**Lab 11: Online Privacy and Anonymity**

**Part 1: Check Out Your Data**

Several major companies allow you to check out and examine the data they have on file for you. This can be very revealing

[Use this link](https://www.makeuseof.com/tag/make-backups-online-social-media-accounts-windows/) to learn how to download your data from one or more of the following services:

* Facebook (highly recommended)
* Instagram
* Google (If you use Gmail or Google Drive, note that downloads can be large)
* Instagram
* LinkedIn
* Pinterest
* Twitter

Alternatively, see the links below to download your data from these companies:

* [Amazon](https://www.usatoday.com/story/tech/columnist/saltzman/2018/04/04/amazon-and-alexa-know-whole-lot-you-heres-how-download-and-delete-info/482286002/)
* [Apple](https://support.apple.com/en-us/HT208502)
* [Snapchat](https://support.snapchat.com/en-US/a/download-my-data)

If you aren’t a customer for any of the above companies, try to check out your data for another company you use.

**Question**: What service did you download data for?

**Question**: What type of information did you find about yourself?

**Question**: Did anything you see in the data about yourself surprise you?

**Part 2: Visualize Web Trackers**

Install the Firefox Lightbeam browser add-on (if needed, first install Firefox) to visualize how web-tracking companies monitor your browsing behavior.

1. Install Lightbeam at:

<https://addons.mozilla.org/en-US/firefox/addon/lightbeam/>x

1. Open the Lightbeam tab by selecting **Show Lightbeam** from the **Tools** menu. Browse around the web visiting sites you typically frequent.

**Question**: How many connections between sites via third-party trackers do you see after browsing 10 popular sites?

**Part 3: Turn on Do Not Track in your Web Browser**

Turn on Do Not Track in your web browser.

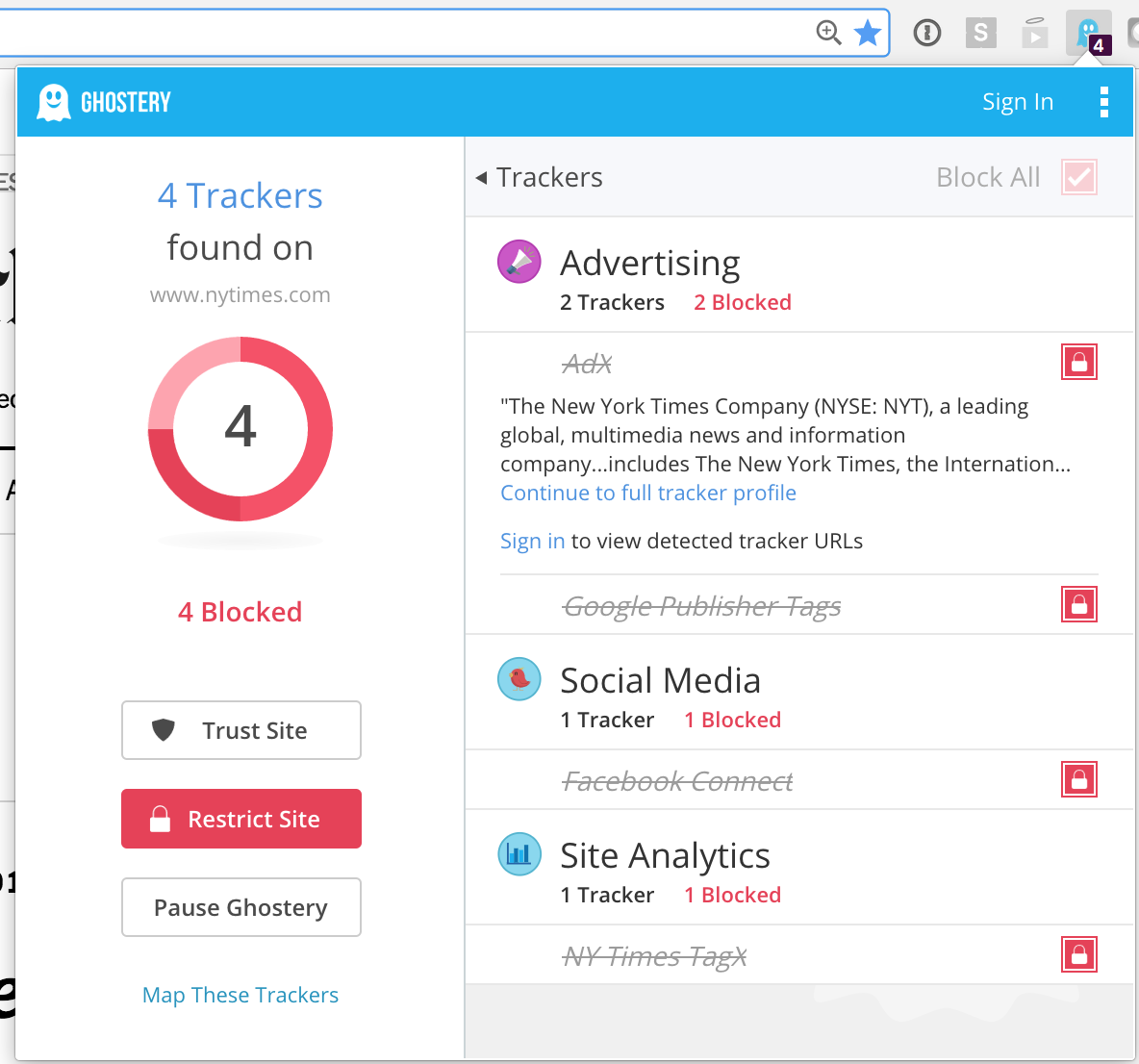
1. Turn on Do Not Track (DNT) in your web browser. Search the Web for instructions on how to do so for your browser favorite browser.
2. Visit <http://donottrack.us> to see if DNT is enabled in your browser.

**Question**: Did you turn on Do Not Track in your browser (yes/no)?

**Part 4: Blocking Web Trackers**

While DNT politely asks web trackers not to track you, you can install software that blocks trackers.

1. Visit https://www.ghostery.com/our-solutions/ghostery-add-on/ and install the Ghostery extension in your browser.
2. Choose whether you’re going to allow Ghostery to sell your browsing information (I said “No Thanks”).
3. By default, Ghostery won't actually block anything anymore. Let’s change that.
   1. Click the Ghostery icon in your browser, and click the three vertical dots to open the settings menu.
   2. Click “Settings.” Check “Block new trackers added to Ghostery by default”
   3. Click the three dots again, choose “Advanced Blocking.”
   4. Click "Block All" if you want. Or, be selective.
4. Browse to your favorite sites and click the Ghostery icon after each page load. Which of your favorite sites uses the most web trackers?
5. Click on the struck-through name of an add tracker and click the “Continue to full tracker profile” link on Chrome or the “Click here for more information about…” link in Safari to learn more about the add tracker (see figure below).



1. “While viewing one of the “full tracker profiles”, click on the down arrow next to “Privacy Information” to learn about the tracker’s privacy policy.

**Question:** What is the name of the third-party tracker you read about, and what kinds of information is its company collecting about you?

**Note:** [Privacy Badger](https://www.eff.org/privacybadger) and uBlock Origin are also good options. Privacy Badger is smarter and less draconian about what it blocks, and requires no hoop-jumping to actually get it to block something. You customize uBlock Origin in “advanced mode” to get it to block what you want. Customizing is not for the faint of heart, the default works pretty well.

**Part 5: Disable Third-party Cookies in Your Browser**

1. Search the web for instructions for how to disable third-party cookies in your browser of choice.
2. Disable third-party cookies in your browser.

**Question**: Did you enable-third party cookies in your browser (yes/no)?

**Part 6: Browser Fingerprinting**

1. Visit <https://panopticlick.eff.org>.

**Question**: Is your browser blocking tracking ads?

**Question**: Is your browser blocking invisible trackers?

**Question**: Does your browser unblock 3rd parties that promise to honor Do Not Track?

**Question**: Does your browser protect against fingerprinting?

1. Click on the link, “Show full results for fingerprinting.” Look over the browser characteristics and how bits of identifying information each one provides.

**Note**: The bits of identifying information means that your browser can be uniquely identified out of a set of 2bits of identifying information. A lower score is better, because it means that you can be less precisely identified. For example:

“We observe that the distribution of our finger- print contains at least 18.1 bits of entropy, meaning that if we pick a browser at random, at best we expect that only one in 286,777 other browsers will share its fingerprint. Among browsers that support Flash or Java, the situation is worse, with the average browser carrying at least 18.8 bits of identifying information. 94.2% of browsers with Flash or Java were unique in our sample.”

<https://panopticlick.eff.org/static/browser-uniqueness.pdf>

**Question**: How many bits of information does Panopticlick report for your browser?

**Part 7: Anonymous Web Browsing**

1. Go to <https://whatismyip.com/> and note your IP address.
2. Turn on your browser’s privacy mode (e.g., “Incognito Mode” in Chrome, “Private Browsing” in Firefox and Safari).
3. Go to <https://whatismyip.com/> again and note your IP address.

Note that your IP address didn’t change.

**Question:** If your true IP address can still be seen by webservers, what does your browser’s privacy mode do?

1. Run the Tor Browser (install if necessary) available for Linux, Mac, and Windows [here](https://www.torproject.org/download/download-easy.html).

**Note**: If you’re using a Mac and MacOS refuses to open the Tor Browser app because it is from an unknown developer, hold the control key and right-click the Tor Browser app and then select “open.” This will create an exception for the Tor Browser app and open it.

1. Reload <https://whatismyip.com> inside of the Tor Browser and verify that your IP address has changed.
2. Determine your IP address using three different websites (e.g., <https://whatismyip.com>, <https://whatismyipaddress.com>, <https://whatsmyip.com>). Note what IP addresses each site reports for your browser.
3. Look up the location of each IP address you noted in step 6 using a service like wolframalpha.com.

**Question**: Which parts of the world do the IPs you noted in step 6 belong?

1. In your Tor Browser, read the about how to use Tor effectively: [https://www.torproject.org/download/download-easy.html#warning](https://www.torproject.org/download/download-easy.html" \l "warning)
2. Tor also provides the functionality of a server only being accessible via the Tor network. This is what is known colloquially as “the dark web.” While it’s true that there are many sites providing illegal services on the dark web, there are also legitimate uses for the dark web as well.
3. Read this short article about the dark web:

<https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/>

1. Access the legitimate TOR services:

ProPublica (non-profit news site):

<http://www.propub3r6espa33w.onion>

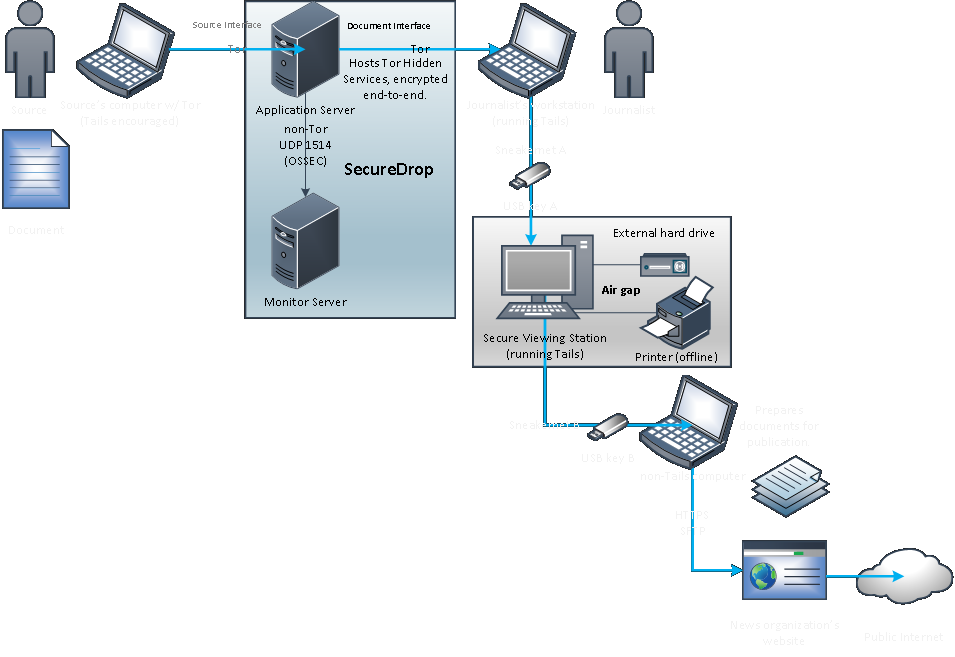
The Federalist Papers (originally published pseudonymously in 1787–1788):

<http://duskgytldkxiuqc6.onion/fedpapers/federa00.htm>

The Washington Post’s SecureDrop site for whistleblowers:

<https://jcw5q6uyjioupxcc.onion>

SecureDrop uses the Tor network to allow whistleblowers to securely share information with the news media:



**Note**: If you’re interested in how SecureDrop works, see here: <https://securedrop.org/faq>.

Visit the Duck Duck Go TOR service search engine, and search for something:

<http://3g2upl4pq6kufc4m.onion>

If you have a Facebook account, access Facebook using their TOR service:

<https://facebookcorewwwi.onion/>

Note: Facebook says that as of April 2016, more than 1 million people access Facebook via Tor:

<https://www.facebook.com/notes/facebook-over-tor/1-million-people-use-facebook-over-tor/865624066877648/>

1. Try to load the same URL in a browser other than the Tor Browser.

**Question**: What error message do you receive?

**Question**: What do you think about the experience of accessing TOR services?

**Lifelong Learning**

|  |  |  |  |
| --- | --- | --- | --- |
| ../../../../Desktop/Unknown.jpeg | “Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World,” by Bruce Schneier.  Great book about the threats of surveillance to society, and what we can do about it. After reading the book, you probably won’t view surveillance the same way again.  Amazon: <http://amzn.com/0393244814> | | |
| Macintosh HD:Users:anthony:Desktop:Unknown.jpeg | | “Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance,” by Julia Angwin  Award-winning journalist Julia Angwin reports from the front lines of America’s surveillance economy, offering a revelatory and unsettling look at how the government, private companies, and even criminals use technology to indiscriminately sweep up vast amounts of our personal data.  Amazon: <http://amzn.com/0805098070> |
| Macintosh HD:Users:anthony:Desktop:Cover-NTH-FINAL-revised-large (2).jpg | | “Nothing to Hide” by Daniel Solove  A book that debunks the most common attack to privacy arguments.  Amazon: <http://amzn.com/0674035070> |
| Macintosh HD:Users:anthony:Desktop:Screen Shot 2013-11-11 at 8.25.07 AM.png | | “1984” by George Orwell  A prescient classic that coined the term “big brother.” Many issues of privacy and surveillance are told in this novel.  Amazon: <http://amzn.com/0451524934> |
| Macintosh HD:Users:anthony:Desktop:MV5BNDUzNjYwNDYyNl5BMl5BanBnXkFtZTcwNjU3ODQ0MQ@@._V1_SX214_.jpg | | Movie: “The Lives of Others” by F. Henckel von Donnersmarck  The 2007 Oscar winner of Best Foreign Language Film of the Year, this film tells the story of a secret police agent in East Berlin in 1984 who surveils a writer and becomes increasingly absorbed his life.  Note: I have an edited copy if you would like to borrow it. |
| Macintosh HD:Users:anthony:Desktop:MV5BMjY0NjYzNjkwNF5BMl5BanBnXkFtZTcwNTk3MzU3Mg@@._V1_SX214_.jpg | | Movie: “The Conversation” by Francis Ford Coppola  A 1974 film psychological thriller starring Gene Hackman that revolves around surveillance. It is more relevant today than when it debuted.  Available on Netflix  Amazon: <http://amzn.com/B005FUTBZA> |