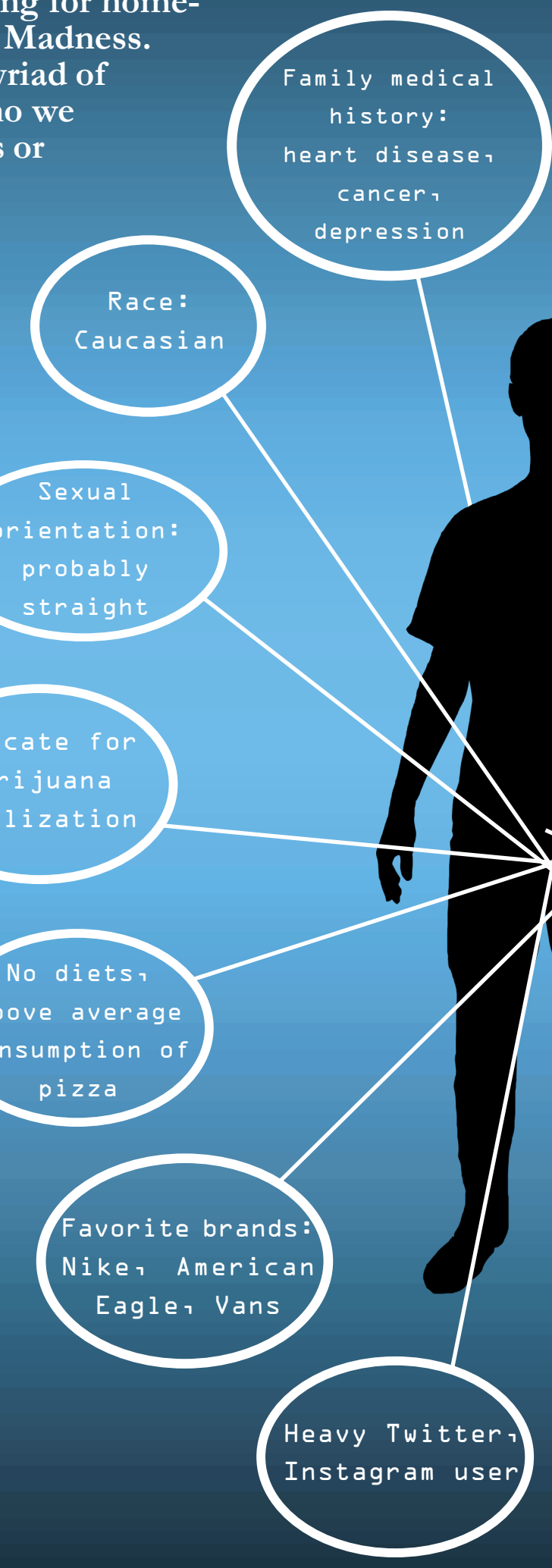
You Are What You Search

How online activity is monitored, compiled and sold

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.



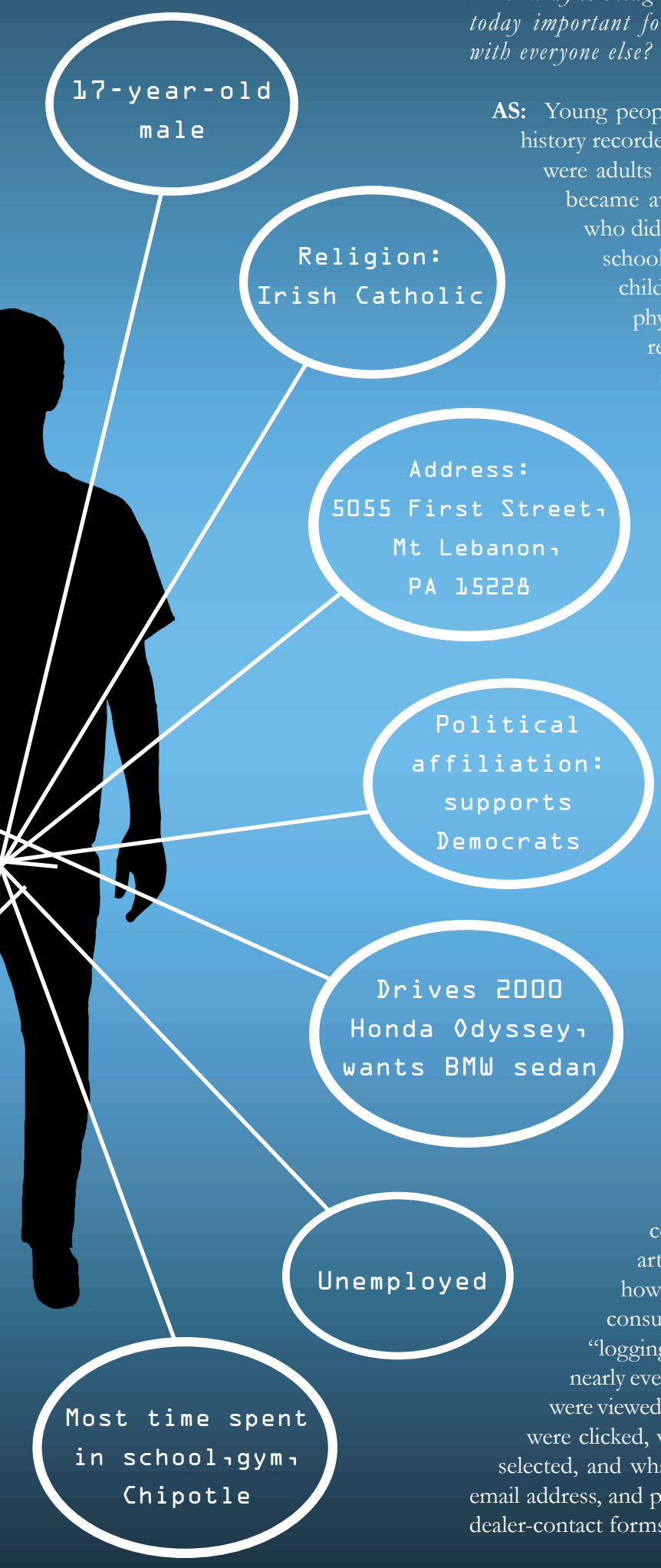
According to 60 Minutes, one of the largest data brokers, Acxiom, claims to have an average of 1500 pieces of information on over 200 million Americans.

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

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: Young people will have a longer personal history recorded online than those of us who were adults when these services and tools became available. For example, people who didn't have digital cameras in high school have all of our embarrassing childhood photos stored safely in physical photo albums, far from the reach of Google. It's worth it to spend some time thinking about what your 30-year-old selves are going to want recorded online about this period of your life, keeping in mind that **once a digital file is shared, it is out of your control.** Digital files can be copied and stored without your knowledge and are very difficult to delete once dispersed.

DA: What kind of information are data brokers getting?

AS: In addition to which sites you visit, companies can track what links you clicked, what other sites you have previously visited, and sometimes what information you enter into an online form. Not every site is collecting all of this information - these are just a few examples of what can be collected. A Wall Street Journal article I contributed to described how the company Dataium tracks consumers interested in buying a car, "logging information about a visitors' nearly every action — not just what pages were viewed, but also what parts of the page were clicked, which dropdown options were selected, and what information (such as name, email address, and phone number) were entered in dealer-contact forms."

DA: Is the information collected from smart phones different, and can it be more revealing?

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: How can citizens and students protect their information?

AS: There are a few things people can do to try to limit the ways they are followed online - like using private browsing mode and using tools like **Ghostery** and **Disconnect** to observe or block some of the third party tracking. But some of the things I would recommend could also be risky because of a piece of legislation called the Computer Fraud and Abuse Act (CFAA).

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.

centerspread by abby xie and steve helmeci