MY WEIRD PROMPTS

Podcast Transcript

EPISODE #222

Your Life for Sale: Navigating the Data Broker Economy

Published January 13, 2026 • Runtime: 19:29

https://myweirdprompts.com/episode/data-broker-privacy-protection/

EPISODE SYNOPSIS

In this episode, Herman and Corn pull back the curtain on the massive $430 billion data broker industry, exploring how your most private information is harvested, packaged, and sold to the highest bidder. From the hidden mechanics of Real-Time Bidding to the "Trojan horse" nature of mobile apps, the duo uncovers the invisible infrastructure of modern digital surveillance. They also provide a roadmap for fighting back, discussing the groundbreaking California Delete Act and practical tools you can use to break the chain of attribution and secure your digital footprint.

DANIEL'S PROMPT

Daniel

I'd like to discuss the industry of data brokers as a privacy threat. How do these companies aggregate massive amounts of public data, and who buys their services? For those of us who use the internet and streaming services, how can we avoid ending up in these databases? Are there efficient ways to request data removal that aren't overly time-consuming, and what is a good balance between privacy efforts and convenience?

TRANSCRIPT

Corn

You know, Herman, I was looking at my phone the other day and I realized just how much of a trail we leave behind. It is not just the stuff we post on social media or the things we buy. It is like there is this invisible layer of the internet that is constantly watching, recording, and then selling our lives to the highest bidder. I was reading a report that the global data broker industry is projected to hit over four hundred and thirty billion dollars this year, in twenty twenty-six. That is a staggering amount of money being made off of information we often do not even know we are giving away.

Herman

Herman Poppleberry here, and you are absolutely right, Corn. It is a bit like walking through a city where every single person you pass is taking a photo of you, writing down what shoes you are wearing, and then meeting in a back alley to trade those notes for cash. Our friend and housemate Daniel was asking us about this recently. He sent over a prompt about the data broker industry, and it really struck a chord because it is something people often feel is just an urban legend or a minor annoyance. But in reality, it is a massive, highly sophisticated industry that knows more about us than we probably know about ourselves. Daniel wanted to know how they aggregate this data, who buys it, and most importantly, how we can actually protect ourselves without living like hermits.

Corn

It is funny you say that. Daniel was wondering if these companies are actually a legitimate privacy threat or if it is just a bit of a bogeyman scenario. I think for a lot of people, the term data broker sounds like something out of a cyberpunk novel. But when you start looking at the sheer volume of information they handle, it is staggering. We are talking about thousands of data points on almost every adult in the developed world. And it is not just the shadowy companies anymore. Even the big players have had to pivot. Remember back in twenty twenty-four when Oracle, one of the biggest names in the business, actually shut down its entire advertising and data arm? They cited the massive shift in privacy regulations and the decline in revenue. When a giant like Oracle walks away from a two billion dollar business, you know the landscape is shifting.

Herman

Exactly. And I love that Daniel brought this up because it bridges that gap between high tech surveillance and our everyday lives. These companies are not just some shadowy figures in a basement. They are massive, publicly traded corporations. You have the big credit bureaus like Experian, Equifax, and TransUnion, who have been doing this for decades. Then you have companies like Acxiom, Epsilon, and CoreLogic. They started with mailing lists and credit reports, and they have just scaled up to the digital age with frightening efficiency. They have essentially become the librarians of our private lives, except they are selling the library cards to anyone with a checkbook.

Corn

So, let us get into the mechanics of it. How are they actually getting this data? I mean, I do not remember signing a contract with a company called Acxiom. If I am just using a streaming service like Netflix or browsing a news site, how does my data end up in their hands?

Herman

That is the fascinating, and frankly, frustrating part. It is a multi pronged approach. First, there is public data. We are talking about property records, marriage licenses, voter registration files, and even court records. If it is in a government database, a data broker has probably scraped it. But then you have the commercial side. Every time you use a loyalty card at the grocery store, that data is often sold. Every time you sign up for a free app and agree to those fifty page terms and conditions, you are likely giving that app permission to share your data with third parties. But the real engine of the industry today is something called Real Time Bidding, or R T B.

Corn

I have heard that term. Is that the auction that happens in the milliseconds it takes for a webpage to load?

Herman

Precisely. When you click on a website, before the page even finishes loading, an auction takes place. Your browser sends out a bid request that includes your location, your device type, your browsing history, and sometimes even your interests. Hundreds of companies bid on the right to show you an ad. Even if a company loses the bid, they still get to see that data. It is a massive, constant leak of personal information that happens billions of times a day. It is the primary way that brokers keep their profiles updated in real time.

Corn

Right, and those third parties are the brokers. I remember we touched on this a bit back in episode ninety eight when we were talking about financial A P Is. The way data flows between these entities is often invisible to the user. It is not like there is a pop up saying, hey, we are selling your purchase history to a broker in Nebraska today. It is all hidden in the fine print. And it is not just what we do online. It is where we go in the physical world.

Herman

And it goes even deeper than just what you buy. Think about your smartphone. Many apps use what are called Software Development Kits, or S D Ks. These are pre built blocks of code provided by third party companies to help app developers with things like analytics, maps, or advertising. Those S D Ks can be collecting your location data, your device I D, and even information about other apps you have installed. They bundle that up and send it back to the broker. So, even if the app itself seems harmless, like a simple flashlight app or a weather app, it could be a pipeline for your personal information. There was a famous case where a weather app was caught selling precise location data to a broker that then sold it to hedge funds to track foot traffic at retail stores.

Corn

That is a great point. It is like the app is a Trojan horse for the broker. But what I find really interesting is the concept of the shadow profile. Even if you are someone who is very careful and you do not use social media, these brokers can still build a remarkably accurate profile of you by triangulating data from your friends, your family, and your public records. They can guess your age, your income level, your political leanings, and even your health concerns just by looking at the people you live with or the neighborhood you live in. In twenty twenty-six, with the rise of generative A I, these brokers are now using large language models to fill in the gaps of our lives with terrifying accuracy.

Herman

It is all about pattern recognition and large scale aggregation. If you have a thousand data points, you can fill in the blanks for the missing five hundred with a high degree of accuracy. It is predictive modeling. And this leads directly into Daniel's other question, which is, who is buying this stuff? Why is this information so valuable?

Corn

Well, the obvious answer is marketers, right? They want to show you an ad for a lawnmower because they know you just bought a house with a big yard. But I suspect the list of buyers is much longer and more diverse than just retailers.

Herman

Oh, it is much broader. You have insurance companies who want to assess risk. This is where it gets scary. If they see you are buying a lot of high calorie food or searching for information about certain medical conditions, that might influence your premiums or your eligibility. It is called dynamic pricing, and it is becoming more common. Then you have banks and credit lenders who use this data to supplement traditional credit scores. There are even risk mitigation firms that sell data to employers for background checks. And perhaps most concerningly, government agencies often buy this data.

Corn

That is the data broker loophole we have talked about. If the government needs a warrant to track your location directly from your phone provider, they can often just bypass the Fourth Amendment by buying that same location history from a broker who bought it from a weather app. It is essentially outsourcing surveillance to the private sector. I know there has been a lot of talk in Congress about the Fourth Amendment Is Not For Sale Act, but as of early twenty twenty-six, that loophole is still being exploited by agencies like I C E and the D H S.

Herman

It absolutely is. And because these are private transactions, there is very little transparency or oversight. Most people do not even know which brokers have their data, let alone what that data says about them. It could be full of errors. Imagine being denied a loan or having your insurance rates spike because a broker incorrectly flagged you as a high risk individual based on a neighbor's search history. You would have no way of knowing and no easy way to fix it.

Corn

So, if we accept that this is a pervasive problem, how do we actually fight back? Daniel was asking about how to avoid ending up in these databases in the first place. For those of us who live in the modern world and use streaming services and the internet, is it even possible to stay off the grid?

Herman

It is extremely difficult to stay completely off the grid, but you can certainly reduce your footprint. The first step is what I call digital hygiene. You have to be ruthless with app permissions. Does your calculator app really need access to your location and your contacts? Probably not. You should also use privacy focused tools. Browsers like Firefox or Brave, and search engines like DuckDuckGo, do a lot more to block trackers than the standard options. But the biggest news for twenty twenty-six is actually a legal one. Have you heard about the California Delete Act, Corn?

Corn

I saw something about that! It is Senate Bill three sixty-two, right? I think the main platform just launched a couple of weeks ago.

Herman

Exactly! As of January first, twenty twenty-six, the California Privacy Protection Agency launched the D R O P platform. That stands for Delete Request and Opt Out Platform. It is a one stop shop for California residents. You go to one website, verify your identity, and with a single click, you can tell every single registered data broker in the state to delete your data and stop tracking you. It is a game changer. The brokers have forty-five days to comply once they receive the request. While it is currently just for California, it is setting a massive precedent that other states are already starting to follow.

Corn

That is a huge win for consumers. But for those of us not in California, or for the thousands of brokers not covered by that specific law, what else can we do? I also find that using masked emails and virtual credit cards can be a huge help. If you sign up for a streaming service with a unique email address and a virtual card that is tied only to that service, it makes it much harder for a broker to link that data to your primary identity. It breaks the chain of attribution.

Herman

That is a pro move, Corn. It is about creating silos for your data. If every service you use thinks you are a slightly different person, the brokers have a much harder time stitching those pieces together into a coherent profile. But then there is the problem of the data that is already out there. Daniel asked about requesting data removal. Is there an efficient way to do that? Because I have tried doing it manually, and it is a nightmare.

Corn

It really is a full time job. You have to find the opt out page for each individual broker, and they do not exactly make it easy. They often use what are called dark patterns. They might require you to upload a copy of your driver's license or provide even more personal information just to prove who you are, which feels incredibly counterintuitive. You are giving more data to a company you want to delete your data. It is a psychological barrier designed to make you give up.

Herman

It really is. However, this is where those automated removal services come in. Companies like DeleteMe, Incogni, or Privacy Bee. They basically act as your agent. You pay them a subscription fee, usually around one hundred dollars a year, and they go out and send those legal requests to hundreds of data brokers on your behalf. They also monitor the sites to make sure your data does not reappear, because these companies are notorious for re scraping your info a few months after you delete it. For most people, this is the only realistic way to handle the problem without losing your mind.

Corn

I think that is the answer to Daniel's question about the balance between privacy and convenience. Is it worth the money? For me, the answer is yes, because my time is worth more than that. But I also think it depends on your personal risk profile. If you are someone in a sensitive profession, or if you have a history of being stalked or harassed, this kind of service is almost essential. For the average person, it is about peace of mind. It is knowing that your home address and phone number are not just one Google search away on a people search site.

Herman

Those people search sites are a specific breed of data broker that is particularly nasty. Sites like Whitepages or Spokeo. They take all that aggregated data and put it behind a paywall for anyone to see. It is essentially a menu for identity thieves and doxxers. Using an automated service to scrub those specific sites is probably the highest impact thing you can do for your immediate physical and digital safety. It is about making yourself a harder target.

Corn

I like that. Being a harder target. It reminds me of what we discussed in episode two hundred and eighteen about the agentic mesh. As A I agents become more prevalent in twenty twenty-six, they are going to be the ones navigating these databases. If your data is clean and your footprint is small, your personal A I agent is going to have a much easier time protecting your interests and negotiating on your behalf without leaking your life story to every server it touches.

Herman

That is a great connection. We are moving into an era where our data is not just being used to show us ads, but to train models that will make decisions about our lives. The stakes are getting higher. If a data broker has a flawed profile of you, and an A I uses that profile to determine your creditworthiness or your suitability for a job, that has real world consequences. We are seeing more and more companies use third party data to train their internal A I for hiring and lending.

Corn

So, to wrap up Daniel's question about removal, I would say this: Start by doing a search for yourself. See what comes up on the first few pages of results. If you see your address and phone number on a site like MyLife or Radaris, try to remove those manually first to see how it feels. If you find it overwhelming, consider one of those subscription services for a year to get a clean slate. And if you live in California, get on that D R O P platform immediately. It is free and it is your right.

Herman

And for the everyday stuff, like streaming and browsing, use a V P N when you can, use a privacy focused browser, and most importantly, just be mindful. You do not have to be a hermit living in a cave in the Galilee, but you should at least know where the cameras are. The goal is not total invisibility; it is agency. You should have a say in how your story is told.

Corn

Exactly. These data brokers are essentially writing a biography of us without our consent, and often with incorrect information. Taking back control of that narrative is a fundamental part of digital citizenship in twenty twenty-six. It is about reclaiming our autonomy in a world that wants to turn us into a spreadsheet.

Herman

I could not have said it better myself. It is a constant battle, but it is one worth fighting. And honestly, it is also about supporting legislation that puts the burden on the companies rather than the individuals. We need more laws like the Delete Act that require opt in consent by default, rather than making us opt out of a system we never joined in the first place.

Corn

That is the dream, Herman. But until then, we have to use the tools we have. I really appreciate Daniel sending this in. It is one of those topics that feels heavy, but once you break it down into actionable steps, it feels much more manageable. It is about incremental progress. Every tracker you block and every account you silo is a win for your future self.

Herman

Definitely. And hey, if you are listening to this and you have found some value in our deep dives into these weird prompts, we would really appreciate it if you could leave us a review on your podcast app or on Spotify. It genuinely helps other curious minds find the show and helps us keep this collaboration going. We are up to almost three hundred episodes now, and it is all thanks to you guys.

Corn

Yeah, it really does make a difference. We love hearing from you all. You can also find us at our website, myweirdprompts dot com. We have an R S S feed there for subscribers and a contact form if you want to send us your own weird prompts, just like Daniel does. We read every single one of them.

Herman

We are also on Spotify, of course. This has been My Weird Prompts. I am Herman Poppleberry.

Corn

And I am Corn. Thanks for joining us in the rabbit hole today. We will be back next week with another exploration of the things that keep us curious. Stay safe out there in the digital wild.

Herman

Until then, stay curious and stay private!

Corn

Bye everyone.

Herman

Take care!