I tried to delete myself from the internet. Here's what I learned

It was MyLife that broke me. After spending hours studying FAQ pages, sending terse emails and making occasional phone calls in an earnest-if-naive attempt to take back some control of my personal information online, I had my first demoralizing moment.

MyLife pulls together vast amounts of public data to create background reports and "reputation scores" on millions of people in the US, all available to those willing to pay for a monthly membership. On it, I found a sometimes inaccurate but eerie amount of personal information about, well, my life: my birthday and home city; my previous job title (though curiously not my current one); a list of people "Seth maintains relationships with," including the names of both my parents, each linked to their own profile pages with still more data. All there in one place waiting to be discovered.

When I called the site, a customer service representative stressed that the information doesn't come from MyLife, but rather from across the "interwebs." Following some back and forth, the representative agreed to delete my profile page. I felt victorious -- until two hours later when I received the first of many promotional emails from the company, one encouraging me to sign up for a membership, another talking about raising my credit score.

As I would learn through my brief, manic campaign in December to scrub as much of my personal data as possible and start the new year with a clean digital slate, it's hard not to feel like you're just scratching the surface of an impossibly large data industrial complex. By the end of my experiment, I felt even worse off about my ability to wrestle back control of my data than when I started.

Our data is out there. Now what?

n recent years, it's become a truism in certain tech-savvy Twitter threads that much of our personal information is already out there somewhere thanks to an ever-growing list of hacks.

Banks, retailers, social networks -- both popular and defunct -- have all disclosed massive data breaches. In 2017 alone, Verizon (VZ) confirmed that every single Yahoo account -- all 3 billion of them -- had been affected by a massive breach and Equifax (EFX) disclosed that a breach had potentially exposed the names, Social Security numbers, birth dates, addresses and credit card numbers of as much as nearly half the US.

There are only two viable emotional reactions to such a total collapse of personal privacy: denial or helplessness. After trying the former for a time, I shifted to the latter, prompted, as with so many moments in my life, by belatedly listening to a sobering podcast about a hack. I followed the usual measures recommended in informational cybersecurity stories -- implementing two-factor authentication; signing up for a password management app; freezing credit reports indefinitely -- all with an overriding sense that none of these steps eliminated any of that personal information floating around in some dark corner of the web.

As cybersecurity expert Bruce Schneier recently put it to one of my colleagues: "So my password was stolen, is there any way I can go to every criminal on the planet, to their computers, and delete my name? No."

But there had to be something more to be done, I thought. The fact of the matter is, the internet is already littered with information that could be used against us, much of it collected through entirely legal means. Mothers' maiden names. Birthdays. Home addresses. I might not be able to prevent my favorite stores from getting hacked, or sweet talk a bunch of hackers after the fact, but I could make it just a little bit harder for a bad actor to find my personal information online -- and in the process, regain some sense of control of my data and my life.