Gifts have been bought. Presents wrapped. Now all that remains is the giving and receiving. Oh, and the tracking, of course. Little did you know that all the while you were searching out that perfect gift, you were unknowingly leaving a trail for others – namely, the government and its corporate cohorts – to follow.

Thanks to the wonders of technology, the indifference of the general public to the growing surveillance state, the inability of Congress to protect Americans' privacy, and the profit-driven policies of the business sector, the corporate state could write a book about your holiday shopping habits: the Web sites you've visited when trying to decide what to buy, the storefronts you've browsed while wandering the mall, and the purchases you've made.

Even the store mannequins have gotten in on the gig. According to the *Washington Post*, mannequins in some high-end boutiques are now being outfitted with cameras that utilize facial-recognition technology. A small camera embedded in the eye of an otherwise normal-looking mannequin allows storekeepers to keep track of the age, sex, and race of all their customers. This information is then used to personally tailor the shopping experience to those coming in and out of their stores. As the
Washington Post
report notes: "A clothier introduced a children's line after the dummy showed that kids made up more than half its mid-afternoon traffic. ... Another store found that a third of visitors using one of its doors after 4 p.m. were Asian, prompting it to place Chinese-speaking staff members by that entrance."

At $5,072 a pop, these EyeSee mannequins come with a steep price tag, but for store-owners

who want to know more – *a lot more* – about their customers, they're the perfect tool, able to sit innocently at store entrances and windows, leaving shoppers oblivious to their hidden cameras. Italian mannequin maker Almax SpA, manufacturer of the EyeSee mannequins, is currently working on adding ears to the mannequins, allowing them to record people's comments to further tailor the shopping experience.

While this may be the creepiest instance of targeted advertising in recent memory, these surveillance mannequins provide a window into a $100-billion-per-year data-mining industry that gathers vast amounts of information about every facet of consumers' lives to target them with personalized advertisements. Granted, businesses "have been tracking shoppers for years through people-counters, security cameras, heat maps, and even undercover researchers," notes journalist Annalyn Censky. Yet the advent of the Internet age, with its abundance of personal computers, smart phones, and other technological software and gadgets vaunted for their convenience and ease of use, has made corporate snooping that much easier.

All of the Web sites you visit collect some amount of information about you, whether it is your name or what other sites you have visited recently. Most of the time, we're being tracked without knowing it. For example, most Web sites now include Facebook and Twitter buttons so you can "like" the page you are viewing or Tweet about it. Whether or not you click the buttons, however, the companies can still determine which pages you've visited and file that information away for later use.

For example, it was recently revealed that the advertising agency Epic Marketing was engaging in "history sniffing" by surreptitiously tracking the Internet-browsing habits of unsuspecting people. Epic Marketing was specifically looking for people who had searched for information on "fertility issues, impotence, menopause, incontinence, disability insurance, credit repair, debt relief, and personal bankruptcy." Epic then targeted them with advertisements based upon their surfing history.

As the EyeSee mannequins show, you no longer even have to be in front of your computer to have your consumer data accessed, uploaded, stored, and tracked. In August 2012, for example, data-mining agency Redpepper began testing a service known as Facedeals in the Nashville, Tennessee, area. Facial-recognition cameras set at the entrances of businesses snap photos of people walking in, and if you've signed up to have a Facedeals account via your Facebook account, you receive instant coupons sent to your smart phone. Similarly, a small coffee chain in San Francisco, Philz Coffee, has installed sensors at the front door of their stores to capture the Wi-Fi signal of any smart phone within 60 yards. Jacob Jaber, president of Philz Coffee, uses the information gleaned from these sensors to structure his stores according

to the in-store behavior of customers.

Of course, these personalized marketing campaigns are just the beginning. Not too far in the future, stores will create our shopping lists for us. Thanks to the ongoing expansion of the Internet of Things – the rapidly developing digital connection between one's home appliances and digital devices – you may one day soon find your phone telling you that you've run out of milk. "A lightbulb could blow at home and automatically add itself to your weekly shop. You wouldn't need to tell us you need to feed a family of four; we'll know," said Phil Clarke, the CEO of supermarket Tesco. "We'll even know your budget."

Not even politicians are immune to the lure of data-mining. In the run-up to the 2012 presidential election, the Romney and Obama campaigns followed voters across the Web by installing cookies on their computers and observing the Web sites they visited in an attempt to gather information on their personal views. CampaignGrid (a Republican-affiliated firm) and Precision Network (a Democrat-affiliated firm) both worked to collect data on 150 million American Internet users, or 80 percent of the registered voting population.

The government has done little to regulate this booming industry and safeguard consumer privacy, leaving corporations to take the lead in determining how this data is collected and used. Not surprisingly, privacy is low on their list of priorities. However, the fact that all of this information can also be data-mined by the police and a multitude of government agents through their vast network of fusion centers and information-collecting agencies just adds an Orwellian luster to the overall picture.

Constitutional attorney and author John W. Whitehead is founder and president of The Rutherford Institute (Rutherford.org). His newest book, The Freedom Wars, is available at Amazon.com , and he can be reached at johnw@rutherford.org .