10 ways you give up data without knowing it

By **Ryan Broderick** and **Emanuella Grinberg**, BuzzFeed/CNN

(BuzzFeed/CNN) -- Edward Snowden, a 29-year-old former technical assistant for the CIA, revealed himself as the source behind one of the most notorious intelligence leaks in recent U.S. history. Snowden's leak revealed the shocking amount of information the National Security Agency was collecting as a way to track down foreign targets. And while the NSA's tactics may be unsettling, it's not just the U.S. government that is messing with your data.

It's a brave new world of information mining. Here are a few ways your data are already being collected and put to use, even if you don't know it.

1. Facebook knows what you're buying.

Facebook purchased data in 2012 on 70 million U.S. households from a data mining firm called Datalogix. Facebook then revealed in February what many users were already noticing: The social network was, in fact, tracking users' behavior to better advertise to them.

The backlash from creeped-out users has since led Facebook to become even more transparent about its targeting programs. Users now also have the ability to opt out.

2. Your Facebook likes reveal personality traits.

Liking something on Facebook is a simple, almost mindless way to pass time on the social networking site. But choosing to "like" beer, crappie or "Real Housewives" allows researchers to extrapolate far more intimate details about you, such as sexual orientation, political leanings and religion, according to a University of Cambridge study released in March.

If you're curious, you can visit youarewhatyoulike.com and see exactly how much your Facebook can predict.

3. Ad firms watch your tweets to better market to you.

Twitter, not to be outdone by Facebook's ad targeting, came up with its own version. Leading advertising firm WPP announced last week that it was partnering with Twitter in what the two companies are calling a "global strategic partnership."

What does that mean for you? Twitter is allowing WPP to analyze Twitter data to set up a way to better monitor real-time consumer behavior.

4. Companies use retina trackers to see how your eyes move in the store.

Social media companies are not the only ones scrambling to use your data for more precise targeting. Marketers and consumer-products companies have come up with an effective and very science fiction-y method to better monitor how you interact with products, according to a Wall Street Journal report.

Using computer simulations of product designs and store layouts, companies like Procter & Gamble and Kimberly-Clark Corp. are experimenting with eye-tracking technology to better understand how things like how shelf placement or logo size affects consumer behavior.

5. Department stores can track your smartphone.

Similarly, a Denver news station learned that some Nordstroms were using their WiFi network to track customers' smartphones and create a heatmap of their movements and how long they stayed in each section of the store.

The WiFi tracking program does have an opt-out, which you can learn more about here.

6. Amazon has ads that watch what you look at online.

Amazon was one of the first major companies to use what's now a commonly known practice: cookie tracking. In the most basic sense, cookies track and analyze where you're browsing and what you're looking at and then advertise Amazon products that match up.
It was one of the first mainstream uses of cookie-tracking and definitely ruffled a few feathers. Amazon still tracks users' cookies, but there are also a lot of resources available to help people turn trackers off.

7. Target can tell if you're pregnant before you do.
Target made news last year when it was revealed that its mailer system tracks purchase history and mails coupons based on those purchases. The system got a little too accurate for comfort when a Target in Minneapolis determined that a teenager was pregnant before she did. The mailer system analyzed her previous purchases and noticed that what she was buying in terms of groceries and toiletries fit a trend that usually meant a customer was in the early stages of pregnancy. Unfortunately, the girl and her family didn't know that yet. Sure enough, though, the mailer system was right, the girl was pregnant, and Target's purchase analysis figured it out before the humans it was monitoring did.

8. Qantas Airlines flight attendants carry iPads with up-to-the-minute data on frequent flyers.
In the same way Target's algorithms were creeping people out with how much they revealed about their customers, Qantas Airlines learned that too much data can backfire. According to The Harvard Business Review, when Qantas armed its flight attendants with real-time, data-tracking iPads to better accommodate frequent flyers, the customers started getting a little uncomfortable. Qantas decided that the flight attendants needed more training if they were going to incorporate that level of information into customer service but said nothing about the ethics of using it in the first place.

9. An app can use data from your smartphone pictures to pinpoint where you took the photo.
Chances are, if you have a smartphone, you've used it to take photos and upload them to share with family, friends and followers. What you may not know is that all of those photos have specific digital fingerprints known as EXIF data, which reveals where they were taken, when they were taken and how they traveled online. So what might an online stalker want to do with all that data? The aptly named Creepy is an app that can aggregate geo-located photos from all over the Web. There are other sites that can do it too, and it's very often what Anonymous uses to track targets down.

10. DNA databases are not just for the FBI anymore.
Local law enforcement agencies across the country are building unregulated DNA databases under the radar, The New York Times reported this week. New York's database has 11,000 crime suspects in it, while the version in Orange County, California, has a whopping 90,000 profiles. The DNA is usually taken from low-level defendants who give their DNA to law enforcement in exchange for having charges against them dropped. So if you've given DNA to police in recent years, there's a chance they might still have it.