Consumerism and Privacy: How Consumer Data Collection Impacts Privacy

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Gabriel Morales

Spring 2022

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Sean M. Ferguson, Department of Engineering and Society

Consumerism and Privacy: How Consumer Data Collection Impacts Privacy

It is well known that almost all companies have gathered consumers' data to make business decisions that optimize profits. However, the rise of the internet has allowed corporations to use externally sourced data to develop databases that contain what is now called Big Data (VU, 2020). Much of this data is used to provide targeted advertisements and unique user experiences, but has also resulted in severe impacts on the privacy of the user's personal information and on consumer welfare.

Ashworth & Free (2006, p. 108) discuss how many of the practices used by tech companies to acquire this consumer information are either unavoidable or undetectable by users. This makes it so consumers are forced to either choose the convenience of these services or risk the misuse of their data. Additionally, researchers Kumar et al. (2010, pgs. 471-472) identify the concerns of untrustworthy agencies having personally identifiable information (PII) and "quasi-identifiers" (gender, age, and zip code) that can make users susceptible to re-identification through anonymized data. This can result from breaches of these agencies due to lack of proper security measures on PII or even experienced hackers who are able to bypass the agency's security. The authors explain the collection of these quasi-identifiers in general makes users statistically more susceptible to these "linking attacks" of re-identification. They suggest this can only be mitigated by introducing a new anonymity-preserving data collection technique or by not collecting the user's information if the agency does not meet the user's personal privacy constraints. Furthermore, André et al. (2017, p. 29) explains the paradox resulting from the use of artificial intelligence (AI) in micro-targeted marketing practices. They suggest that the over usage of micro-targeted marketing can sometimes backfire because consumers feel as though their ability to freely choose is inhibited by the AI technology that provides suggestions.

Tensions over data privacy and illegitimate data collection by privacy advocates, civil libertarians, tech companies, and advertisers is explored through these stakeholders' own publications and existing scholarship evaluating the construction of these concerns.

Commodification of Privacy and Psychological Justice

Previous research has been conducted by several individuals examining how different stakeholders analyze what data privacy is comprised of. For example, Baik (2020) conducts a case study on the California Consumer Privacy Act (CCPA) by examining the different points argued by corporate representatives and consumer advocates. They specifically identify seven major areas in which these stakeholders differed:

- The purpose of CCPA
- Definitions of personal information and consumer
- Operationalization of opt-out
- Non-discrimination rules
- Economic ramifications
- Consumer literacy
- Comparison with other privacy frameworks.

Using these seven identified areas, any form of legislation or policy can be examined from various perspectives and can provide insight on how each of the stakeholders feel they are impacted. These seven areas allow us to see each stakeholder's view on the purpose of a policy, what groups are being addressed, the expectation for opt-out procedures, policy biases towards a specific group, the policy's economic impacts, and how coherent the policy is to each stakeholder. Additionally, the author states in their findings that there are two frames of privacy,

where corporations view privacy as a commodity while consumers view it as a right. The goal of this author's research is to examine the dynamics that have shaped the United States privacy regulatory framework, specifically using CCPA as its reference since it was one of the first state privacy laws introduced in the U.S.

Additional research by Ashworth & Free (2006, pgs. 108-110), prior to the creation of CCPA, attempted to apply a psychologically informed understanding of how consumers and corporations conceptualize privacy concerns. They began by examining surveys and other research that have revealed that consumers care about their control over their personal information, especially when dealing with data collection techniques and its usage. Privacy concerns are heightened when consumers discover information is collected without their permission; however, there is less concern when permission is granted by the user. Furthermore, Ashworth & Free (2006, pg. 110-112) build off of the frame of exchange between consumer and a firm which is commonly seen in marketing interactions. This idea helps provide an understanding of how consumers can perceive this exchange as "unfair" when no benefit or negative outcome occurs as a result of providing personal information. Lastly, Ashworth & Free (2006, pgs. 112-116) use theories of psychological justice in an attempt to understand consumers' privacy concerns. Specifically, they examine distributive and procedural justice of consumers, where perceived justice references the outcomes of an event and procedural justice implies the fairness of the procedures involved. They suggest this knowledge of distributive and procedural justice can then be applied to current data collection techniques and help to understand how this idea of perceived justice affects the perception of what is considered a violation of one's privacy.

The purpose of this document is to use both frameworks to focus on practices of data collection for targeted marketing, the specific stakeholders' beliefs in this debate, and their response to legislation and regulations such as CCPA. These stakeholders include the American Civil Liberties Union (ACLU), Privacy International (PI), the Digital Advertising Alliance (DAA), Facebook, and Google. Similar to Baik's research (2020), I will be examining the two frames of thinking of privacy as either a commodity or a right, while also concentrating on stakeholders' definitions of personal information, operationalization of opt-out, non-discrimination rules, economic ramifications, consumer literacy, and comparisons with other privacy frameworks. Additionally, the examination of distributive and procedural justice explained by Ashworth & Free (2006) will also be used in defining each stakeholder's understanding of privacy and legitimate data collection.

Policy Studies of Stakeholders and Data Collection Practices

American Civil Liberties Union (ACLU), Facebook, and Federal Privacy Legislation

The ACLU is an organization that "works in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws of the United States guarantee everyone in this country " (ACLU, n.d.). This group has been heavily involved in demanding tech corporations to no longer self-regulate but be held accountable by federal privacy legislation. The ACLU has several projects in place to examine the practices of these tech companies and identify what they claim to be illegitimate data collection practices for financial gain. For example, Gillmor (2018) who is a part of the ACLU Speech, Privacy, and Technology Project states that "Facebook and other massive web companies represent a strong push toward unaccountable centralized social control" through their services. Additionally, Gillmor (2018) adds how he has "never 'opted in' to Facebook or any of the other big social

networks", yet they are still able to create a detailed profile about him and his interests. This was done through connections of others on Facebook's platform or through his browsing habits that are linked through web pages that incorporate Facebook's like button into their content.

This case is a prime example of the operationalization of opt-in, where Gillmor (2018) states he feels as though there is no option for him to consent to Facebook's data collection practices since Facebook has a "globe-spanning surveillance and targeting network" that cannot be avoided by internet users. This relates to the procedural justice of Facebook's data collection practices, where consumer advocates like Gillmor feel as though Facebook has crossed over the boundary of consent and attached itself to users who have explicitly avoided agreeing to its terms of service. Additionally, the discussion of privilege and discrimination is addressed by Gillmor as he describes how protection of privacy can be directly related to social contexts; those who cannot afford the time and expense to communicate with electoral representatives and political allies via other channels are forced to utilize social networks such as Facebook in order to communicate. Gillmor argues this results in privacy becoming a luxury good as many individuals such as journalists, organizers, politicians, and others feel the need to use Facebook for its scale and connectivity to other individuals while sacrificing their own personal privacy for this service.

After the passage of CCPA, the ACLU Senior Legislative Counsel Neema Singh Guliani (2018) warned that the tech industry's push from self-regulation to federal privacy legislation should not be seen as tech companies' efforts to have consumers' best interests in mind. Guliani (2018) believes these actions are "companies' efforts to weaken state-level consumer privacy protections." Guliani lists several state legislation efforts, such as the CCPA and Illinois legislation setting limits on commercial collection and storage of biometric information, that have resulted in the protection of consumer privacy. However, Guliani (2018) suggests that

private companies are seeking to put a stop to this by creating a "federal privacy framework that preempts state law." The lobbying effort of The Internet Association (which represents digital companies like Amazon, Airbnb, Google, etc.) and other tech companies (Facebook, IBM, and Microsoft) to push for these preemptive laws is seen by Guliani (2018) as an effort to create a federal law "wiping out — otherwise known as preempting — state protections." She argues this would be a "bad deal for consumers" because it would "likely put existing consumer protections, many of which are state-led, on the chopping block and leave states bound by a federal law that could prevent additional consumer privacy protections from ever seeing the light of day. State regulators could lose the authority to sue or fine companies that violate their laws. And consumers may even be barred from taking companies to court" (Guliani, 2018). This leads to her suggestion that federal legislation should not be avoided, rather that:

> "any such legislation must put consumers in control of their own data. It must require companies to clearly inform consumers about their data practices and get consent to retain, share or otherwise use consumer data. It must address coercive practices that condition services on consumers' consent to unnecessary data collection, and put in place limits on how data can be retained and used. And, perhaps most importantly, it must give the government a large stick for enforcement and consumers a way to take companies to court that violate privacy." (Guliani, 2018)

It is clear from Giuliani's points that there is a reference to exchange between companies and consumers that, with the passage of federal legislation, could potentially threaten the current state protections in place that are allowing this exchange to move closer to "fairness". Furthermore, Giuliani hints at the idea of unfair distributive justice that could result from the

implementation of generalized federal regulation, where the outcomes could solely benefit tech companies by allowing them to avoid prosecution by consumers for unlawful use of personal data.

Privacy International (PI) and Google/Alphabet Inc.

PI is another privacy advocate that has identified international tech companies that have shifted their focus to collecting large amounts of personal data, sometimes at the expense of the user, in order to better target their advertisements to consumers and remain competitive (PI, n.d.b). Specifically, PI explains how advertisement technology (AdTech) makes sense in that it provides users with free websites and services while allowing websites and developers to monetize their products and advertisers to reach their audiences (PI, n.d.a). However, PI (n.d.a) argues that in the past decade, AdTech has become increasingly more invasive with data collection in order to create effective targeted advertising. Furthermore, PI states that many of the advertisements can be discriminatory, manipulative, limit user control over how their data is being shared with third parties, and that shared personal data can come with a growing security risk if the data is breached or not protected. With these identified risks of AdTech, PI has taken strong efforts to support legislation such as the General Data Protection Regulation (GDPR) set by the EU and has attempted to hold companies accountable that may be practicing privacy-violating techniques for data collection.

In terms of the United States, PI has specifically identified Google as one of many "gatekeepers" that regulates how users access information on the web. They state that data collection is a way for large companies to dominate in the digital economy and has caused companies to overstep the boundary of "'just' affecting the realm of digital advertising" (PI, n.d.b). In an effort to protect the privacy of consumers, PI's Advocacy and Policy Team Lead

Tomaso Falchetta (2018) submitted a letter of comments to the Federal Trade Commission (FTC) covering several issues relating to the topic of the "intersection between privacy, big data and competition" (p. 1). In this letter, he encourages the FTC to examine the "information and power asymmetry between companies and users" which he argues has "significant implications for the privacy of users and for competition"(Falchetta, 2018, p. 1). Expanding upon this, he examines the pronounced power asymmetry where companies rely on consent for processing personal data. This places users in a position where they are forced to consent or else remain without access to the company's services. Falchetta (2018) states that this is an "imposition of terms and conditions that lock users into using services with poor privacy safeguards" (p. 2) and believes it is the direct result of business models of dominant companies that increasingly rely on users' data.

Further into the letter, he continues explaining how companies who exploit personal data often then view privacy and data protection legislation as a threat to their business model. He directly addresses Facebook who fears its "business may be negatively affected by privacy, data protection, consumer and competition laws" (Falchetta, 2018, p. 4). He also cites Google's parent company Alphabet Inc. and its 2017 Annual Report to the US Securities and Exchange Commission where it argues that "these legislative and regulatory proposals, if adopted . . . could, in addition to the possibility of fines, result in an order requiring that we change our data practices, which could have an adverse effect on our business and results of operations. Complying with these various laws could cause us to incur substantial costs or require us to change our business practices in a manner adverse to our business" (Falchetta, 2018, p. 4).

Falchetta believes this is because of a lack of competition in the market, resulting in current dominant companies not having the incentive to implement practices that promote

individual privacy. Additionally, he even notes that companies with market power can even seek to exclude privacy enhancing players to prevent competition from entering the market. An example from the letter is Google's ban of a mobile ad-blocker called Disconnect from the Google Play Store, which resulted in a $5.1 billion fine from the European anti-trust authority (Falchetta, 2018, p. 4). He closes section two of this letter, urging the FTC to develop explicit guidance on having privacy standards as "part of any assessment of the quality of a digital service for the purpose of determining competitiveness of a market " (Falchetta, 2018, p. 4).

All of the arguments made by PI can be viewed through the lens of exchange discussed by Ashworth & Free (2006) and the economic ramifications mentioned in Baik's (2020) work. Falchetta's first point about users choosing either services or privacy underscores this tension of exchange and how PI views this as unfair for consumers. This goes even a step further when referring to the "power asymmetry", which highlights the lack of distributive justice in the eyes of consumers. The injustice, from PI's point of view, is that companies are forcing users to relinquish their data and personal privacy so that companies can profit by using provided data to create targeted advertisements on their web services. For the consumer, there appears to be no advantages in this exchange since they not only sacrifice their privacy for services, but are now being targeted through advertisements based on this information they have given companies consent to collect.

On the other side of the debate, tech companies see privacy legislation as an economic ramification to their current business models as quoted by Falchetta in the Alphabet Inc.'s Form 10-K 2017 Annual Report (Alphabet Inc., 2017). Several times in the annual report, Alphabet Inc. (2017) refers to legislation like GDPR and CCPA as being "adverse to our business" because it will cause the company to "incur costs or require us [Alphabet Inc.] to change our

business practices" (p.11). Alphabet Inc. seems to emphasize the point of privacy regulations as a severe cost to its company, especially if it requires change to its current and very profitable business model. This is where PI argues on the subject of economic ramifications, saying that the lack of these standards and tech companies' willingness to adopt new practices is because of the fear of losing market power. Furthermore, PI argues that this is the result of privacy being seen as "a mere economic asset" by tech companies, rather than a right where "data protection laws must be construed as capable of limiting the application of competition law, when such application would result in a violation of users' rights to privacy and data protection" (Falchetta, 2018, p. 5).

Digital Advertising Alliance (DAA) and Self-Regulation Principles

The DAA is a collection of advertising and marketing trade associations that "establishes and enforces responsible privacy practices across the industry for relevant digital advertising" while also striving for transparency and control on the use of multi-site data and cross-app data gathering (DAA, n.d.a). The DAA has designed several principles for advertising practices and uses the BBBNP and ANA to investigate and enforce any violations that consumers, business entities, or other stakeholders have observed (DAA, n.d.b). Through these actions to enforce violations of consumer privacy, the DAA has been commended by the FTC in its efforts to "inform consumers of data practices, allow consumers to opt out of behavioral advertising, maintain reasonable security for the data collected, and refrain from using sensitive information for behavioral advertising without consumers' opt-in consent" (FTC, 2017, p. 1). The FTC Cross Device Tracking report (2017) also highlights the DAA as one of the leading organizations to specify guidance and provide principles to apply to online behavioral advertising. This made it a

distinguished organization that has been highly influential in the debate of data collection and targeted advertising.

In the DAA's (2009) Self-Regulator Principles for Online Behavioral Advertising, there are 7 principles present that correspond to the "'Self-Regulatory Principles for Online Behavioral Advertising' proposed by the Federal Trade Commission in February 2009" (p. 1). Additionally, the DAA (2009) defines behavioral advertising as "the collection of data online from a particular computer or device regarding Web viewing behaviors over time and across non-affiliate Web sites for the purpose of using such data to predict user preferences or interests to deliver advertising to that computer or device based on the preferences or interests inferred from such Web viewing behaviors" (p. 2). This definition sets the stage for how the DAA plans to explain the principles it will enforce. The 7 principles listed in the document are education, transparency, consumer control, data security, material changes, sensitive data, and accountability. These principles are defined as educating consumers about online behavioral advertising, fully disclosing and informing consumers about data collection, giving the consumer the choice to have data collected, the need for reasonable security, obtaining consent by the consumer for data collection changes, recognizing certain data is more sensitive than others, and having entities that will hold companies accountable to uphold these principles. Following the definition and need for these principles, the DAA gives clear steps for data collection entities to take which allows consumers to opt-out of data collection and also provide notifications at each stage of the data collection process so the consumer is aware of when and how their data is being used.

From these principles, it is clear that the DAA is heavily focused on data collection transparency with consumers and giving them the opportunity to opt-out during any stage of a company's collection process. They also focus on having strong consumer literacy where

consumers are aware of what type of personal data is being used and requiring companies to request consent whenever they plan on collecting new information. Most of these principles and practices suggested by the DAA focus on the procedural justice found in a company's data collection practices. The DAA views that a just practice of data collection requires that if companies want to have access to a consumer's set of data and use it across several device platforms, then they must inform the user of how it is distributing this data across devices, to what third-parties it is being shared with, and allowing the consumer to choose if they wish for this transfer to occur. This view of procedural justice ultimately argues that a single instance of consent to data collection on a device or platform should not be assumed to be carried over to other connected devices or related platforms unless explicitly agreed to by the consumer.

Conclusion

Data collection is still a growing issue that has begun to reach the discussion floor of many state and national legislatures in the United States. This paper has shed light on a few of the prominent figures involved in the development of these federal regulations, each with their own ideas of how equitable legislation for both consumers and tech companies should be constructed. As mentioned in Ashworth & Free's (2006) work, many of the arguments can be boiled down to the idea of exchange between consumers and companies, all of which have components of distributed and procedural justice. Additionally, as Baik (2020) alludes to in their work, much of these conflicts on justice lie within a mis-communication between the stakeholders on what opt-out, non-discrimination rules, economic ramifications, and consumer privacy should look like in a legal framework. Overall, these stakeholders mentioned have continued to test the current standards of consumer privacy in an effort to find the balance between providing an efficient and personalized experience while still respecting the privacy of

each user. This has opened the door to a deeper exploration of the practical and social impact that these digital services have on consumers in the United States and will continue to lay the foundation for future data-dependent services and federal legislation.

References

ACLU (n.d.). American Civil Liberties Union. Consumer privacy. https://www.aclu.org/issues/privacy-technology/consumer-privacy.

Alphabet Incorporated. (2017). Annual Report 2017. https://abc.xyz/investor/static/pdf/20171231_alphabet_10K.pdf

André, Q., Carmon, Z., Wertenbroch, K., Crum, A., Frank, D., Goldstein, W., Huber, J., van Boven, L., Weber, B., & Yang, H. (2017). Consumer choice and autonomy in the age of Artificial Intelligence and big data. *Customer Needs and Solutions*, *5*(1-2), 28–37. https://doi.org/10.1007/s40547-017-0085-8

Ashworth, L., & Free, C. (2006). Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns. *Journal of Business Ethics, 67*, 107–123. https://doi.org/10.1007/s10551-006-9007-7

Baik, J. (2020). Data Privacy against innovation or against discrimination?: The case of the california consumer privacy act (CCPA). *Telematics and Informatics, 52*, 101431. https://doi.org/10.1016/j.tele.2020.101431

DAA. (n.d.). Digital Advertising Alliance. About the Digital Advertising Alliance. https://digitaladvertisingalliance.org/about

DAA. (n.d.). Digital Advertising Alliance. Enforcement. https://digitaladvertisingalliance.org/enforcement

DAA. (July, 2009). Digital Advertising Alliance. Self-Regulatory Principles for Online Behavioral Advertising. https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/seven-principles-07-01-09.pdf

Falchetta, T. (August 20, 2018). *Submission to the US Federal Trade Commission on the intersection between privacy, big data, and competition* [Electronic Letter]. https://privacyinternational.org/sites/default/files/2018-09/PI%20comments%20on%20FTC%20Consultation%2020%20August%202018.pdf

FTC. (2017, January). Federal Trade Commission. Cross Device Tracking: An FTC Staff Report. https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf

Gillmor, D. K. (2018, April 5). Facebook is tracking me even though I'm not on Facebook. American Civil Liberties Union. https://www.aclu.org/blog/privacy-technology/internet-privacy/facebook-tracking-me-even-though-im-not-facebook

Guliani, N. S. (2018, October 5). Don't be fooled by the tech industry's push for federal privacy legislation. American Civil Liberties Union. https://www.aclu.org/blog/privacy-technology/internet-privacy/dont-be-fooled-tech-industrys-push-federal-privacy

Kumar, R., Gopal, R., & Garfinkel, R. (2010). Freedom of Privacy: Anonymous Data Collection with Respondent-Defined Privacy Protection. *Informs Journal on Computing, 22*(3), 471-481. https://doi.org/10.1287/ijoc.1090.0364

PI. (n.d.). Privacy International. Adtech: Privacy International. https://www.privacyinternational.org/learn/adtech

PI. (n.d.). Privacy International. Competition and Data. https://www.privacyinternational.org/learn/competition-and-data

VU. (2020, March 12). Villanova University. The Evolution of Data Collection and Analytics. https://taxandbusinessonline.villanova.edu/blog/the-evolution-of-data-collection-and-analytics/