Data Brokers, Advertisers, and Governments: The Market for Your Personal Information

A few years ago, I tried to find out what kind of information data brokers had stored about me. But as it turns out, viewing specific information is difficult. I visited at least half a dozen sites without finding any clear way to request my data.

Even when dealing with the company that *did* eventually let me see their data, Acxiom, the process proved difficult and convoluted, and many people would reasonably give up before obtaining the records.

At the time, Acxiom directed me to a website called "aboutthedata.com" in order to access my info. That website, as of this writing, is no longer active, and Acxiom says that they are "in the process" of building a "consumer portal" where you can manage your data.

So what did I discover from Acxiom when I asked to see what they knew about me?

Quite a bit. It seems that they gather data largely by household, and at the time I requested the data, I was living with my parents, which conflated the information somewhat. Nonetheless, it proved pretty accurate.

Acxiom knew that, at the time, I drove a 2001 Subaru Forester and sometimes a 2001 Ford Escape. Acxiom knew when my parents and I had moved into the house we occupied, along with the approximate value of the house and size of the lot. They estimated a little high in terms of our household income, but they were dead on with my parents' age and marital status.

In addition to this, Acxiom correctly listed three adults in

the household, and the company was aware of several of our interests, including gourmet cooking, home furnishings and decorating, and gardening, to name a few. Certainly, that's a lot more information than I recall ever giving out.

But according to a 2013 *New York Times* article on the topic by Natasha Singer, all of this is just a taste of the information Acxiom actually had on me, at least in its initial form. Singer writes:

> *Critics say the new consumer site omits so many details about Acxiom's data-gathering and analysis practices that it sanitizes the data mining behind data-driven marketing.*
>
> *Aboutthedata.com, at least in its initial incarnation, leaves out many data elements that Acxiom markets to its corporate clients — intimate details like whether a person is a 'potential inheritor' or an 'adult with senior parent,' or whether a household has a 'diabetic focus' or 'senior needs.'*

As it turns out, data broker companies like Acxiom use many sources, online and off, to gather personal information about you and me and then sell that information to marketers. They maintain massive databases about us, with information ranging from marital status to education level to things we've purchased. The companies then sort us into categories and, for a fee, share characteristic-based lists with advertisers.

Data-sharing isn't the only problem, though. According to Acxiom, said data is collected from public records, self-reported information, or "data from other commercial entities where consumers have been provided notice of how their data will be used, and offered a choice about whether or not to allow those uses."

"Provided notice," however, is unhelpfully vague. What Acxiom is really saying is that when we sign up for some new website or service, somewhere in those pages of terms and conditions

is likely a sentence or two about how data we give to the service will be used—it will be sold to data brokers (like Acxiom). So when we agree to those terms and conditions on that discussion board or retail site, we give both the website and Acxiom permission to accumulate data about us.

But did we really? Because who reads every line of the complex legal jargon of most sites' terms and conditions? Very few of us.

Yes, maybe it's laziness that prompts us to click that "I Agree" button, but it still seems unreasonable for companies to expect us to devote half an hour to reading incoherent terms. Couldn't they put information in clearer and more concise forms? Shouldn't companies be required to put issues dealing with privacy in big, bold letters near the front of the document? That would certainly improve the rate of understanding and true consent among consumers.

Plus, in recent days, the data-selling industry was under an Energy and Commerce Committee investigation because the committee questions whether the companies use the data ethically and fear that "existing laws do not sufficiently protect Americans' data from misuse."

Indeed, current data laws primarily operate by state, meaning that there are few federal laws that comprehensively protect consumers' data from unauthorized use. And—since the regulation is weak—"many companies…can use, sell or share your data without notifying you," according to *Forbes*. Consumer information is not truly secure, and online security can lead to serious breaches in privacy.

To illustrate this, consider the recent data leak in online genetic testing company 23andMe. According to *Reuters* reporter Zeba Siddiqui, 23andMe recently notified customers of several unauthorized entries to the "DNA Relatives" account feature—a feature that holds intimate data "including relationship

labels, ancestry reports and matching DNA segments, location, birth year and family names, among other things." While authorities are investigating the security breach, consumer information has already been greatly compromised.

To be fair, many data brokers have an "Opt Out" option that would presumably allow us to get them to delete or at least not share their records on us and not add to those records any more. The problem presents itself, though: There are hundreds of data broker companies, which means that a concerned citizen would have to go through literally hundreds of opt-out forms just to protect their basic information—and that wouldn't even cover those companies who don't provide an opt-out option.

Add to this toxic recipe the fact that many people don't even know that brokers exist, and we have a real mess. In his book *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, Brue Schneier says, "Most of the companies tracking you have names you've never heard of: Rubicon Project, AdSonar, Quantcast, Pulse 260, Undertone, Traffic Marketplace." How can we protect our privacy from entities we don't even know are out there?

Certainly, we need an opt *in* option. Why are we all automatically enrolled in these data collection programs? We should be given the choice to join, not the choice to leave.

But what about the cases when we can't opt in or *out*? Just recently, it's been revealed that the U.S. government uses the pop-up notifications on our phones to read our messages. Why are they spying on our personal conversations? And what else are they doing to access our personal data that we don't yet know about?

Given the scope of these problems, there are not any easy solutions—at least not ones that could reverse the damage that has already been done. Still, the first step to finding ways to return our privacy is simply being aware of what has been

taken.

—

Image credit: *Pexels*