As millennials, we spend quite a bit of our time online. Checking Facebook, sending tweets, looking for clothes, buying concert tickets, reading the news, messaging friends near and far, researching for homework assignments and even filling out brackets for March Madness. Each of our browser histories have most likely logged a myriad of online activity, enough to assemble a decent picture of who we are and what we like. Our profiles, regardless of our wishes or knowledge, exist and are for sale.

Entities known as “data brokers” monitor all information available online about a person, compile it all and sell it as a profile to advertising agencies and possibly future employers. The data ranges from innocuous bits of information like age and gender to personal details like sexual orientation, family medical history and sometimes where you go throughout the day. As you can see, these profiles can be fairly extensive.

Below are a few facts on data brokers and the extent to which they monitor our daily lives.

According to 60 Minutes, one of the largest data brokers, Axiom, claims to have an average of 1500 pieces of information on over 200 million Americans.

The marketing firm Euclid Analytics monitors the locations of customers in stores by tracking the GPS on their cell phones, noting the aisles they walk through and time spent in each aisle without customers’ knowledge.

On a computer, you can download one of these tools for blocking third party trackers: Disconnect, Ghostery or Abine. Some smartphones also have the option to block third party trackers in Safari settings.

According to Ghostery, the websites with the most trackers are:
- Huffington Post: 351 trackers
- Weather.com: 300 trackers
- NY Times: 287 trackers

**Race:** Caucasian

**Family medical history:** heart disease, cancer, depression

**Sexual orientation:** probably straight

Advocate for marijuana legalization

No diets, above average consumption of pizza

Favorite brands: Nike, American Eagle, Vans

Heavy Twitter, Instagram user
Ashkan Soltani has worked as a renowned technology consultant for more than 20 years, with the goal of “demystifying technology” by raising consumer awareness about online privacy and data security. His work with the Federal Trade Commission and Wall Street Journal, where he’s published eye-opening research on online trackers, has made him one of the nation’s leading experts on privacy and technology. We asked him a few questions about how his work relates to our generation.

DA: Why is being informed about digital privacy today important for high school students, along with everyone else?

AS: The method of collecting data in a mobile environment is basically the same, but there are some tracking tools that apply specifically to phones. And you are right that your phone can reveal more sensitive data. Because your phone is always communicating with cell towers and other signal infrastructure, the location of your phone can be more precisely determined than the location of your computer. There are companies that take advantage of this by installing technology that passively collects the signal your phone emits while you browse in physical stores and keeps track of what aisles you visited and how long you stopped in front of a particular product.

DA: What restrictions exist against the selling of our information to companies, and how effective are they?

AS: Most of the time your information isn’t being sold to a company, but rather collected directly from your online activity by first parties (the site you know you are using) and by third parties (companies who have contracts with the first-party and whose names are not necessarily shared with you on the site). Typically, companies use cookies to track users who have agreed to this, sometimes actively by accepting the “terms and conditions” and sometimes passively by not changing the default settings, which are typically set to allow collection of data. The companies that collect this data do trade and sell it amongst each other in order to create a more robust profile of an individual user. There are no laws governing this market. Basically, as long as companies don’t mislead their users or violate their own terms and conditions, there are few regulations governing what they can do with the data they collect. Some exceptions include regulations specifically governing financial information, health-related information (HIPPA), and online privacy for children.