CSE 484 / CSE M 584 - Homework 3

This homework is focused on a variety of topics from the last ~third of the quarter, with the goal of giving you some more hands-on experience with various tools.

Overview

- **Due Date:** Friday, Dec 6, 2019, 11pm
- **Group or Individual:** Individual
- **How to Submit:** Submit a PDF via Canvas
- **Total Points:** 12 points -- **you pick which one of the three parts to do**; you can do other parts for extra credit.

Part 1: Web Tracking (12 Points)

Experiment with an anti-tracking browser add-on, such as Ghostery, Lightbeam, or Privacy Badger. Pick three websites (e.g., www.cnn.com, www.facebook.com, and www.weather.com -- though you may pick any sites), visit them with the add-on installed, and report on what you find.

What to Submit:

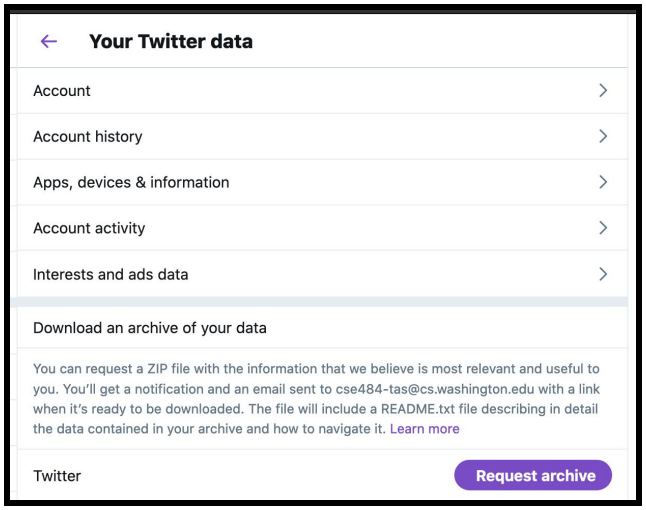
1. **(5 points):** Describe or sketch how third-party tracking allows advertisers or others to track users across multiple sites. Your answers may be brief as long as they are clear. In your answer, please discuss:
    a. (2 points) 3rd-party cookies;
    b. (1 point) browser fingerprinting;
    c. (2 points) how a third-party tracker knows the site that one is visiting.
2. **(1 point):** Which add-on did you try?
3. **(6 points):** Include a screenshot of the add-on's output for each of the 3 pages you tested. How many trackers did you find on each page?

Part 2: GDPR (12 Points)

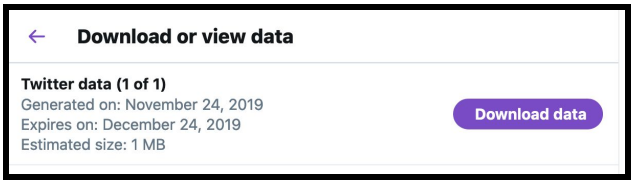
In this exercise, you will get experience requesting GDPR data from Twitter. You may choose to use your own Twitter account, or if you don't have one or would prefer to use a provided dataset, you can use a CSE484 Twitter account's dataset. If you would like to use a different social media account to complete this exercise, you may (but indicate which account it was in your response); we will only provide instructions for retrieving Twitter. We encourage you to complete this exercise with your own Twitter (or other) account though to see the extent of data you can retrieve from a GDPR report.

Directions for retrieving data:

1. On Twitter, go to the following link: https://twitter.com/settings/your_twitter_data (under Profile) and select the "Request archive" button for Twitter.



Step 1: Request archive



Step 2: Download data (may take up to 24 hours to appear)

2. You will receive a notification from Twitter in an email, usually within the next 24 hours. If you don't receive an email notification, make sure to check this same page; the data may be available (on the same page you requested it) before the email. You can find more information about accessing the data here. Once you have downloaded the data, unzip and review the contents and answer the questions on the following page.

What to Submit:

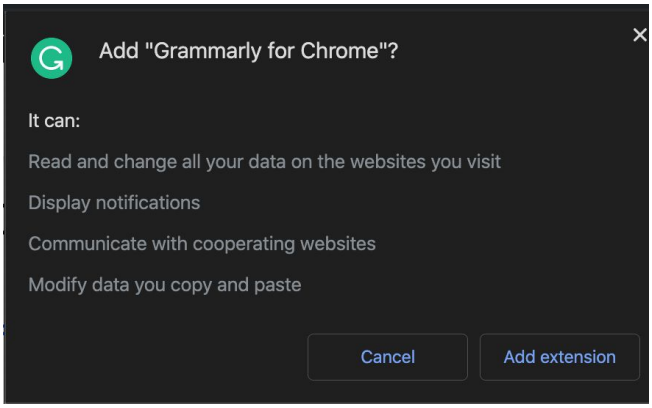
1. **(1 point).** What account did you use (indicate if you chose to use a non-Twitter account)? You don't need to tell us your account name, just whether you used Twitter or something else.
2. **(3 points).** What are 3 pieces of information you were surprised to see in the returned archive? Explain why you were surprised.
3. **(2 points).** Is there any information that you think Twitter (or another social media platform) should not be tracking for users based on what you found? Explain your answer (e.g., if you answer no, explain why not; if you answer yes, give examples of such information and explain why you think that Twitter should not be tracking that information).
4. **(2 points).** Will this change your habits when using this (or other) social media accounts? In what ways? Explain your answer.
5. **(4 points).** GDPR is currently only enacted in the European Union, but there have been discussions about the potential in the U.S. In 2018, the California Consumer Privacy Act was signed into law which incorporates elements of GDPR, such as requiring businesses to share with users what data they have on them, where the data comes from, and where it's going.
    a. (2 of the 4 points) What is one benefit for U.S. companies to have a policy like GDPR? What about a challenge faced by companies? Explain your answers
    b. (2 of the 4 points) What is one benefit for U.S. citizens to have a policy like GDPR? What about a challenge faced by citizens? Explain your answers.

Part 3: Browser Extension Exercise (12 points)

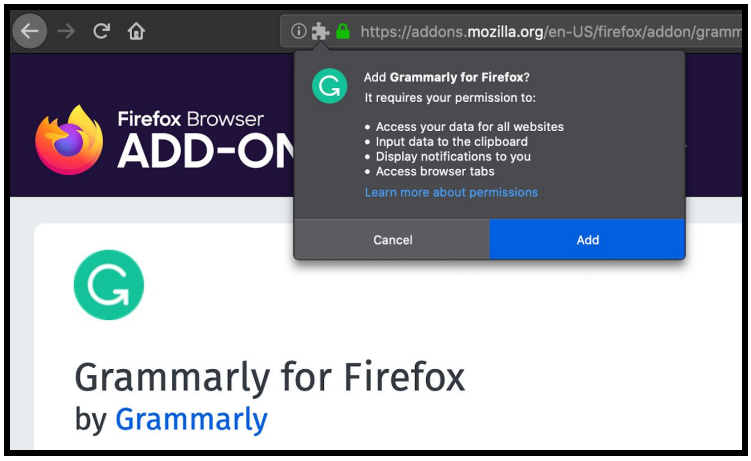
This exercise will give you an opportunity to consider privacy and security in everyday browser extensions. Both Chrome and Firefox browsers offer an Extension Store for users to install extensions that can improve the user experience, such as changing page themes (DOM), monitoring browser activity, overriding new tab pages, etc. As discussed in class, sandboxing restricts access between different windows and tabs. However, JavaScript API's are available for developers to access different types of information about the user's page or session, depending on the permissions set.

Instructions:

1. Go to the Chrome Web Store or Firefox Web Store and find an extension that interacts with a web page DOM or tab(s).
2. Select "Add to Chrome" or "Add to Firefox" (depending on your browser) - a popup will appear to request permissions (example for Grammarly extension below; do not use Grammarly for your answer).



Installing Grammarly on Google Chrome



Installing Grammarly on Firefox

If your selected extension has only one or two permissions requested, find an extension that has at least three bullet points in the result requested permissions.

You do not need to actually install the extension, but use the information to answer the following questions.

You should pick three (3) extensions to study.

What to Submit:

1. **(1 point).** What are the three extensions that you chose?
2. **(3 points).** What permissions did each of the extensions request after you clicked “Add to <browser>”? Were you surprised by any of the permissions requested?
3. **(8 points).** With some basic HTML/JS experience, any developer can easily publish browser extensions on the browser’s store (like this TA-created one!). Consider four (4) browser permissions that you encountered; if you encountered less than 4, you may pick permissions shown in the above screenshots. For each permission, mention one (1) possible asset the an adversary compromise if they created an extension that received that permission, as well as one (1) bad thing that an adversary could do if they compromised that asset.