Data Brokers

Summer 2022 W231, Section 2, Tuesdays 6:30PM – Samantha Williams

OVERVIEW

Information is everywhere. You are constantly leaking a trail of breadcrumbs about yourself across all facets of your modern life online and offline. Geolocation of your phone or smartwatch, the health data collected by these devices, your circle of friends on social media, your political affiliations, what you watch on television, who your internet provider is, your telephone number, and all your prior home addresses are up for grabs if you know where to look. The organizations that know where to look go by many names: Information brokers, information resellers, database marketers, consumer data analytics, or data brokers but they all have the same goal – they make it their business to know as much about you as possible and then sell that information to anyone willing to pay for it. With sparse regulation, almost by design, the question, "what happens when the government purchases and uses this information?" should stop you in your tracks.

WHAT IS A DATA BROKER?

Think of data brokers as professional collectors of all the data that can be gathered about an individual. This includes geolocation data, health data, social media data, voter data, spending habits, income, age, email addresses, social security number, gender, education level, occupation data, financial data, hobbies and interests, home addresses, telephone numbers, and a person's full name. A study done by the Federal Trade Commission (FTC) in 2014 of 9 different Data

Brokers found that a single data broker can have billions of data points for almost every consumer in the United States.[1] The FTC's analysis discovered that 1.4 billion consumer transactions and more than 700 billion aggregated data elements were held by a single data broker. The agency also found that 3 billion new records were being added every month by one data broker and another had over one trillion dollars in consumer transactions contained within their database. Finally, one of the nine data brokers included in the study had 3000 data segments for nearly every U.S. consumer. Technology has advanced substantially in the last 8 years since that study was conducted, including the efficiency in data processing, it is far more likely that these companies have petabytes of data for sale.

The collection of this data is done in several ways. Internet cookies are information jackpots in that they put a tiny snippet of code on your computer that acts as trackers to help remember some of the things you have looked or shopped for. While this can be a helpful way to be more efficient and productive, it also allows third-party trackers to follow you across the internet and collect information about your online activities. Loyalty cards operate a similar way in that they track all the places you use the card, frequency, and the types of items purchased. The famous case of Target inferring that a teen was pregnant based on her purchase history is an example of how her loyalty card data was used to market additional products to her.[2] Data brokers will also seek out all publicly available data such as public records (property tax, campaign contributions, etc.) and any information shared on social media. Free apps, games and services are free because

---

[1] Federal Trade Commission, (2014, May), *Data Brokers: A Call For Transparency and Accountability*, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

[2] Hill, K. (2016, April 1). How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did. Forbes. https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=13d232466668

they sell your data, which is what their real product is. In 2021, it was reported that LinkedIn made more than $3 billion over 12 months by selling access to its more than 700 million users to advertisers.[3] The free app, Muslim Pro, which was downloaded 98 million times was investigated and found to be sharing the location data of its users to government agencies such as ICE, U.S. Special Operations Command and CBP.[4] The FTC went after a free flashlight app for similar violations because the app deceived users by not telling them they sold their data in the terms and conditions or privacy policy.[5] Finally, data brokers get their data from third parties including other data brokers.

Once this data is collected, the information is aggregated into groups such as: compulsive buyers, newlyweds, pregnant women, people with depression and substance abuse. A Data Broker called MEDbase 200, landed a congressional hearing in 2013 for the sale of 1000 profiles for $79 for such lists as “Rape Suffers”, “AIDS/HIV Suffers”, and “Erectile Disfunction Suffers.”[6] Politicians were outraged, but not enough to carry on with the task of regulating some of the more distasteful practices of data brokers.

WHO IS A DATA BROKER?

There are three types of data brokers. Companies that sell data for marketing purposes (Acxiom & Oracle), companies that are subject to the Federal Credit Reporting Act (Equifax, Experion,

---

[3] Graham, M. (2021, April 28). *Microsoft says LinkedIn topped $3 billion in ad revenue in the last year, outpacing Snap and Pinterest*. CNBC. https://www.cnbc.com/2021/04/27/microsoft-linkedin-topped-3-billion-in-ad-revenue-in-last-year.html
[4] Cox, J. (2020, November 16). *How the U.S. Military Buys Location Data from Ordinary Apps*. Vice. https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x
[5] FTC. (2014, April 10). *FTC Approves Final Order Settling Charges Against Flashlight App Creator*. Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2014/04/ftc-approves-final-order-settling-charges-against-flashlight-app-creator
[6] Hill, K. (2013, December 19). *Data Broker Was Selling Lists Of Rape Victims, Alcoholics, and “Erectile Dysfunction Sufferers.”* Forbes. https://www.forbes.com/sites/kashmirhill/2013/12/19/data-broker-was-selling-lists-of-rape-alcoholism-and-erectile-dysfunction-sufferers/?sh=664926b21d53

Transunion) and companies that offer services that locate individuals/detect fraud. (PeekYou, Pipl, Instant Checkmate). This final group is not regulated by the Federal Credit Reporting Act and does not sell data for marketing purposes. Many of these companies you have never heard of and it is unlikely you will encounter them going about your daily life. This is by design as they tend to be secretive about their practices. In 2020, 25 data broker companies spent $29 million combined in federal lobbying; for reference Facebook, Amazon and Google spent less than $20 million each in the same period.[7] It is estimated that there are around 540 individual data brokers in the United States.[8] This is only an estimate as there is no federally required registry for these types of companies.

WHO ARE DATA BROKERS' CUSTOMERS?

The goal of a data broker is to sell information to anyone who wants to create a personalized experience, verify credit worthiness, or provide location data for a specific group of data subjects. For example, a data broker might sell information to a company trying to market a widget and want to advertise to those searching for a similar widget online. The data broker is acting as the middleman and connecting the data user and the organization that purchased the information. In most cases, personally identifiable information (PII) is removed from the data set. However, a study conducted in 2019 found that "…99.98% of Americans would be correctly re-identified in any dataset using 15 demographic attributes."[9] Some data brokers do include PII,

[7] *The Little-Known Data Broker Industry Is Spending Big Bucks Lobbying Congress – The Markup*. (2021, April 1). The Markup. https://themarkup.org/privacy/2021/04/01/the-little-known-data-broker-industry-is-spending-big-bucks-lobbying-congress
[8] PrivacyRights.org. (2022, February 22). *Registered Data Brokers in the United States: 2021 | Privacy Rights Clearinghouse*. https://privacyrights.org/resources/registered-data-brokers-united-states-2021
[9] Rocher, L., Hendrickx, J.M. & de Montjoye, YA. Estimating the success of re-identifications in incomplete datasets using generative models. *Nat Commun* **10,** 3069 (2019). https://doi.org/10.1038/s41467-019-10933-3

but one could argue it is a reasonable use considering the benefit that it may provide such as credit verification or financial risk mitigation.

Our modern digital life is built on the buying and selling of data. It has become the economic backbone of the internet by providing free services in exchange for data. While there are a host of privacy concerns, lack of consent, transparency issues and general protections that should be addressed when it comes to corporations profiting from your information, there is one category of data broker customers that raises some serious concerns.

UNDERSTANDING THE PROBLEM – GOVERNMENT ACCESS

Of all the organizations/individuals that have access to this data, none is more alarming than the government. With the same access and ability to purchase this information (with our tax dollars), agencies can use it however they see fit, including against the US population. Agencies such as IRS, DOJ (including the FBI and the DEA), Department of Homeland Security (including Advanced Research Projects Agency, Customs and Border Protection, ICE, Secret Service), DOD, military, intelligence agencies, and state, and local law enforcement – have all purchased information from data brokers warrantlessly, without any need to publicly disclose their actions or be subjected to any oversight.[10] Because of a complete lack of regulation of this industry, a loophole the size of the Grand Canyon has gutted the Fourth Amendment. The right that protects people from unreasonable searches and seizures by the government. Not only are we weakening

[10] Sherman, J. (2021, August 23). *Data Brokers Know Where You Are—and Want to Sell That Intel*. Wired. https://www.wired.com/story/opinion-data-brokers-know-where-you-are-and-want-to-sell-that-intel/

our constitutional rights, but this information is available to foreign governments and agencies, creating a huge national security risk.

With unrestricted access, the US government can track down illegal immigrants, find suspected tax evaders, locate those who have jumped bail, and surveil private citizens of interest and politicians with conflicting agendas from the current administration. The government can manipulate our election process by serving up political ads that speak directly to your specific concerns or interests and by creating an echo chamber where contrasting ideas are censored from the discussion. Republican Reince Priebus has bragged in several interviews on national television about how data is used to identify, target, and advertise to constituents using information purchased from data brokers.[11]

CONSENT

Consent is complicated and is not the same thing as privacy. Users are bombarded with privacy policies, cookie notifications and terms and conditions, that are there more as a formality than to inform despite the Federal Trade Commission's best efforts to protect PII by enforcing the scant laws enacted by Congress. Companies design these documents to be intentionally long, full of legal terms and hard to understand. Many companies also limit a user's options of acceptance to only allow for consent. The option to download, print and email the document is not a substitution for the choice to decline. This makes consent an illusionary decision where individuals have lost the right to self-determination and free choice.

[11] Last Week Tonight [HBO]. (2022, April 11). *Data Brokers: Last Week Tonight with John Oliver (HBO)* [Video]. YouTube. https://www.youtube.com/watch?v=wqn3gR1WTcA

The practice of getting a user's consent is a shift of burden. Organizations have put it on the user to be informed of their policies and practices in real-time without much effort required for notification of changes. Most data brokers do not offer an opt-out option. For example, credit reporting data brokers have an opt-out of receiving marketing offers for credit but will still collect and report your credit data. Other data brokers such as those that people finding information allow data subjects to opt-out by providing more data to confirm their identification and limit it to only 5 years unless you fill out another set of paperwork. Finally, data brokers like Acxiom will allow for data corrections, but do not provide options to opt-out or be deleted.

In considering the Belmont report, the data subject is likely unaware they are a data subject to begin with meaning that no consent was directly given by the data subject to the data broker nor was consent given to the government when information was purchased from the data broker. This violates the first basic ethical principle, respect for persons, as data subjects are stripped of their autonomy.[12] Additionally, there are no limits for protected classes or groups such as children, illness suffers, or marginalized groups leaving plenty of room for the remaining two principles, beneficence and justice to also be routinely violated by the government's use of this data.

Furthermore, we fail to account for the information that the government infers or calculates about a person based on the data that they have purchased. New state laws restricting abortions are being enacted almost daily since the overturning of Roe v. Wade. Period and pregnancy

[12] Office for Human Research Protections (OHRP). (1979, April 18). The Belmont Report. HHS.Gov. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html

tracking apps are selling user data, in states where the government can buy this data to identify women who likely got an abortion and prosecute them. Consent was provided to the initial apps but how far should that consent stretch before justice becomes one-sided in favor of the government? Can a user even consent to the use of information that is calculated or inferred about them?

PRIVACY

In Solove's paper, *A Taxonomy of Privacy*, he points out that privacy is hard a thing to pin down. What each of us considers private is dependent on a variety of factors including to whom information is being shared. Instead of trying to define the concept of privacy, Solove designed his Taxonomy of Privacy which is comprised of four activities with the purpose to "aid in the development of the law that addresses privacy."[13] Solove identifies the first activity that impacts privacy as information collection made up of two subcategories; surveillance, and interrogation. Data brokers are essentially doing the leg work of surveilling consumers by collecting all known data points about an individual and selling that information to the government. This leaves data subjects open for additional questioning or information probing by either entity. Information processing makes up the second group of activities that address the way data is manipulated, used, and stored. It is made up of five subcategories: aggregation, identification, insecurity, secondary use, and exclusion. Data brokers and the government manage to execute each of these subcategories with ease. Think of the data breach by Equifax (insecurity) or the fact that we cannot know exactly what data the government has about us (exclusion). Information dissemination makes up the third group that includes activities that transfers PII to others. Since

[13] Solove, Daniel J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review,* 154:3 (January 2006), https://ssrn.com/abstract=667622

the government is more than happy to pool its resources and share the data they have purchased they manage to check off all 7 of the subcategories in this group. The final group Solove identifies is invasion and it specifically address the invasion of privacy. Privacy is something so sacred to this country that is addressed it in the first, third, fourth, fifth, ninth and fourteenth amendment.[14] By allowing the government to purchase information from data brokers, each of Solove's four groups that can be used to construct better laws for privacy protections are violated.

A report by Wang et al., (2022)., found that the government agency known as ICE has several contracts with data brokers to increase its surveillance in the pursuit of deporting illegal immigrants. By purchasing this information ICE amassed a database that includes Biometric Data, Geolocation Data, telecom data, public record data and data purchased by other government agencies of the US population at large.[15] That is a database of legal residents and citizens that have no reason to be an ICE data subject. This practice infringes on all four groups of Solove's taxonomy. It also violates the HEW Report's five basic principles: transparency, individual participation, limitations of purpose, data accuracy, and data integrity which was intended to safeguard PII contained in data systems. The HEW Report is the framework for the Fair Information Practice Principles (FIPPs).[16] According to the DHS who oversees ICE, FIPPs

[14] F. (2019, September 30). *Is There a Right to Privacy Amendment?* Findlaw. https://www.findlaw.com/injury/torts-and-personal-injuries/is-there-a-right-to-privacy-amendment.html#:%7E:text=Fourth%20Amendment%3A%20Protects%20the%20right,the%20protection%20of%20private%20information.

[15] Wang, N., McDonald, A., Bateyko, D., & Tucker, E. (2022, May). *American Dragnet, Data-Driven Deportation in the 21st Century*. Center on Privacy & Technology at Georgetown Law. https://americandragnet.org

[16] U.S. Department of Health, Education *and Welfare.* (July 1973) *Records, Computers and the Rights of Citizens,* Retrieved May 19, 2022, from https://aspe.hhs.gov/reports/records-computers-rights-citizens

is used to inform the department's treatment of PII.[17] However, ICE has been able to blur these ethical lines at the cost of US populations privacy.

LEGAL PROTECTIONS

In the United States protections of data subjects are limited at best. The FTC is the body responsible for ensuring the protection of PII but it stops there. And while we have constitutional amendments around privacy, there is nothing that guarantees your rights to your data, making it so easily available for purchase. At the federal level, the Federal Credit Reporting Act provides protections to data subjects by ensuring accuracy, fairness, and privacy of consumer information as it pertains to financial data collected by companies like Equifax, Experian and Transunion. The law regulates the way data can be collected, accessed, used and shared. However, it does not provide data subjects the option to not be included.

At the state level, California and Vermont are the only two states that have laws that data brokers register with the state and disclose how data subjects can opt out or have their data deleted if that is allowed. Failure to register with the state has a fine of $100 or $50 per day respectively rendering these laws toothless for most of the data brokers with annual revenues in the billions.[18]

The California Consumer Privacy Act (CCPA) which went into effect on January 1, 2020, does provide more protections for California residents. These include the right to know what data is

[17] Fair Information Practice Principles (FIPPs) in the Information Sharing Environment. https://pspdata.blob.core.windows.net/webinarsandpodcasts/The_Fair_Information_Practice_Principles_in_the_Information_Sharing_Environment.pdf

[18] PrivacyRights.org. (2022, February 22). *Registered Data Brokers in the United States: 2021 | Privacy Rights Clearinghouse*. https://privacyrights.org/resources/registered-data-brokers-united-states-2021

being kept, the right to have your data deleted and the right to opt-out. Unfortunately, the law is limited in several ways. First, you can only opt-out from some data brokers, and it may not be forever. Many data brokers will start amassing your data again from other sources that you interact with over time, requiring repeated opt-out or deletion requests. Secondly, it is on the consumer to follow up and find out if they have in fact been deleted or opted out. And finally, there is no federal law that requires opt-out requests to be granted.

PROPOSED SOLUTIONS

At this juncture, it seems impossible to regulate all data brokers as an industry, but we can build laws around data usage as it pertains to government entities. Using the CCPA as a framework, Congress can enact a federal law that would create a universal right to opt-out, a right to be deleted, and the right to know and make corrections to data collected about individuals thus providing a degree of transparency, restoration of some privacy and possibly gathering a data subject's consent. A national registry would need to be created and include steeper financial penalties for failure to register or provide the appropriate steps to contact them regarding opt-outs, deletions, or information correction. Because all requests are made at the federal level, data subjects' choices could then be disseminated to all data brokers through the registry making enforcement a more manageable task. Congress can further limit the government's use of data brokers by banning the sale of information to any government agency domestic or foreign. This would restore many of the protections outlined in the Fourth Amendment of the Constitution and would require the government to proceed through the proper channels for searches and seizures. It would also mitigate some of our national security risks. Congress could further enact a law that would limit the use of this data to a specific time frame and restrict who has access and the

sharing of data across government agencies. While the FTC is the primary agency tasked with enforcement and penalties, a separate watchdog agency should be created to monitor compliance and adjudicate transgressions. Penalties should be clearly identified with an escalating penalization structure for failure to comply with any part of the law and citizens should be allowed to seek damages from any infractions that could have directly impacted them. Only with these in place will begin insulating ourselves from government abuses of our personal data.

REFLEXIVE STATEMENT

I am a biracial, able-bodied, cisgender, woman, wife, and mother in my late 30s. I belong to the upper-middle class, non-religious, unaffiliated voter block. I am the product of growing up among a family made up of newly arrived immigrants from all parts of the globe (Ghana, Lebanon, Philippines, China, and Ecuador) where I witnessed what it means to build your life in a foreign land. I had the privilege of seeing a variety of religions practiced, political sides chosen, and languages spoken.

My diverse upbringing highlighted how a government and its laws can be used to protect the people or exploit them for profit and power. As I have advanced in my marketing career, I have concluded that data has become a foundational part of every modern-day marketer's tool kit as it is increasingly used to drive the marketing mix of channel options, target demographics, buyer cycles, and content. As a marketing leader, this comes with a certain degree of power, as different marketing initiatives are designed to persuade, influence, and inform. If abused or not thoughtfully considered it can have serious impacts on the data subjects. The practice of data

science is not that different from marketing in this regard. Both require the person in power to consider who makes up the data and prevent predatory behavior. I cannot remove my biases, nor that of the organization that employs me, but I can acknowledge that they exist and seek out other perspectives from groups/segments that are not represented. I can also be an advocate for regulation especially when it comes to government uses circumventing laws. This should be a fundamental practice for all marketers, advertisers, data subjects and politicians. Because at the end of the day, this is about all our personal data, or privacy and our rights as individuals from our government.