The Hidden Cost of Data: Data Collection in American Society

Alexandria Farhat

College of Communication Arts and Sciences, Michigan State University

MI 304: Information and Society

Dr. Ruth Shillair

April 7th, 2025

The Hidden Cost of Data: Data Collection in American Society

Data collection- everyone's heard of it, but how many Americans truly understand just how much of their personal information isn't private or protected? So, what exactly is data collection and what are data brokers? Data brokers collect personal information about consumers from many different sources and then analyze and share that information with anyone willing to buy it (Arango, 2023), which is a lot of people! However data collection comes with many problems, a lot of which end up affecting the person whose data is being collected, not the data broker. One of the more significant reasons is the lack of laws protecting American's sensitive information from being collected and sold, which will be discussed in this paper.

Data collection has become a huge source of profit in the last decade b in the United States but who is the one benefiting? The data broker industry started to emerge in the 1990s (Swartz, 2006) and started to take off by around 2004 (Bhatia, 2024). Data collection by data brokers is when companies gather a large amount of personal information about individuals from many different sources and compile it together (Bhatia, 2024). This data can be collected through many different ways such as an individual's online activities, public records, and by buying it from other companies and other data brokers. The type of data that is collected by these brokers is vast, but some examples include: names, addresses, phone numbers, email addresses, browsing history, location data, health data, and much more. Depending on the consumers' location this data can either be more or less protected. An example of what these brokers do with this data is Life360. In 2020 it was found that Life360 was selling precise location data of its customers without the express consent or knowledge of this happening (Arango, 2023). Another example in 2005 ChoicePoint, one of the largest information brokers at the time, revealed that scammers posing as legitimate businesses had opened accounts and accessed databases used for pre-

employment background checks and public record searches. On top of that ChoicePoint waited to inform consumers about this breach for several months, even though in California law it is required to notify consumers about data and security breaches that can put them at risk (Swartz,2006). The lack of accountability, ethics, and regulatory legislation should raise alarm bells for Americans but many do not know the extent to which this industry has grown and the lack of action by the American government to protect its citizens is disappointing.

Now that we've covered the basics of the data collection industry, why should you be concerned? The buying and selling of American data affects each and every citizen in the entire country. Currently, there is no federal limit on the amount as well as the type of data these data brokers can collect about consumers (Arango, 2023). Some states like Vermont and California have more rigorous legislation for residents in those states that allow consumers to opt out of data collection and even have their information deleted. However, these laws are yet to be implemented across the country and compared to European privacy laws are light years behind. But how does all of this really affect the average consumer? According to Cinnamon (2024) by 2020 the data broker market was estimated to be a $200 billion industry in the United States. The major reason for this is the lack of comprehensive privacy legislation to protect United States citizen's personal private information from being profited on. The sale of American data can become problematic because with enough money anyone can obtain this information. Identity fraudsters, bad actors, foreign adversaries, and many more, all of these entities can buy your data from a data broker and there is no limit to how they can use it once they have it. On top of that, the type of data these brokers are absolutely and universally prohibited from selling under U.S. federal law is practically nonexistent. This means that if they can get their hands on it, then they have the unlimited ability to sell your data to anyone they want, whenever they want to, as much

as they want. This includes social security numbers, locations, names, addresses, contact information, health information, and more.

What legislation in the United States does exist to protect United States citizens from data collection, data privacy, and the sale of data? Currently, there is no comprehensive federal legislation to protect consumers. There are a few states that have passed their own legislation that was mentioned previously, these states are Vermont and California. The few key pieces of legislation that are used to protect citizens were created in the 1990s, right as data collection and sale were taking off and before there was a big need for legislation to protect consumers. Some of the federal legislation that protects our data today include the Fair Credit Reporting Act of 1970 and its 2003 version, the Drivers Privacy Protection Act of 1994, HIPAA (1996), Gramm-Leach-Bliley Act of 1999 that governs the use of personal information collected by financial institutions, and a few others all created in the 1990s. The thing all of these legislation have in common is that none of these address data brokers and there seems to be no legislation that has been able to be passed into law to address concerns about the sale of data. However, there have been some proposed legislation such as the Fourth Amendment Is Not For Sale Act, which would “prohibit data brokers from selling U.S. citizen data to law enforcement and intelligence agencies "without court oversight” (Arango, 2023., p. 130). Along with this Act another has also been proposed to Congress it is the Protecting Americans' Data From Foreign Surveillance Act. While both of this legislation address more specific issues with data privacy and limit who this data is being sold to, they aren’t any form of overreaching protection that citizen require to prevent identity theft or more serious crimes. Both of these acts have been confirmed to have bipartisan support, yet both have stalled in Congress (Arango, 2023., p. 130). There is one piece of legislation that would be beneficial for American consumers and that is the DELETE Act.

This legislation was proposed to Congress and it mirrors California's own Delete Act. This legislation's main goal would "establish a centralized system to allow individuals to request the simultaneous deletion of their personal information across all data brokers, and for other purposes." (118th Congress, 2023) Having this passed into law would be a huge step for American citizens to gain control over the sale and collection of their sensitive information. The bad news is that despite being introduced in 2023, the bill is only in the 'introductory' stage of legislation and that is only one of the first steps out of the many it takes to get it passed as a law. All of these Acts would help address the emerging issues that American citizens are faced with when it comes to data privacy. Yet, none of these acts have been put into effect making them useless to citizens and leaving us just as unprotected as if they were never introduced.

The growing issue of data protection and data privacy in the United States will only continue to get worse without our government stepping in to help. The United States is decades behind European countries when it comes to protecting its citizen's privacy. While Americans have only a few laws that don't explicitly cover data privacy, the EU has been passing laws to protect its citizens. The European Union in 2018 enacted the General Data Protection Regulation (GDPR). This legislation is most characterized by its "stringent provisions, ensures transparency, consent, and accountability in the management of personal data. By instilling confidence in individuals that their personal data is gathered, stored, and utilized securely and legitimately" (Wu,Y., 2024). The GDPR has been recognized globally as providing protection for consumers. The US however, currently utilizes a "sectoral model" where businesses essentially self-regulate for privacy protection, making it much more ineffective and much less protective for consumers (Fairclough, 2016). This lack of protections in the United States has led to companies being able to possess massive amounts of personal information about citizens. This can lead to increased

cases of identity theft, fraud, surveillance and stalking, and even national security risks without proper regulation and protections.

As American citizens, there are several actions people can take to show their support for these proposed data privacy acts, all of which could potentially help expedite their transition into law. First, you can contact your elected Congress officials in both the House and Senate to show their support for the bills by finding their contact information on the congress members' website (congress.gov/members) or directly mailing them. Next, keep up to date with state-level initiatives and legislation and show support for any legislation that might come through or contact your state's elected officials. Finally, you can spread awareness about this issue to friends, family, and anyone else you might know. This is an issue that affects all Americans and transcends political alignment, spreading awareness can make a huge impact.

Works Cited

Arango, Steven Joseph. (2023). Data brokers: benefit or peril to u.s. national security?. *Ohio State Technology Law Journal, 20(1),* 107-138.

Bartlett, J. (2015). iSPY: How the internet buys and sells your secrets. In N. Merino (Ed.), *Opposing viewpoints: Privacy*. Greenhaven Press. (Reprinted from *Spectator*, 2013, December 7). https://link-gale-com.proxy1.cl.msu.edu/apps/doc/EJ3010434267/OVIC?u=msu_main&sid=bookmark-OVIC&xid=1b844d5f

Bhatia, R. (2024). *A loophole in the Fourth Amendment: The government's unregulated purchase of intimate health data*. *Washington Law Review Online, 98*(2), 67. https://digitalcommons.law.uw.edu/wlro/vol98/iss2/1

Cinnamon, M. (2024). *You have the right to be deleted: First Amendment challenges to data broker deletion laws*. *Georgetown Law Technology Review, 9*(II). https://ssrn.com/abstract=5009948

118th Congress. (2023). *Text - H.R.4311 - 118th Congress (2023-2024): Delete act | congress.gov | library of Congress*. H.R.4311 - DELETE Act. https://www.congress.gov/bill/118th-congress/house-bill/4311/text

Cozzens, Christopher. (2022). The patchwork privacy problem: how the united states' privacy regime fails to protect its businesses and data subjects. *Seton Hall Law Review, 52(4),* 1157-1182.

Farhad, A. Mohsin. (2024). Consumer data protection laws and their impact on business models in the tech industry. *Telecommunications Policy.* Volume 48, Issue 9.

Fairclough, Bradyn. (2016). Privacy piracy: the shortcomings of the united states' data privacy regime and how to fix it. *Journal of Corporation Law, 42(2),* 461-480.

Swartz, N. (2006). Data Brokers Must Be Regulated to Prevent Identity Thefts. In J. Carroll (Ed.), *Opposing Viewpoints*. *Privacy*. Greenhaven Press. (Reprinted from *Information Management Journal*, 2005, May-June, *39*, 20 (4)) https://link-gale-

com.proxy1.cl.msu.edu/apps/doc/EJ3010434230/OVIC?u=msu_main&sid=bookmark-OVIC&xid=b9ec2c54

Wong, W.H., Duncan, J. and Lake, D.A. (2025), Why data about people are so hard to govern. Regulation & Governance, 19: 236-252. https://doi.org/10.1111/rego.12591

Wu,Y. (2024).Balancing Data Protection and Data Utilization: Global Perspectives and Trends.Lecture Notes in Education Psychology and Public Media,44,134-140.