Most informed citizens probably know by now that corporations collect information about them, but they may well be unaware of the extent and scope of the invasions of privacy that are now widespread. Many may be aware of tracking tools referred to as “cookies,” which are installed on one’s computer by visited websites. They are used to identify the person and to remember his or her preferences. Some people protect themselves from such tracking by employing software that allows them to clear cookies from a computer. However, corporations have recently begun to install “supercookies” that are very difficult to detect, and if removed, secretly reinstall themselves. As one report concluded: “This means that privacy-sensitive consumers who ‘toss’ their HTTP cookies to prevent tracking or remain anonymous are still being uniquely identified online by advertising companies.”

Major cell phone and mobile technology companies offer services that allow lovers, ex-spouses, lawyers, or anyone else to find out where a person is—and track their movements—by using their cell phones’ GPS capabilities. A German politician who inquired about location storage information discovered that over a six-month period, his longitude and latitude had been recorded over 35,000 times.

There are two kinds of corporations that keep track of what Internet users buy, read, visit, drink, and who they call, e-mail, and date, among other things. Some merely track users’ activity on their sites as part of regular business; recording purchases and viewed products helps them increase sales. This is true for nearly every major online retailer. Other corporations make shadowing Internet users—and keeping very detailed dossiers on them—their main line of business. (I will refer to them as privacy merchants. They sell information to whoever pays the required price.
In 2005, one such company—ChoicePoint—had records on over 220 million people. Professor Christopher Slobogin notes that the amount of information culled by corporate data miners can provide the inquirer with a wide array of data about any of us, including basic demographic information, income, net worth, real property holdings, social security number, current and previous addresses, phone numbers and fax numbers, names of neighbors, driver records, license plate and VIN numbers, bankruptcy and debtor filings, employment, business and criminal records, bank account balances and activity, stock purchases, and credit card activity.

For example, in 2009, a law professor at Fordham University gained minor notoriety when he assigned his class to create a dossier on Justice Antonin Scalia using only the information they could find online. The result was a fifteen-page document “that included the justice's home address and home phone number, his wife’s personal e-mail address and the TV shows and food he prefers.” Some privacy merchants even keep dossiers on the crimes a person has committed, their divorces, political leanings, and their interests in topics that include religion, the Bible, gambling, and adult entertainment. Other companies amass lists of “victims of sexual assault, and lists of people with sexually transmitted diseases. Lists of people who have Alzheimer’s, dementia and AIDS. Lists of the impotent and depressed.”

Although several data-mining companies allow individuals to opt out of their databases, people must contact each company individually, and even then information may still linger in some search results or websites. Google, for example, generally does not remove search results if the information contained is truthful and not illegal.

The privacy merchants are limited by laws that Congress (and states) have enacted that carve out subsets of data, particularly medical and financial records, in which the privacy merchants cannot freely trade. However, very little attention has been paid to the fact that information is fungible. Through a process that might be called “privacy violating triangulation” (PVT), one can readily derive much about a person's medical, financial, or other protected private side by using “innocent facts” that are not privileged by law. A piece of seemingly benign information—for instance, the number of days a person failed to show up for work, or whether the person purchased a wig—suggests volumes about one’s medical condition. By building a portfolio of many such apparently innocuous facts, one could infer a great deal, effectively violating the realm of privacy surrounding individuals’ most sensitive information. Thus, a study of Facebook shows “how the on-line social network data could be used to predict some