

John Daniel Norombaba

Professor Inman

ENGL B1A

30 November 2020

Addressing the Debacles of Data

In the digital age of connected devices and services, a complex series of zeros and ones easily translate into one's identity or brand. Consequently, both Google and Facebook use this data to serve curated or targeted advertisements to their users. The exploitation of data appears from within and throughout the Internet. With the rise of data breaches from the likes of Equifax (a major credit-reporting agency) and Yahoo (a search and email provider), the question of handling user data is now a global discussion, with answers presented by the European Union and State of California in the form of legislation. The United States must enact nationwide legislation to regulate technology-utilizing companies and their management of user data and privacy in order to maintain a safe Internet ecosystem by protecting Internet users from domestic and international, internal and external threats.

Within the European Union, the General Data Protection Regulation, or GDPR, establishes strong regulation over the collection of data. Matthew Crain and Anthony Nadler in *Political Manipulation and Internet Advertising Infrastructure* briefly discusses the GDPR's role. To citizens in the EU, the GDPR "...provides individuals with a range of data rights and privacy protections and is often cited as an international model for policymakers," (393). Meanwhile, with the implementation of the California Consumer Privacy Act, or CCPA, Californian users have similar rights, in comparison to the EU's counterpart. Specifically, the right to access

personal information and the right to be informed of data collection (Rothstein and Tovino 5).

Because of the GDPR acting as a direct model to the CCPA, the framework of implementation is already present on the domestic level. Internationally, the GDPR establishes precedence in answering the question on how companies should handle user data. Between the major power of the United States and the European Union, the US is overtly weak and is behind with data and privacy regulation. Because the GDPR and CCPA intend to give more rights to end-users, approving countrywide regulation would extend benefits to the larger audience of Internet users present in the United States.

Without privacy and data regulation, the traditional business model of technology companies will continue to harm users, as they are without repercussion, allow their users to be both the product and consumer. While simultaneously collecting data through cookies and other algorithms that track interactions across the Internet, the social media giant Facebook also allows third parties access to sell advertisements (*Knowledge@Wharton*, “Your Data Is Shared and Sold...What’s Being Done About It?”). Through a lack of mandated data security on their back end, Facebook’s business model implicitly favors their third parties over users. Users are vulnerable, as the lack of transparency allows malicious data use. On an internal level, the possible exploitation leaves leeway for Facebook employees themselves to access or manipulate users and or their data, a level where regulators could closely investigate. This infrastructure is not only present on Facebook, but also on digital advertising as a whole. Matthew Crain and Anthony Nadler in *Political Manipulation and Internet Advertising Infrastructure* examine the role digital advertises plays into political manipulation. These capacities explain the infrastructure of Internet advertising:

The first is the capacity to use consumer monitoring to develop detailed consumer profiles.

The second is the capacity to target highly segmented audiences with strategic messaging across devices and contexts. The third is the capacity to automate and optimize tactical elements of influence campaigns. (376)

What drives platforms like Facebook, Google, and others solely rely on the users who use their platforms. The first capacity strongly alludes that between companies and their users, there is no indication of privacy; there is no clear and transparent choice. Those who work with providers of advertisements raise an ethical question of the collateral created by a campaign; the end goal is never about the users but is always about the profit and reach. With the third capacity to automate and optimize, these user profiles dangerously threaten the individuality of digital users, as their privacy disappears between the platform's lines of code. In Ellen Kennerly's "Privacy and the Internet", Kennerly analyzes the discussion of Internet privacy and data breaches. When Experian, a major credit reporter in the US sold data to Alteryx, a software company in California, a data breach exposed that the data sold, "...contained millions of records about U.S. households..." unbeknownst to Experian's clients ("Privacy and the Internet"). Unfettered data collection, without consent, consequently, jeopardizes users and raises flags on the ethics of companies. Prioritizing business endangers users not only on a social level, but to an economic and livelihood level, as real threats like identity theft and fraud are present within the world. Protecting Internet users from these threats involves protecting users from not only external forces, but the internal forces utilizing technology.

With national security, the major influence companies and platforms have over the data they collect place businesses and the sociopolitical climate at strong risk for the United States

and their users. In the report, *Data is Dangerous*, specifically in “The Cases” Susan Ariel Aaronson analyzed the risks of data posed by different tech companies. Evidently, during the 2016 election cycle, Facebook’s lack of data protection allowed Cambridge Analytica to target voters through advertisements, and Russian ““malicious actors”” to gather data from staffers involved with political campaigns (9). The lack of transparency Facebook presents to their users created the strong influence Cambridge Analytica used to deliver targeted ads, while Russian entities with the intent of harm openly abused Facebook’s tools. As a result, the abuse of Facebook’s tools, due to the lack of regulation, poses a risk on the United States’ democratic institutions. Economically, businesses are at odds with their own platforms. Reporting on the anti-trust hearing of Amazon, Apple, Alphabet (Google), and Facebook, Bobby Allyn, Shannon Bond, and Alina Selyukh in an *NPR* article summarizes the probing questions each CEO faced. Lawmakers inquired CEO Jeff Bezos on whether Amazon used their seller’s data to benefit their own brands, to which he replied, ““I can't answer that question yes or no,”” (“Heads Of Amazon, Apple, Facebook And Google Testify On Big Tech's Power”) Since Jeff Bezos could neither confirm nor deny, his answer implies that Amazon establishes an unfair playing field for their products and their competitors. Amazon’s unethical business practices harms small businesses and other users attempting to serve products through their platform, as they dominate as an online retailer. Their personal ability to access their seller’s data carries the influence on specific markets, and the very own direction of Amazon’s personal brands and shares of stock.

Although maintaining the general notion that imposing data privacy regulations harms businesses, like the digital advertising industry, providing choices leaves benefits for users and no disadvantages for businesses. Published in the October 2014 issue of *Journal of Marketing*

Research, Catherine E. Tucker experiments with the engagement of internet ads when users are aware of control over their data. According to the data, "...Facebook users were nearly twice as likely to react positively to personalized ad content and click on personalized ads," with "...generally no economically significant change in their reactions to untargeted or merely targeted," (Tucker 557). Users more aware of how companies manage data respond better, and financially, the impact is slight. The data strongly conveys that digital advertising businesses benefit from a user's perception of security. Adopting user transparency, and providing a choice leaves no harm to businesses. Conversely, the lack of choice affects users more than businesses employing practices prioritizing the data from a user, rather than the user themselves. A study cited in "Political Manipulation and Internet Advertising Infrastructure" found in the *Journal of Information Policy* states that "68 percent of respondents found 'tracking online activity to tailor advertisements' to be unethical," (Crain and Nadler 395). Since users find the practices of internet advertising as unethical, allowing users to have a choice can vastly improve the negative feelings surrounding companies who manage large amounts of user data. Improving such a statistic helps strengthen the amount of control users have and the amount of data shared with companies, which overall sustains a healthy Internet ecosystem through consent.

Creating a better and motivating atmosphere is a start on repairing harm companies have experienced at the expense of their users. An individual's data alone holds power and influence, as seen with Facebook and the integrity of the 2016 election, and compromises small businesses, with Amazon supporting their own brands through private seller data. Without the backbone of user privacy and data regulation, the practices employed by some companies have resulted in serious harm to the users who trust companies to safely and responsibly use their information.

Breach after breach, scandal after scandal, the global conversation on data privacy has escalated and has some regions already implementing regulation. Companies alone cannot self-regulate, and with the European Union enacting the GDPR, and California with their Consumer Privacy Act, the spotlight is on the United States to establish a precedent, similar to their European counterparts. Legislation to regulate technology-utilizing companies and their management of user data and privacy in order to maintain a safe Internet ecosystem by protecting Internet users from foreign and domestic, internal and external threats.

Works Cited

- Aaronson, Susan Ariel. *The Cases*. Centre for International Governance Innovation, 2020, pp. 8–15, *Data Is Dangerous: Comparing the Risks That the United States, Canada and Germany See in Data Troves*, www.jstor.org/stable/resrep24303.9.
- Allyn, Bobby, et al. “Heads Of Amazon, Apple, Facebook And Google Testify On Big Tech’s Power.” NPR, npr, 29 July 2020, www.npr.org/2020/07/29/894802424/watch-heads-of-amazon-apple-facebook-and-google-testify-on-big-techs-power.
- Crain, Matthew, and Anthony Nadler. “Political Manipulation and Internet Advertising Infrastructure.” *Journal of Information Policy*, vol. 9, 2019, pp. 370–410. JSTOR, www.jstor.org/stable/10.5325/jinfopoli.9.2019.0370.
- Kennerly, Ellen. “Privacy and the Internet.” *CQ Researcher*, 9 Feb. 2018, pp. 121-44, library.cqpress.com/cqresearcher/cqresrre2018020900.
- Rothstein, Mark A., and Stacey A. Tovino. “California Takes the Lead on Data Privacy Law.” *The Hastings Center Report*, vol. 49, no. 5, Sept. 2019, pp. 4–5. EBSCOhost, doi:10.1002/hast.1042.
- Tucker, Catherine E. “Social Networks, Personalized Advertising, and Privacy Controls.” *Journal of Marketing Research*, vol. 51, no. 5, 2014, pp. 546–562., www.jstor.org/stable/43832316.
- “Your Data Is Shared and Sold...What’s Being Done About It?” *Knowledge@Wharton*, 28 Oct. 2020, knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done.