points, how likely can I obtain your identify in Twitter's records.
  - High-order vector matching
  - Can uniquely locate a user with 6 – 10 distinct time points.

User1	0	1	0	0	…	1	…	0
User2	1	0	1	0	…	1	…	0
Target	?	?	1	?	…	1	…	?

- How to obtain the time points of twits?
  - Network activity can be monitored by apps from /proc of Android without permission.

Route Identification

- Can you identify routes without using GPS?
    - Speaker will be on when there is a turn.

User1	0	1	0	0	…	1	…	0
User2	1	0	1	0	…	1	…	0
Target	?	?	1	?	…	1	…	?

Summary

- Beyond Web, from the system angle
  - IoT Security
  - Web3?
- Privacy vs. Security
  - Subtle and more difficult to decide
  - Anonymity network
  - Fingerprinting
  - Mobile privacy