Ghostery Hunting

BACKGROUND

Data protection is a big deal these days (in the wake of all the Facebook missteps[1,2], the Alexa/Google Home debacles[3], and Apple's issues)[4]. Note that some of these famous breaches deal with privacy issues and others deal with data breaches. It is important to know the distinction, and it's even more important to understand what you can do to protect yourself.

DESCRIPTION

This lab will examine one way to see what sources are looking at your data and provide a mechanism to help control which companies can see what data. Note that the Ghostery is a company that offers free and paid services; this lab is not an endorsement of Ghostery, nor is there any financial (or other) interest in Ghostery.

REQUIREMENTS

A web browser (preferably Chrome) and an internet connection.

PART I: Install the Ghostery web extension

1. To install extensions, you will need to be logged into your browser. For the scope of this exploration, you could create a disposable account so you do not have to worry about installing Ghostery on your personal account. However, I keep Ghostery installed in my private account because there are times when I want to use it.

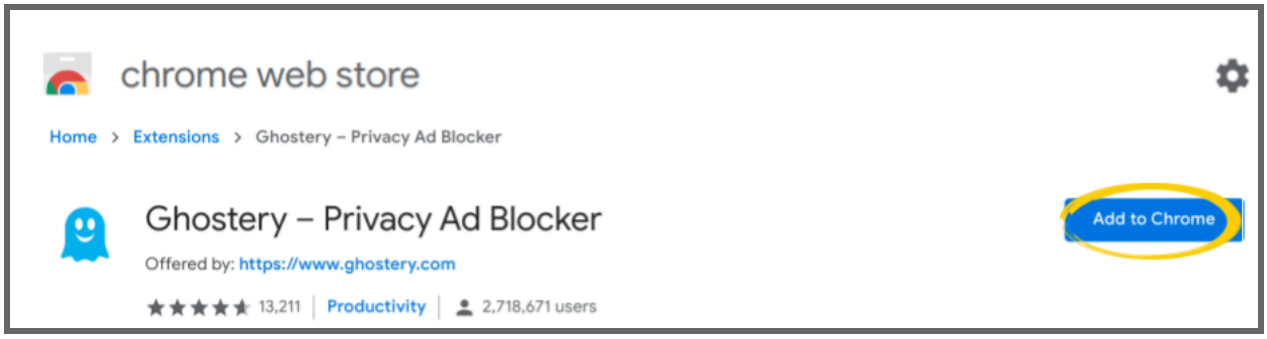
   This page has links to all downloads (browsers, mobile devices, etc.). We will be exploring the Ghostery web extension:

   https://www.ghostery.com/products/

2. Since I'll be installing it in Chrome, I can go directly to the Chrome Web Store link for Ghostery (click here!)

---

[1] A recent history of Facebook security and privacy issues
[2] The big picture: Facebook's year of missteps
[3] Your voice assistant is recording you. Here's how to keep commands private
[4] Making Sense of Apple's Recent Security Stumbles

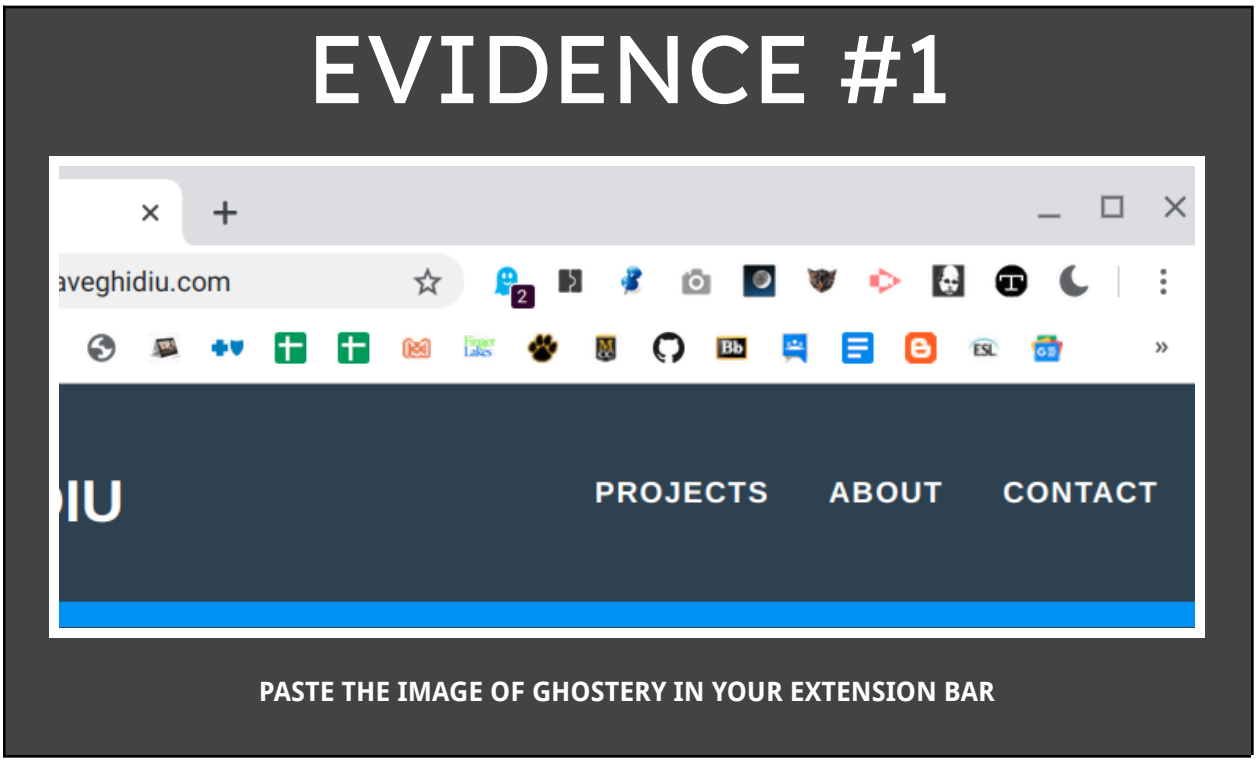


You will be prompted with a permissions screen--this will be the warning that you get:

> Ghostery can read and change all your data on the websites you visit

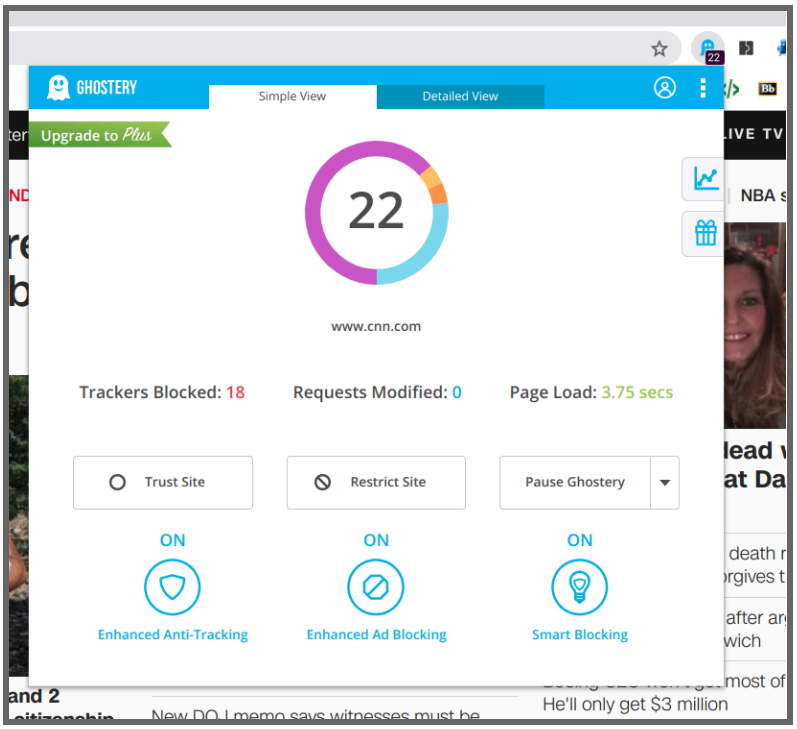
I accepted this (afterall, Ghostery has to scrub through all the content delivered to you so it can determine what agencies are looking for your information), but you can always uninstall the extension, pause it, or get an extension manager.

3. You should see Ghostery in your extension bar (to the immediate right of the address bar in your browser).

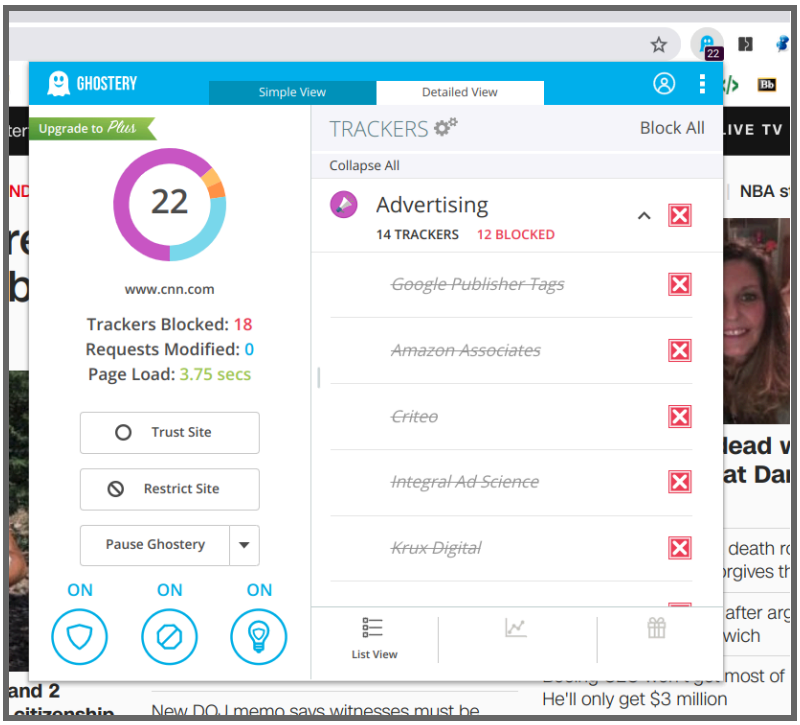


PART II: See what agencies are attempting to access your information

1. With Ghostery installed, you'll notice a little box on the icon in the extension bar; that is the number of interventions that Ghostery has found. If you click on the icon, you'll get a report of all the trackers that Ghostery has found. In this example, I went to www.cnn.com and saw there were 22 trackers!

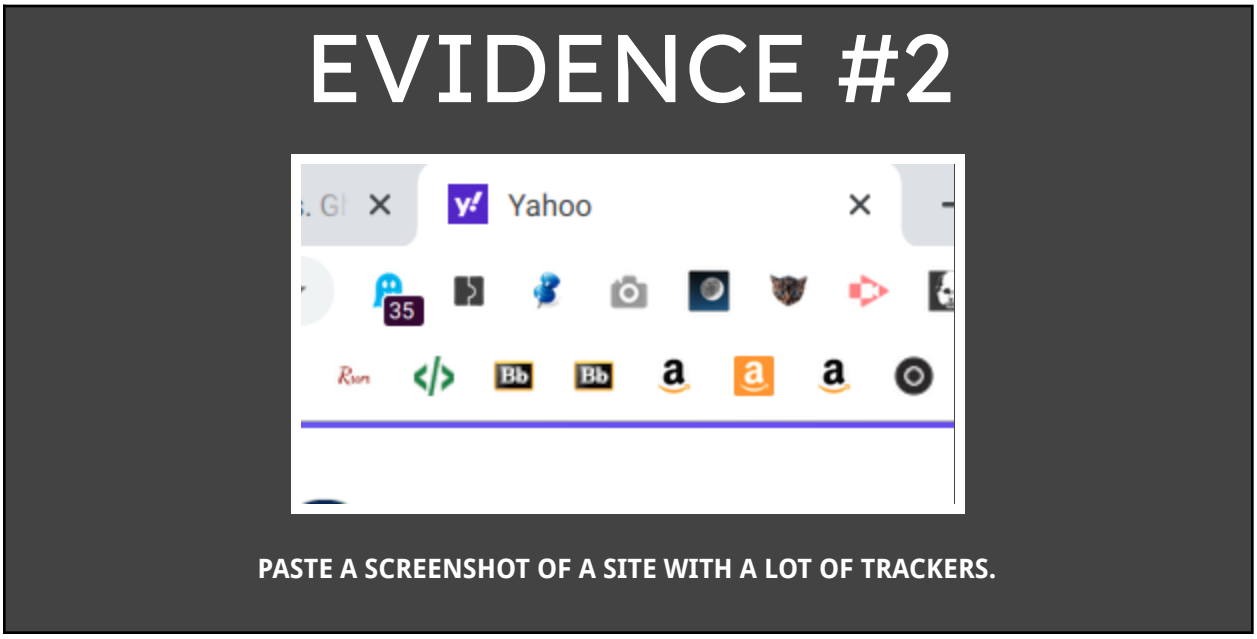


2. Click on the “Detailed View” tab to see how the trackers are categorized (broken down by *advertising*, *customer interaction*, *essential*, and *site analytics*). Of the 22 trackers at CNN, 14 of them were for ads, 1 was for customer interaction, 1 was for essential function, and 6 were for site analytics.



Go to a few sites (maybe yahoo.com, ew.com, imgur.com, cracked.com, or any other site you think may have a lot of trackers) and find out just how many there are. My record is 35 (from yahoo.com), but see if you can beat it. Note that you may have to let some sites load for a while (for instance, in my visit to Yahoo, I let the browser sit for a few minutes and watched the tracker count increase). Also, some sites (imgur.com in particular) have

more trackers on pages that are *not* the landing page (probably because there are more ads on pages with individual posts).



3. Uninstall Ghostery if you'd like (right click on the icon in the extension bar and choose ("Remove from Chrome...").

CONCLUSION

Just having Ghostery is not sufficient to protect yourself (though it's a good start). Ghostery has lots of customizations; you should poke around and check out all the features and customizations that Ghostery has to offer.