FANSHAWE

INFO-6076

Web Security

Social Media & The Dark Web

Agenda

- Social Media
- Terms of Service
- Social Media Attacks/Data
- Mobile Users
- Clearnet vs. Deep web vs. Darknet
- The Onion Router (TOR)
- Lab 11 Overview

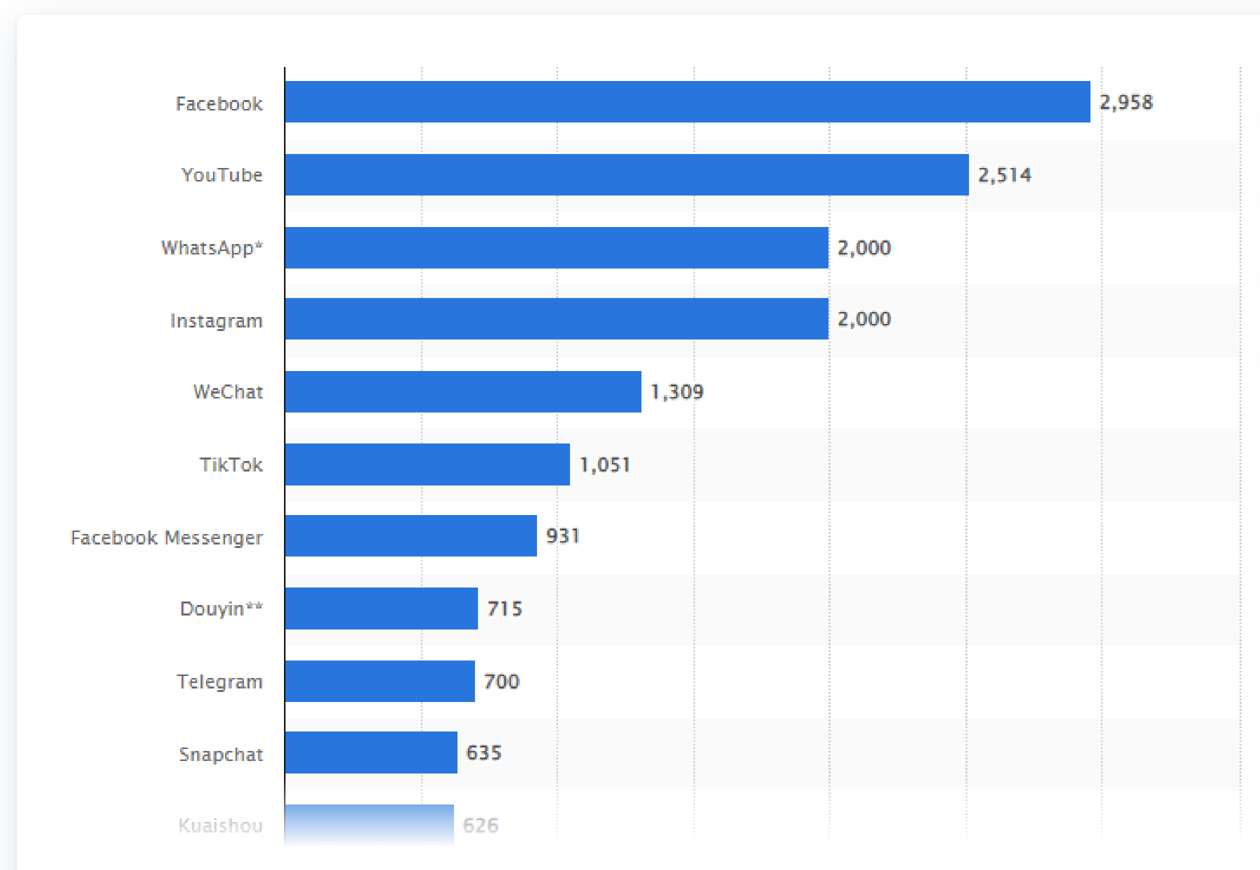
Get Social…

Social Media

Social Media

- How many of you use Social Media?
- How do you use it?
  - Desktop / Laptop
  - Tablet
  - Mobile Phone
  - Smart TV
  - Smart watch

Most popular Social Networks (Jan 2023)



https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Social Media

- How much did you have to pay to use these social media platforms?
- Did it cost you to download their “App” onto your mobile device?
- Are their programmers working for free to provide you with an extensive web application at no cost?
- How do they make a living?

Social Media

- You are posting information about yourself on various social media platforms
- In addition to this, your friends and family may be posting information about you (with or without your knowledge or approval)
- This could be as simple as inputting your contact information or DOB into an application someone has to track their contacts

Social Media

- These social media companies are using their users to give them data that they can turn around and sell
- You are not their customer, but a product
- Some companies use paid surveys to gather information from the public about certain products
- When you post information about companies or their products on social media, this information now belongs to the social media platform and can be sold to third parties

Social Media

- What if you email your friend from your private email address (College or work email) to their Gmail account?
- Does Google scan emails received or sent by their Gmail (free email) service?
- Can this information be used by Google to advertise products to you?

Social Media

What Google has said about this…

“a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”

http://www.cnet.com/news/google-filing-says-gmail-users-have-no-expectation-of-privacy/

Social Media

What is your privacy and data worth?

- Alphabet’s market cap is at over $1.3 Trillion

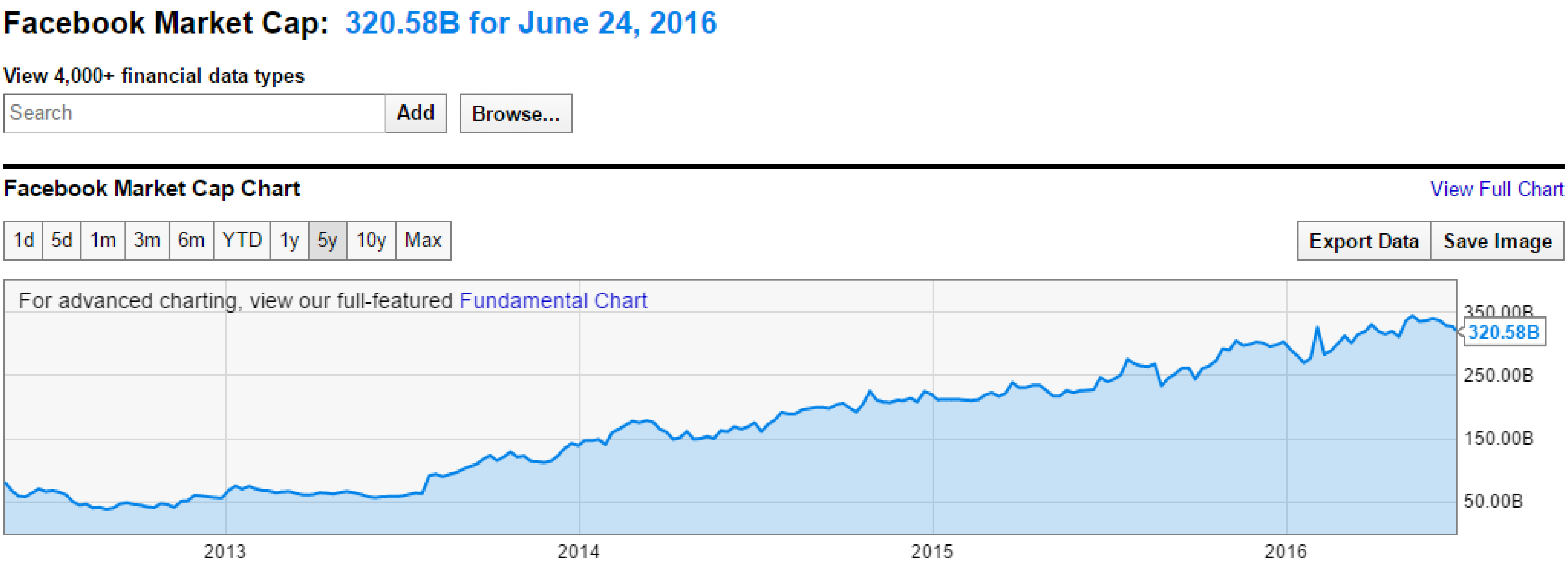
  http://www.nasdaq.com/symbol/goog

- How about other Social Media Platforms?

- What is Facebook worth?

Facebook

- Facebook Market Cap was over $320 Billion (June 2016)



Facebook Market Cap: 320.58B for June 24, 2016

View 4,000+ financial data types

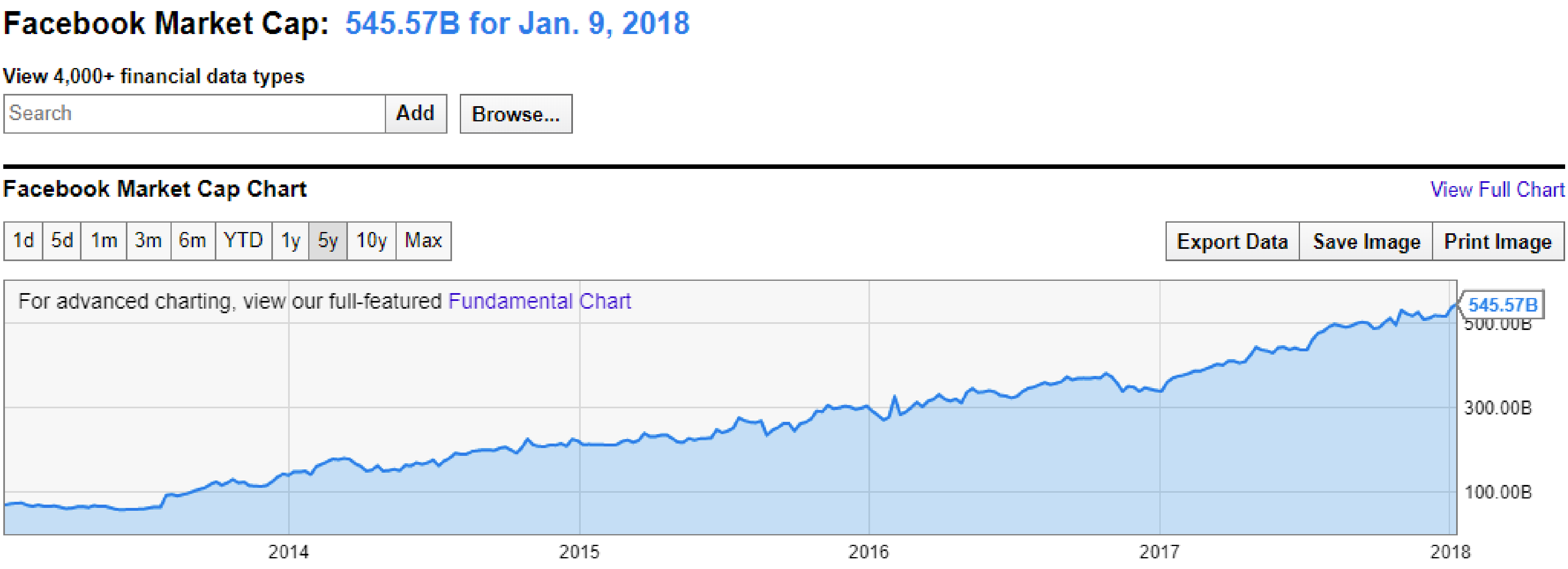
Facebook Market Cap Chart

For advanced charting, view our full-featured Fundamental Chart

https://ycharts.com/companies/FB/market_cap

Facebook

- Facebook Market Cap rose over $545 Billion



Facebook Market Cap: 545.57B for Jan. 9, 2018

View 4,000+ financial data types

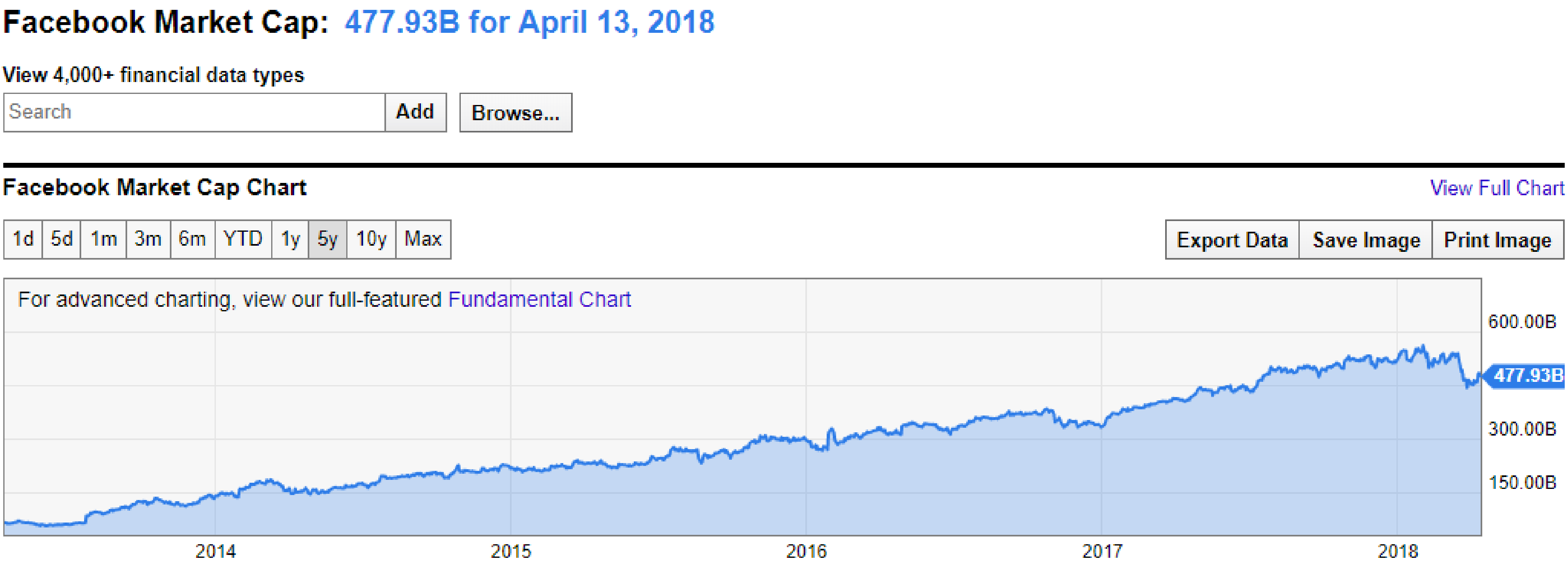
Facebook Market Cap Chart

For advanced charting, view our full-featured Fundamental Chart

https://ycharts.com/companies/FB/market_cap

Facebook

- Facebook Market Cap took a hit (~68 Billion)



Facebook Market Cap: 477.93B for April 13, 2018

View 4,000+ financial data types

Facebook Market Cap Chart

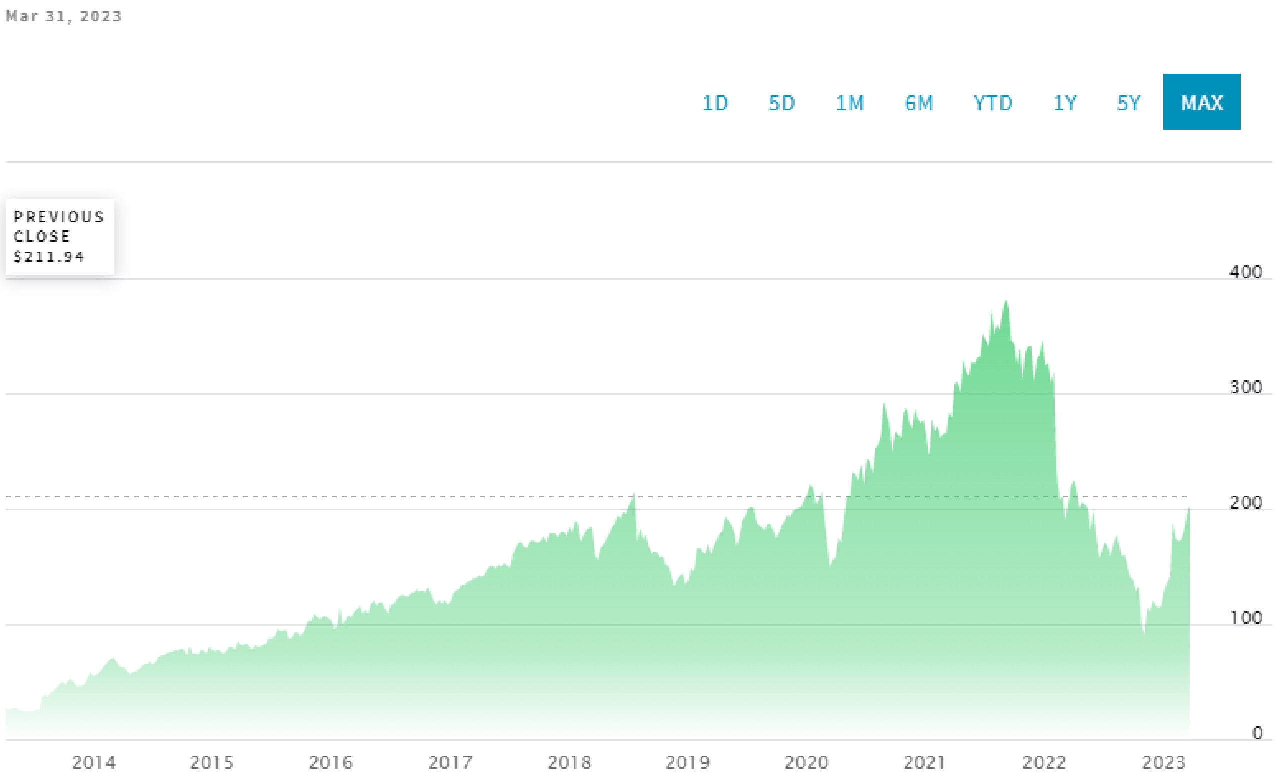
View Full Chart

For advanced charting, view our full-featured Fundamental Chart

https://ycharts.com/companies/FB/market_cap

Meta Platforms Inc

- How are they doing now as META?



Mar 31, 2023

PREVIOUS CLOSE $211.94

Social Media

Who contributes to this value?

http://www.wsj.com/articles/facebook-prods-users-to-share-a-bit-more-1446520723

- Is it you?
- How and why is this happening?

FANSHAWE

Did you read them?

Terms of Service

Terms of Service

I have read and agree to…

- How many times have you read the entire document?
- Do you understand what you are reading?
- These are designed in such a way that most users do not read or understand them
- This is how you agree to forfeit any information you post on the platform you are using

Terms of Service

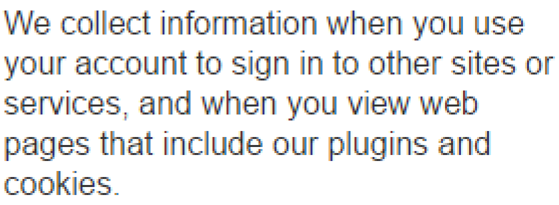
- A study conducted by Carnegie Mellon University concluded that most users do not have the time to read all of the Privacy Policies that they encounter online

http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf

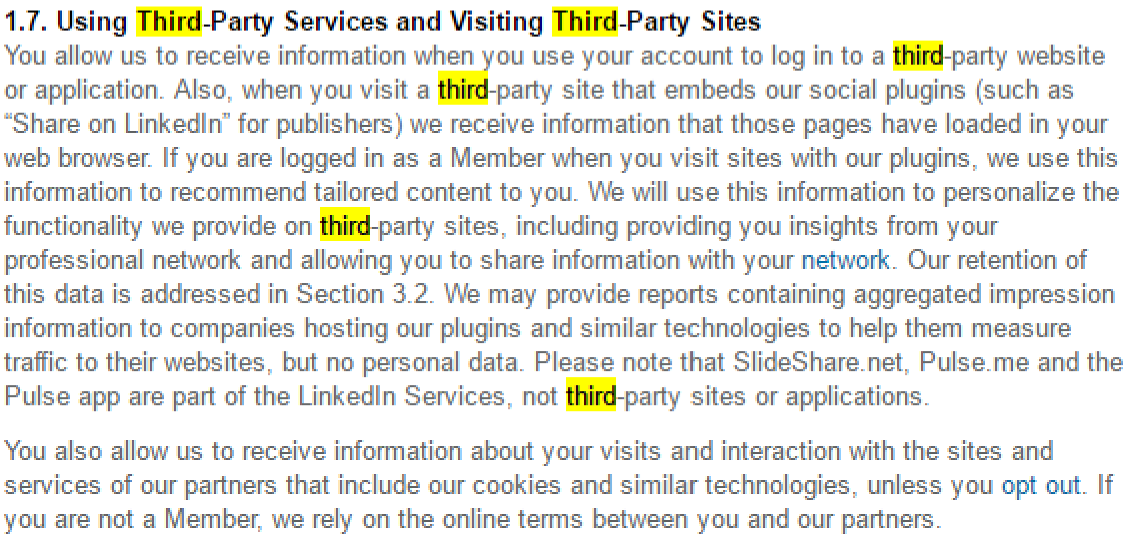
I/S: A Journal of Law and Policy for the Information Society
2008 Privacy Year in Review issue
http://www.is-journal.org/

Terms of Service

- LinkedIN



We collect information when you use your account to sign in to other sites or services, and when you view web pages that include our plugins and cookies.



1.7. Using Third-Party Services and Visiting Third-Party Sites

You allow us to receive information when you use your account to log in to a third-party website or application. Also, when you visit a third-party site that embeds our social plugins (such as “Share on LinkedIn” for publishers) we receive information that those pages have loaded in your web browser. If you are logged in as a Member when you visit sites with our plugins, we use this information to recommend tailored content to you. We will use this information to personalize the functionality we provide on third-party sites, including providing you insights from your professional network and allowing you to share information with your network. Our retention of this data is addressed in Section 3.2. We may provide reports containing aggregated impression information to companies hosting our plugins and similar technologies to help them measure traffic to their websites, but no personal data. Please note that SlideShare.net, Pulse.me and the Pulse app are part of the LinkedIn Services, not third-party sites or applications.

You also allow us to receive information about your visits and interaction with the sites and services of our partners that include our cookies and similar technologies, unless you opt out. If you are not a Member, we rely on the online terms between you and our partners.

https://www.linkedin.com/legal/privacy-policy

Terms of Service

- Companies usually reserve the right to change their privacy policy settings without prior consent of the user
- Your privacy settings on a social media platform may be reset when such changes are applied
  - Might go back to default settings (less secure)
- Do you find it easy to change your privacy settings on Facebook?

How Can They Happen?

Social Media Attacks

Social Media Data

What information have you publically posted about yourself?

- Your home address?
- Your mother’s maiden name?
- Your telephone number?
- Your email?
- Your pet’s name?
- The name of your children?

FANSHAWE

Social Media Data

- Some Social Media platforms claim to reserve the right to sell images you have posted on their platforms
- If you have posted a photograph of your baby, it could be used in advertising
- This is like creating a huge depository of stock images for marketing / advertising companies, magazines, etc.

Social Media

Should I have an account?

- Have you searched yourself online?
- What can you find publicly?

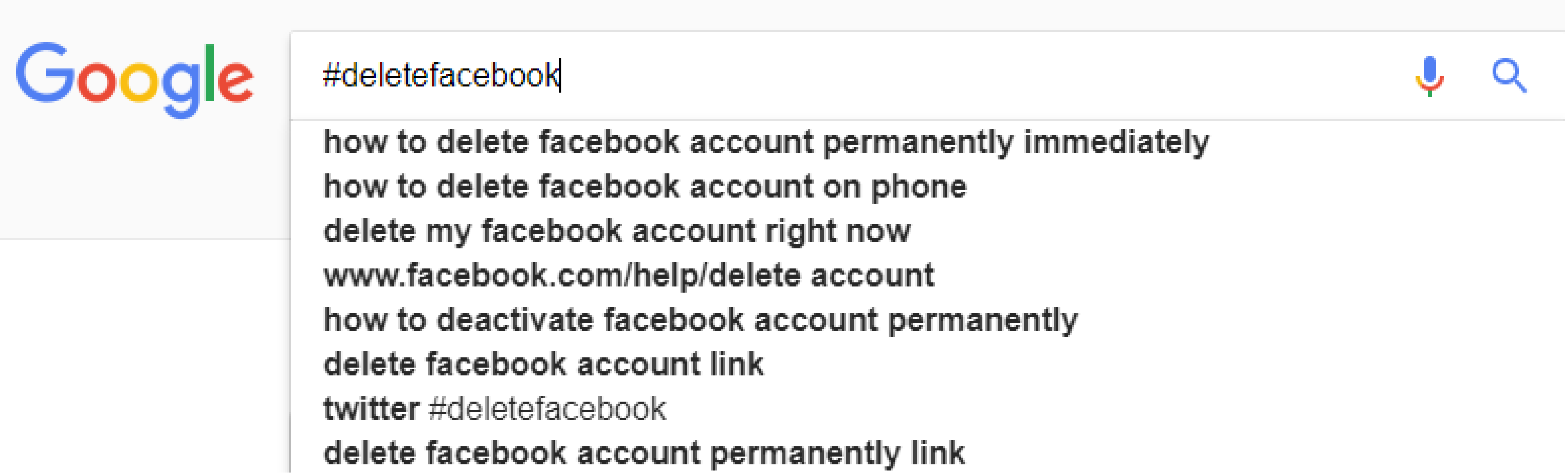
Are you in control of your online image?

- Spoof accounts

https://www.facebook.com/Facecrooks/posts/10151524855310345

#deletefacebook

- Should I have an account?



#deletefacebook

how to delete facebook account permanently immediately
how to delete facebook account on phone
delete my facebook account right now
www.facebook.com/help/delete account
how to deactivate facebook account permanently
delete facebook account link
twitter #deletefacebook
delete facebook account permanently link

Check your “smart” phone lately?

Mobile Users

Mobile Users

- Do you have a smart phone?
- Do you carry it with you everywhere you go?

Do you use it for:

- Games
- Contact Lists
- Texting / Email
- Watching Videos
- Surfing the Web / Social Media / E-Commerce
- Banking
- GPS

Mobile Users

- How often do you use it as a telephone?
- How long can you last without your mobile?

- How much does your mobile device know about you and your activities?
  - Your habits
  - Your location
  - Your communication with others

Mobile Users

Who has access to this information?

- Advertisers
- Spouses
- Governments
- Companies

Mobile Users

What operating system are you using on your smart phone?

How much did this O/S cost you?

Mobile Users

The Android O/S can provide Google with:

- Your mobile phone number
- Storage Data
- Google Account Info
- Call Logs
- Contact Lists
- Location
- Etc.

Mobile Users

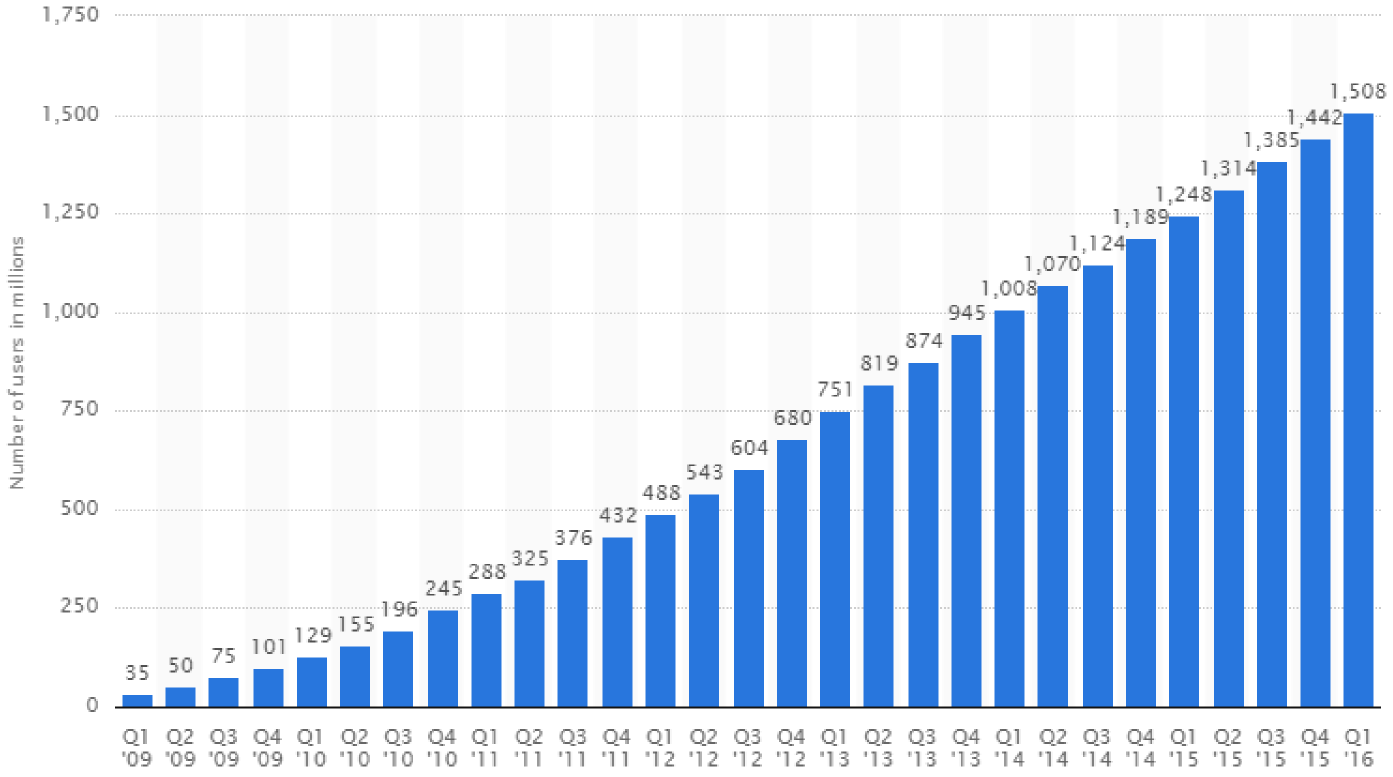
Facebook can listen to your microphone if you have their app installed

- Terms of service!

When they launched the mobile app, their user base surged

- The value of the company soared

Mobile Users on Facebook



© Statista 2016

http://www.statista.com/statistics/277958/number-of-mobile-active-facebook-users-worldwide/

Mobile Users

- According to venturebeat.com most of Facebook's revenue comes from mobile ads:

> "Facebook shared that in Q1 2016, mobile ads accounted for 79 percent of all revenue."

- How much did you pay for your mobile app?

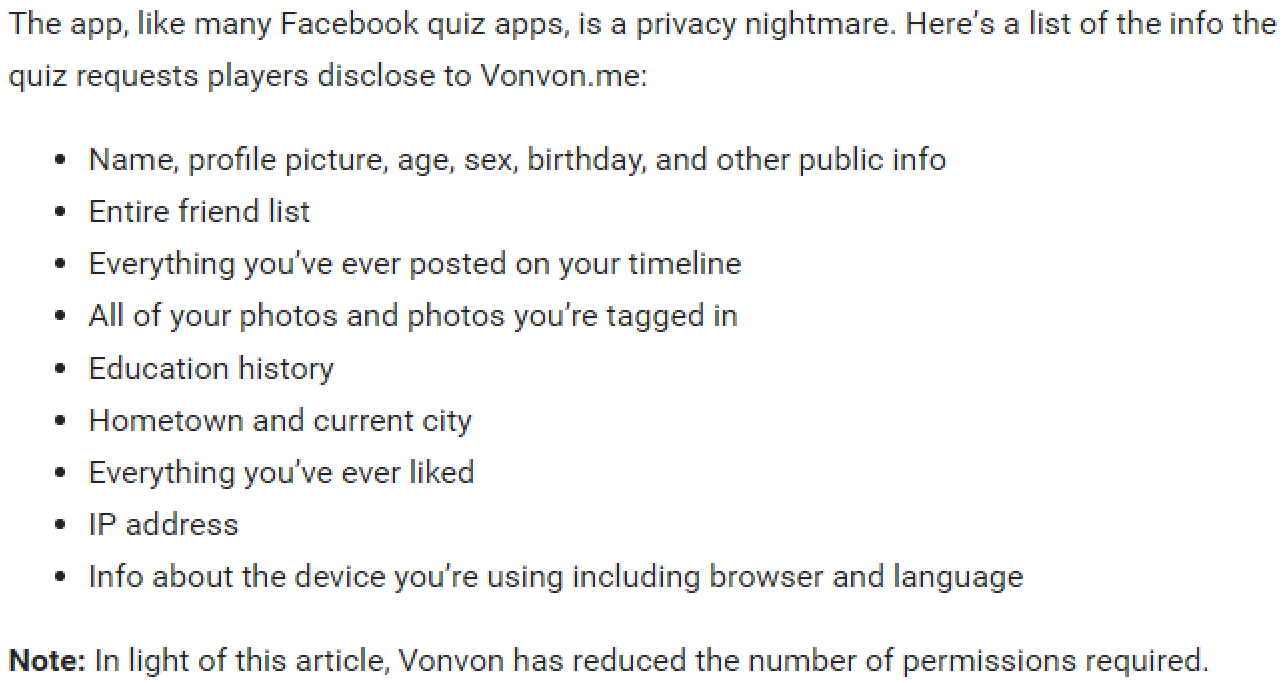
http://venturebeat.com/2016/04/27/facebook-passes-1-65-billion-monthly-active-users-54-access-the-service-only-on-mobile/

Mobile Apps

- What motivates mobile application developers to create apps that are free to download?
- Mobile Apps have become a great way to send over user data to advertisers
- In exchange for downloading and using the app for free, you agree to send your personal information to third parties. How about free games?
  - Angry Birds
  - Candy Crush Saga
  - Clash Royale

Mobile App Example

Facebook quiz: most used words



The app, like many Facebook quiz apps, is a privacy nightmare. Here's a list of the info the quiz requests players disclose to Vonvon.me:

- Name, profile picture, age, sex, birthday, and other public info
- Entire friend list
- Everything you've ever posted on your timeline
- All of your photos and photos you're tagged in
- Education history
- Hometown and current city
- Everything you've ever liked
- IP address
- Info about the device you're using including browser and language

Note: In light of this article, Vonvon has reduced the number of permissions required.

https://www.comparitech.com/blog/vpn-privacy/that-most-used-words-facebook-quiz-is-a-privacy-nightmare/

Mobile App Developers

When you download an app from the online source, you automatically agree to provide some of your personal information to the creators of the app

- What are their privacy policies?
- What do they do with your information?
- Is it secure?

FANSHAWE

Mobile Apps

What protection or regulation is available to you as a consumer?

- Did you agree to the Terms of Service?
  - Angry Birds has been accused of tracking user locations
    - Who was doing the tracking?

http://www.cbsnews.com/news/spies-use-angry-birds-and-other-apps-to-track-people-documents-show/

https://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data

Mobile Users

McAfee Security reports that over 85% of American adult mobile users have an average of 41 apps installed on their smart phones

- Most are tracking your location data

https://blogs.mcafee.com/consumer/apps-tracking-your-location-friendly-or-creepy/

Mobile User Location

- Why is location important?
- What are you looking for?
- Where are you?
- Can it be used for targeted advertising?

http://www.mckinsey.com/business-functions/business-technology/our-insights/big-data-the-next-frontier-for-innovation

Mobile User Location

- How can your location be determined?
  - Your phone's GPS data
  - Your distance between Cell Phone towers
  - WiFi networks you are connecting to

- This data can be stored by numerous apps

Mobile User Location

What happens when you take a picture on your mobile device?

- There is meta data that is stored within the image file:
  - GPS location
  - Coordinates (Longitude / Latitude)
  - Device used to take the picture

The Web

Clearnet vs. Deep Web vs. Darknet

Clearnet

- The Clearnet is what most people use everyday
- This is the regular “internet”
- When you search for sites on Google, you will be presented with results from the Clearnet
- The websites on the Clearnet are meant to be found through the use of regular search engines as their spiders are able to index all of the content

Deepweb

- This is the part of the internet that is typically hidden from or inaccessible by regular users
- Regular internet users are only able to access the "tip of the iceberg"
- Search engines such as Google will not show results for Deepweb sites

Accessing the Deep Web

Google for example, can only index pages that are available to it

Any page that requires authentication is not accessible by Google’s spiders

- Your private banking information
- Hidden Facebook profiles
- Deactivated dating profiles
- Your Private webmail account

Accessing the Deep Web

- It is estimated that 95% of the resources online are considered to be in the Deepweb
- Google has indexed over a trillion pages, but that only accounts for about 5% of available resources
- The sites in the Deepweb are either unavailable due to authentication, or have been restricted by the web servers, etc.

Accessing the Deep Web

Robots.txt

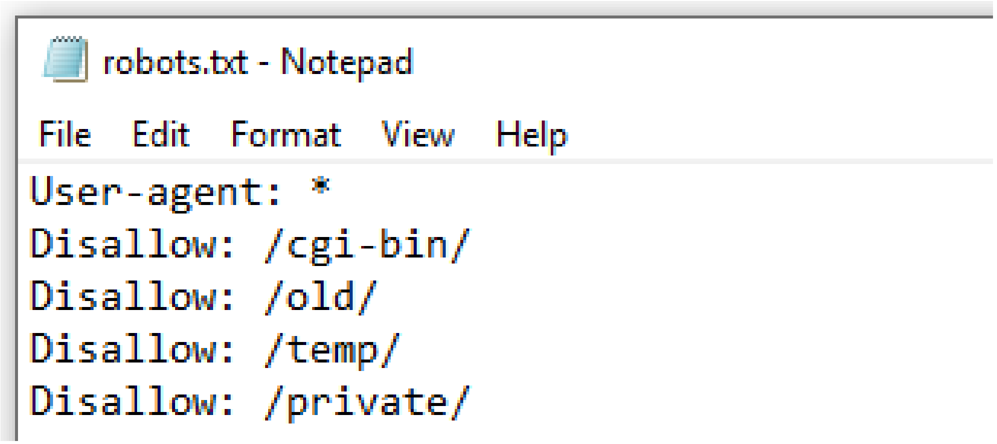
- Also known as the **Robots Exclusion Standard or Protocol**
- Created in 1994, it's purpose was the opposite of site maps, NOT to have a search engine spider or crawler index specified pages on a site
- This is one way of letting any web spider (Google, Yahoo, etc.) know that a page should not be indexed

Accessing the Deep Web

Robots.txt

- It works by specifying which directories and/or files are to be accessible within a web server's directory structure to specified robots

Example:

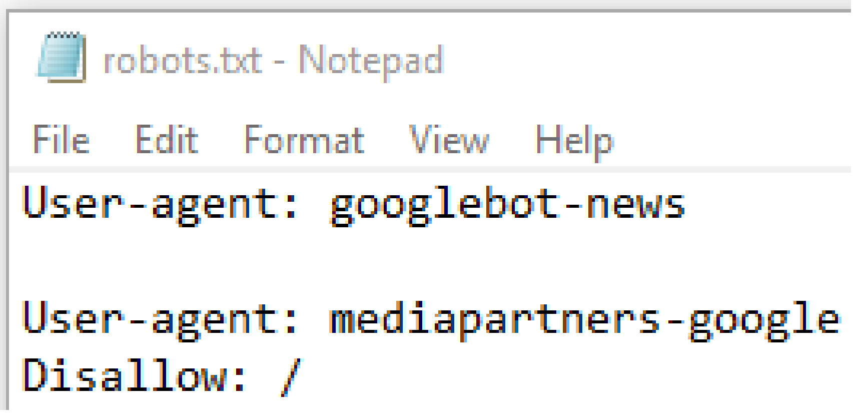


```
User-agent: *
Disallow: /cgi-bin/
Disallow: /old/
Disallow: /temp/
Disallow: /private/
```

Accessing the Deep Web

Robots.txt

- In an ideal world, you can specify which crawler you want to access what resources
- For example, you may want to have Google's News crawler read a certain page, but not allow their Adsense bot to crawl the page



```
User-agent: googlebot-news

User-agent: mediapartners-google
Disallow: /
```

Accessing the Deep Web

Robots.txt

- Different search engines support different components of this de facto standard
- Although most major search engines will adhere to the robots.txt file, they may not acknowledge some of the contents within them like the **allow** directive

Example:

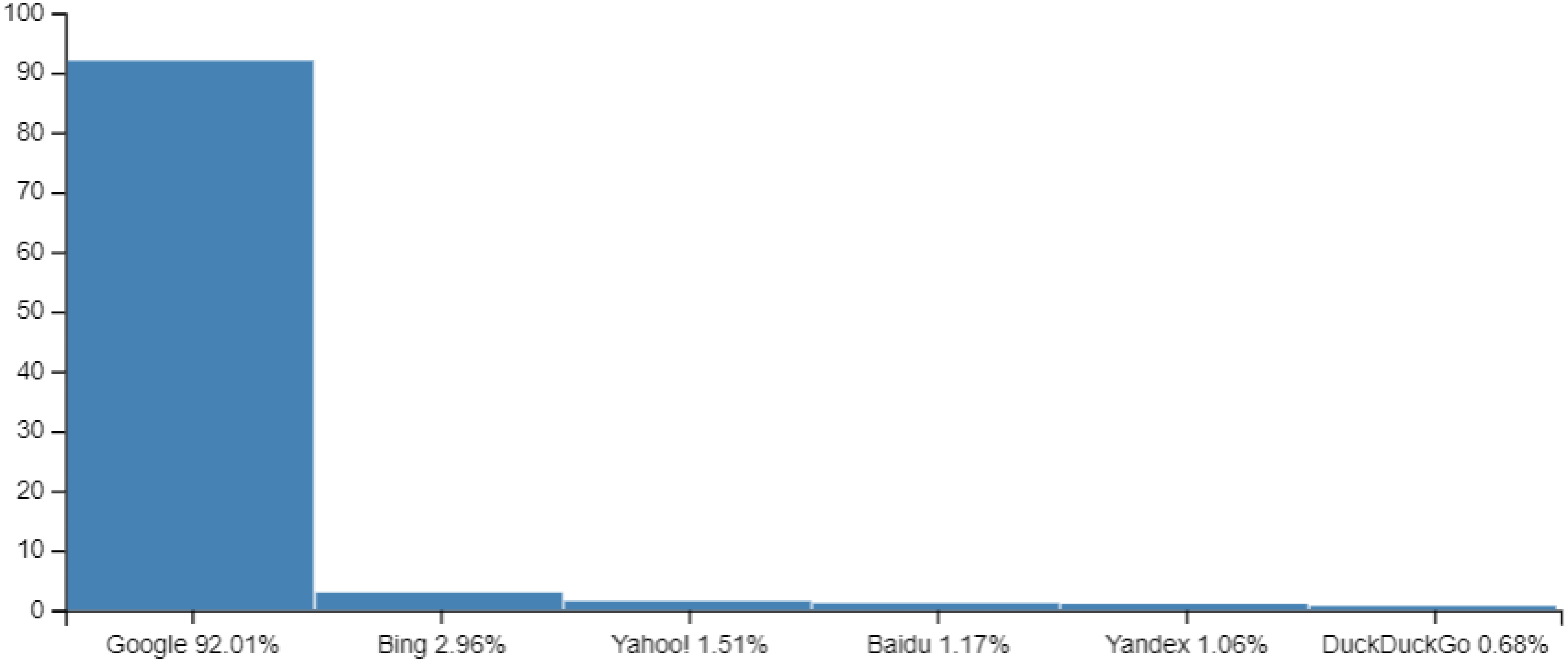
- Allow: /emaildirectory/contactus.html
- Disallow: /emaildirectory/

Accessing the Deep Web

Robots.txt

- Although these methods allow Search Engines to crawl and index different resources and information, it only works for legitimate crawlers
- Malicious crawlers will typically go to the robots.txt file right away, and start from there
- Most legitimate sites can be compromised or may find vulnerabilities in the pages and files listed as disallow in the document

Search Engine popularity



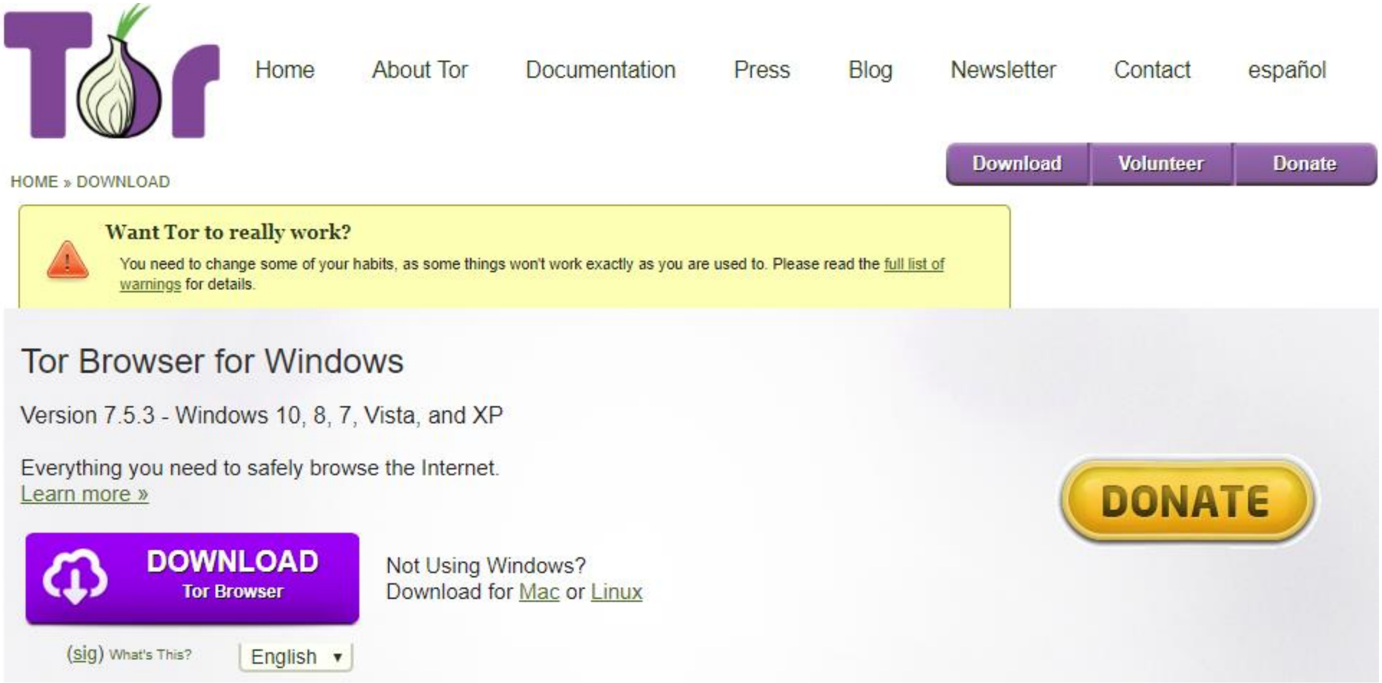
https://en.wikipedia.org/wiki/Search_engine

Darknet

- Although much of the Deepweb is inaccessible to web crawlers/spiders, that still makes up a large portion of the internet that is available to Search Engines like Google but restricted due to authentication
- The Darknet or Darkweb, is another story… most of these sites are “hidden” from the rest of the internet

Darknet - TOR

- The Onion Router (TOR) is a browser specifically designed to access resources located on the Darknet



Want Tor to really work?

You need to change some of your habits, as some things won't work exactly as you are used to. Please read the full list of warnings for details.

Tor Browser for Windows

Version 7.5.3 - Windows 10, 8, 7, Vista, and XP

Everything you need to safely browse the Internet.
Learn more »

Not Using Windows?
Download for Mac or Linux

Darknet - TOR

- It was originally designed by the U.S. Navy to conceal communications
- Websites accessible by TOR include .onion domains
- You can download the TOR browser here:

https://www.torproject.org

The Onion Router

- The TOR network uses **nodes** to route traffic
- Each node only decrypts the information it needs to route the traffic further towards it's next destination
- This is supposed to prevent the node from knowing the source or destination of the traffic
- An **exit node** is used at the end to send the traffic to it's final destination

The Onion Router

- There is an inherent issue with the fact that anyone can run an exit node and read the traffic
- Users can work around this issue by using the TOR browser (a modified version of Firefox that attempts to use HTTPS for all traffic)
- Another layer of security is using a VPN tunnel
  - This is only secure if you can trust the VPN provider to not log your activity

Accessing the Darknet

In addition to the network, it is best practice to include the following when accessing the darknet:

- A “reasonably” secure Operating O/S
  - ✓ Qubes OS
  - ✓ Tails OS
  - ✓ Kali Linux OS
- Using a Virtual Machine
- Anti-Virus

Accessing the Darknet

TOR Hidden Services

- Most of the activities on the TOR network are just users trying to be anonymous
- Keeping that in mind, there are also activities on the dark web that are illegal
  - Drug sales
  - Illegal Pornography
  - Weapon sales
  - Etc.

Accessing the Darknet

Any where on the internet that "hides" traffic or has a lack of accountability will have criminal activity

- Think of technologies such as Bitcoin… it may be used for legitimate purposes, but due to it's anonymity, it will also attract users who are looking to engage in illegal activities

Accessing the Darknet

Hidden Services

- These allow for two-way anonymity
- The Client and the Server do not know each other’s IP address
- Servers will have a .onion hostname and all the traffic will be routed across the TOR network

Accessing the Darknet

Hidden Services

- Servers hosting hidden services need to be properly configured
- These services should be listening only on a localhost address (127.0.0.1)
- Access from the internet should not be available

Accessing the Darknet

Hidden Services

- Servers hosting hidden services should not disclose any identifying information such as software type or version

- If any other resources are being accessed by the server (DNS, etc.), ensure that all that traffic is also routed through the TOR network
  - IPtables to force traffic routing
  - TOR SOCKS Proxy

Accessing the Darknet

Hidden Services

- Multiple ports can be used for each hidden (onion) service
- SSL/TLS is not required, but can add to the layers of the *onion*
- Error messages and the HTTP referer headers may expose the location of a server

Accessing the Darknet

Hidden Services

- Attackers may use Server Side Request Forgery (SSRF) attacks to perform external connections such as a DNS lookup to expose the server’s location
- Egress filtering should be applied to ensure that no external connections are allowed

Accessing the Darknet

Hidden Services

- Bad relays in the TOR network may expose a server’s location
- Onion services should not be hosted on one machine for too long as patterns can be enumerated
- OnionScan can be used to check for information leaks

  https://onionscan.org

Darknet – Other Browsers

There are a number of other browsers that can be used to access sites on the Darknet

- The following link has more information

https://www.airsassociation.org/airs-articles/11-best-illegal-search-engines-to-browse-the-darknet#

Lab Details

LAB-11: Overview

Lab-11: Social Media & TOR

- Social Media searches
- Create a robots.txt file
- Using TOR
- Configure a server for hidden services