Data Brokers

In This Module

- What are data brokers?

- What are some of the risks posed by data brokers?

- How can you manage the risks posed by data brokers?

Data Brokers

Data brokers are businesses that collect, store, package, and sell people's data to other companies, such as marketing firms or advertisers

What Do Data Brokers Do?

Data brokers are part of a whole economy centered around personal data. Data brokers obtain data, package it and categorize it, and then sell it to others, such as marketing firms.

Data brokers obtain their information using a few different tactics:

- They buy it from a third-party
- They look for it online using searching and public records
- They track you using cookies

Where Do Data Brokers Get Their Info?

Data brokers obtain their data through some of the following sources:

- Public records
- Your social media posts
- Your browsing history
- Your search history
- Your online purchases
- Smart home devices

Why Are Data Brokers an Issue?

Regulators, activists, and citizens are increasingly concerned about how data brokers:

- Operate in mysterious ways and lack transparency
- Gather huge amounts of data about people, often without their knowledge
- Sell people's data to places like marketing firms
- Subject people targeted ads and online tracking
- May use insecure systems that are vulnerable to hacks

Discussion

What other risks or issues do you think are associated with data brokers?

How to Remove Your Data

To remove your data from data broker sites, try:

- Opting out of each site one at time

- For guidance on how to do this, see:

  - [The Big Ass Data Broker Opt-Out List](#)

  - [DeleteMe Opt-Out Guides](#)

How to Remove Your Data

You may also consider using paid services that remove your data from data brokers for you. DeleteMe is one such service.

 These services can be expensive though and you should be aware of what you are agreeing to before signing up for one.

Signing up for Opt-Out Lists

A few options for getting off of lists of bothersome data brokers include:

- The [National Do Not Call Registry](#) to remove yourself from telemarketer databases and stop telemarketing calls
- [DMAChoice](#) to remove yourself from direct marketing lists
- [OptOutPreScreen](#) to get yourself off of lists for things like credit card or loan offers

Managing Your Online Presence

- Practice data minimization
- Be mindful of the information you are post and share
- Be aware of who has access to that information
- Audit your social media posts
- Delete things that reveal too much personal information
- Manage your social media settings, browser history and settings, and ad settings to keep your information more secure

Browse More Securely

- Consider using a VPN to browse more privately and securely
- Use a browser dedicated to privacy (and one that doesn't store cookies or history) like [Brave](#)
- Use a private mobile device browser like [Firefox Focus](#) or [DuckDuckGo](#)

Have a Digital Security Plan

- Have a digital security plan to:
  - Maintain your account settings
  - Update passwords
  - Delete browser history
- Resources like the [Consumer Reports Security Planner](#) can help with this

Discussion

What other digital security approaches come to mind for you?

What strategies can you use to deal with the challenges posed by data brokers?

Takeaways

- Data brokers pose many serious issues and potential threats to digital security and individual privacy

- Data brokers are being debated and discussed by many organizations, and many groups dedicated to online privacy are seeking ways to lessen the threats posed by data brokers

- While data brokers pose serious issues, there are ways to remove your information from data brokers

- You can use many digital security best practices to keep your information secure and away from data brokers

Resources

The Big Ass Data Broker Opt-Out List (link)

DeleteMe Opt-Out Guides (link)

Electronic Frontier Foundation (link)

NYC Digital Safety

Privacy & Security