medium.com

I Left the Ad Industry Because Our Use of Data Tracking Terrified Me

Fast Company

6-7 minutes

With every post, click, and purchase, we have become the product. I didn't agree to that, and I bet you didn't either.

By Richard Stokes

It was a little over two years ago that I realized the ad-tech industry had gone too far. I was an executive at a global advertising company, watching a demo from a third-party data provider on how they could help with ad targeting. Their representative brazenly demonstrated how he could pull up his own personal record and share with us his income, his mortgage details, where he worked, what kind of car he drove, which political party he was likely to vote for, and his personal interests (craft beer, of course). It was everything, all in one place.

Not to be outdone, another startup projected a map of San

Francisco with a red line tracking a real, anonymous person throughout their day. He challenged us to infer what we could about her. She left the house at 7 a.m. Went to Starbucks. Went to a school. Went to a yoga studio. Went back to the school. She was a mother with at least one child, and we knew where she lived. We knew this because this woman's cell phone was tracking her every move. As does every other cell phone, including the one in your pocket right now.

When I looked around the room that day, many of my colleagues seemed alarmed. Up until that point, the advertising industry had asked people to trust us with their data. We were about to go back on that promise. I left the ad-tech industry shortly thereafter.

I realized that my industry had changed. Advertising had ceased to be about connecting with consumers—it was now about finding novel ways of extracting evermore personal information from computers, phones, and smart homes. To many of the most powerful and profitable companies in the world, *we* are the products, and the services we all use are just afterthoughts they put out to keep us hooked. And the rest of the ad industry, which depends on their data to compete, has no choice but to go along with whatever whims and changes come their way.

Meanwhile, the rest of us have come to accept that our every move is being tracked and used to manipulate what we read, what we buy, how we vote, and how we see the world. By using 'smart' devices, we have invited a vast network of big tech companies, advertisers, data brokers, governments, and more into our homes and pockets. These companies have been extracting our personal data without permission and making fortunes with it. And now, with every post, click, and purchase, we have become the product. I

didn't agree to that, and I bet you didn't either.

How to unwind this surveillance economy

According to a recent Pew study, 61% of Americans would like to do more to protect their privacy. Two-thirds have said the current laws are not good enough (REF). We need a combined political and technological solution to unwind this surveillance economy. Here's what that should look like.

First, people must have a real choice about what data they share. If you don't want to share personal data with a company, you shouldn't have to. For more than a decade, tech companies and advertisers have said there's no need for opt outs, because people like targeted ads. I'm sure that's true for some, or even most—but the rest of us should have a choice. Real choices mean informed consent—companies should explain what they're doing with your data, why, and for how long, in plain English.

Second, companies must be prevented from refusing service to those who do opt out. If your only options are to forego a useful product or consent to constant surveillance, you don't really have a choice. Even more abusive are so-called *shadow profiles,* which ad-tech companies create without your consent. If you don't have a Facebook account, that's your choice. Facebook shouldn't have an account on you.

Third, we must require technology companies to disclose device end points—in other words, to tell us what data they're collecting, where it's going, and how it's getting there. Offering consumers this visibility will give them a better understanding of what is actually happening to their personal information when they use a device—

and inform their purchasing decisions. In 2018, Microsoft voluntarily disclosed its end points for Windows 10, giving users a granular understanding of what data Windows is collecting, where it's going, and how it's getting there. That's a great start, but more should follow Microsoft's lead.

Finally, there is some data that companies should never be allowed to collect, because of the significant risk of abuse. There is no reason why your ISP should be able to tell advertisers or health insurers that you may have diabetes, based on a connected glucose meter in your home. Location is another example: you should be able to share your location to look up a restaurant without sharing your precise location on a minute-by-minute basis. To its credit, Apple has started to clamp down on apps requesting location data that they don't need to provide functionality—this should be standard practice across platforms.

Adding to this need for a policy solution is Big Tech's 'conversion' to the privacy cause. Google and Facebook have become two of the world's most powerful companies by collecting and selling their users' personal information: they are not about to change that business model unless they are forced to. Their recently announced privacy enhancements are more about monopolizing your data, not protecting it. And they're hoping you don't notice the difference.

There is no one bad actor responsible for this gradual degradation of our privacy. We are living in a system of perverse incentives, where good people clock into work each day and make the problem just a little bit worse, without understanding the bigger picture. We can and must correct course now to create a welcoming environment for innovation that doesn't require us to surrender our

private lives.

Richard Stokes is the founder and CEO of Winston Privacy.