The Ethics and Policy of Personal Data Exchanges

Maria A. Staszkiewicz

Submitted to the Philosophy, Politics and Economics Program at the University of Pennsylvania

in partial fulfillment of the requirements for Honors.

Thesis Advisor: Dr. Raj Patel

Date of Submission: April 24, 2023

THE ETHICS AND POLICY OF PERSONAL DATA EXCHANGES

ACKNOWLEDGEMENTS

This project would not have been possible without the support of numerous individuals. I benefited greatly from the guidance of my advisor, Dr. Raj Patel, who always made time to discuss my ideas. I am thankful for his expert supervision that instilled in me the confidence to pursue this thesis. Dr. Kate Dorsch's generous mentorship has been invaluable, too. Having the opportunity to look up to her during my time at Penn helped me envision the immense positive impact I can only strive to effectuate on those around me. I am also thankful to Dr. Jaron Cordero for encouraging me, time and again, to redirect my focus back to the premises from which I departed.

Indeed, the entire Philosophy, Politics, and Economics Department at Penn deserves a mention for its tireless work. Had it not been for its interdisciplinary approach to knowledge production, I would have hesitated to pursue as multifaceted of a research topic. I owe much of my academic fulfilment at Penn to the PPE faculty, administrators, and students constituting the department.

Lastly, my undergraduate experience, which this thesis culminates, was significantly enriched by friends and family whom I am beholden to for their tireless care. It is both a source of gratitude and an honor to be surrounded by so many who inspire me in the projects I undertake.

ABSTRACT

Regulatory efforts tend to fall behind developments in fast-growing fields. Such a lag is especially evident and alarming in the context of increasingly capable technology. Big data analytics, enhanced by machine learning, provide (usually corporate) agents with unprecedented access to control over individual consumers and social processes. Consumers' actions and decisions in commercial contexts are monitored and studied. The resulting insights inform business practices, such as methods of customer retention. Social processes, such as democratic elections, are impacted too when micro-targeting influences the choices of thousands.

The outlined consequences might seem disproportionate to the actions said to lead to them. After all, how can collecting consumers' data while respecting the prevailing law affect their decision-making or breach their privacy? In this thesis, I explore the ostensibly alarmist stance that personal-data-driven strategies of profit-making encroach on consumer rights, endanger democratic institutions, and enhance the power asymmetry characterizing the relationship of corporate persons to private clients.

Chapter 1 assesses existing and emerging approaches to protecting personal data privacy. Chapter 2 engages with the question of imposing moral duties toward customers on private sector enterprises. Chapter 3 discusses the deficient nature of extant policy governing personal data exchanges and proposes systems to strengthen regulatory measures.

In concluding that multifaceted policy reform is urgently needed, this thesis also draws from scholarship evidencing evolving preferences and social norms around information privacy. A synthesis of the interdisciplinary expertise of academics and practitioners of technology policy, business ethics, law, and behavioral economics proposes paths forward by combining approaches to privacy ranging from enhanced consumer protection requirements to antitrust law.

TABLE OF CONTENTS

INTRODUCTION

Access to online services such as social networks and e-commerce sites is typically dependent on the sharing of personal data. The information disclosed by means of allowing one's digital path to be tracked may be as basic as one's behavior on the website – for instance, time spent browsing – or as extensive as one's detailed profile, which might comprise the location from which a given service has been accessed, previous search history, and preferences inferred from online activity. It is relatively easy to deduce users' characteristics, including those which they would prefer to keep private, by automatically collecting and analyzing a few pieces of data quantifying their behavior.

Consider the examples of social media services (Facebook, Instagram, and TikTok), consumer goods websites (Amazon), and search engines (Google). Harvesting and recycling information about individual users is at the heart of their business models. Note that while there is no monetary payment associated with accessing these sites, few other digital products are expected to demonstrate substantial growth and profit without charging user fees. Is access to consumers' digital tracks truly that valuable?

Facebook (now Meta Platforms) held its initial public offering in 2012. At $38 per share, the company was valued at a record $104 billion (Raice et al., 2012). However, its preceding annual report listed a relatively modest $6.3 billion in total assets (Facebook, 2012). Hence, the staggering (roughly 16:1) ratio likely stemmed from intangible assets capable of fueling the company's operations and further expansion. Given that most of Facebook's revenue comes from fees paid by advertising agencies vying for the social network's large (and, back in 2012, rapidly growing) user base, Facebook's value lies in its ability to monetize individual consumers (Meta, 2023). Specifically, it derives extraordinary profits from the capacity to micro-target at a

large scale by tailoring advertisement (ad) delivery to reach the users most likely to engage with the content, thus minimizing advertisers' cost per ad impression (engagement with the advertisement) unlike any available alternative.[1]

Meta Platforms' algorithms automatically discern between high- and low-ad-engagement users when selecting which ads to present to whom (*United States of America v. Meta Platforms*, 2022). As such, Facebook (and other platforms offering similar advertising services, such as Google), can allow marketing departments to target solely that demographic which they wish to reach – most often simply the one comprised of individuals most likely to make a purchase.

Yet discerning between users based on the likelihood that they are interested in, willing to, and financially capable of buying the object of a given advertisement can prove problematic when pursuing a given group of consumers leads to excluding others, especially when the others constitute a protected class. In a recent case, Facebook's algorithm used characteristics protected by the Fair Housing Act. Consequently, the Department of Housing & Urban Development (HUD) charged Facebook with discriminatory practices in a now-settled lawsuit (which has first been transferred to the Department of Justice). HUD claimed that targeting only those individuals who were likely to engage with housing-related advertisements "denied persons information about housing opportunities" on the basis of characteristics such as race and disability, thus violating the Fair Housing Act (*United States of America v. Meta Platforms*, 2022). The charge of discrimination was taken up by the Department of Justice. The facts of the lawsuit reveal that Facebook's potentially inequitable advertising tools are automated to the extent that they prevent advertising agencies from reaching a diverse user base even when these

[1] Alternatives have, of course, emerged since Facebook's incorporation. However, Meta Platforms – Facebook's parent company – acquired much of its U.S.-based competition, e.g., Instagram. As such, Meta remains one the premier firms offering vast advertising capabilities.

agencies specify that underrepresented groups are those that they want to reach (*United States of America v. Meta Platforms*, 2022). The probability of engagement with the ad thus wholly dictates who sees it.[2]

How are these advertising practices linked to privacy and what are the implications of enabling such far-reaching data collection capabilities and such high degree of automation? First, be they humans or machines, marketers derive information that guides strategy toward maximum engagement at the lowest possible cost from analysis of consumer behaviors and preferences. Those can be learned by surveying individuals and groups or by observing them. However, given the resource-intensive nature of conducting representative surveys and the relative ease of collecting data by quantifying observed behavior, the datafication of online habits has become the norm. Datafication refers to recording and quantifying information that has not been aggregated in such a way before the rise of data-intensive services and platforms (Cukier & Mayer-Schoenberger, 2013). Such collection can occur in transparent or clandestine ways. Yet, regardless of whether users are aware that their behavior is being analyzed, the fact that ubiquitous observation and data collection have become the norm is at the heart of the phenomenon of "all-knowing" marketers.

Second on the list of implications of ubiquitous, automated data collection is the increasingly blurred boundary separating the private and public spheres. Platforms such as social networking sites are public fora owned by private entities. Information exchanged on them can, on one hand, be entirely personal or, on the other hand, affect thousands, if not millions of

[2] This implies two things. One, the algorithm is, admittedly, indiscriminate in regard to user characteristics beyond those that dictate engagement probability. Two, its blindness to other factors can make it discriminate based on those factors regardless. If, e.g., discretionary income tracks race and an ad agency wants to target high-income individuals, then low-income users, who may over-represent certain races and under-represent others, will be excluded. As such, ethical algorithm design may be advised as a more equitable alternative. It is beyond the scope of this thesis, but to learn more, see, for instance, Kearns & Roth (2019).

people. The extent to which the state can regulate spaces owned, operated, and moderated by non-state enterprises might depend on the objectives of such regulation. For instance, the Federal Bureau of Investigation (FBI) or the National Security Agency (NSA) may request data stored in Meta Platforms' servers to further an inquiry into a potential risk to national defense or into a suspect in a criminal trial. Meta has seen a steady increase in government requests for data, as have Google, TikTok, and Amazon.[3] Note that national security requests specifically are often excluded from these general reports (or reported in legally mandated broad ranges with delay), which reflect government data requests that have to do with criminal, civil, and administrative purposes.

Surely, there is value in using data to protect the security of individuals and states. However, there are clear risks for privacy associated with already available surveillance methods and increasingly advanced analytics capable of anticipating crimes that have yet to be committed. Considering that liberal justice systems, including the U.S. one, rest on the presumption of innocence, growing surveillance capabilities may come to exemplify a slippery slope descent into policing intentions rather than actions (Cukier & Mayer-Schoenberger, 2013).

Third, combining data sets and deploying machine learning on partial information can teach third parties what the individual never disclosed (to the particular entity or at all) and may never have wanted to be known about them. For instance, Target's highly accurate algorithm for targeting customers who are likely to purchase certain products can successfully deduce whether clients are pregnant based on their shopping lists and before they share the news with their

[3] Meta's data on U.S. national security requests can be found at *www.transparency.fb.com/data/government-data-requests/country/US/;* Google's – at *transparencyreport.google.co;* and TikTok's – at *www.tiktok.com/transparency/en-us/information-requests-2022-1/.* Amazon's data on national security requests are difficult to obtain, as the company states that it "is prohibited by law from reporting the exact number" of such orders (*Amazon Information Request Report*, 2016).

families (Hill, 2012). This can result in unintended disclosures of sensitive health information, potentially risking individuals' safety.

Imagine, for instance, a relationship in which a woman's abusive partner finds out about her pregnancy because retailers such as Target deduced it and now overwhelmingly nudge her to purchase relevant products. She may not have wanted her partner to know about her state because she fears for her and her fetus' safety. Notably, absent of such fear, she still has the right to control who she shares private health information with and who she withholds it from based on her preferences alone. Whether in an abusive relationship or not, a person has a fundamental right to control information about herself.[4]

Fourth, the automated advertising practices described are ubiquitous, yet poorly understood by the average user. In a recent report, researchers from the Annenberg School at the University of Pennsylvania found that the vast majority of Americans hold mistaken beliefs about basic internet policies and protections governing the collection and sale of personal data (Turow et al., 2023). At the same time, many realize that their knowledge is lacking, wish they could control access to their private information better, and want the federal government to urgently step in to regulate companies' use of personal data (Turow et al., 2023). Clearly, policy change to enhance consumer protection is warranted.

Taken together, the situation illustrates that individuals have all but ceased to expect privacy when using online services. Cookies follow them from website to website, reminding them of products they once viewed or terms they might have googled. Simultaneously, opt-in opportunities and privacy notices that must be acknowledged before accessing a service have lowered the bar for what is considered *informed* consent. Users generally ignore the details, if

[4] This claim will be developed in Chapter 1: Approaches to Privacy Protection.

not entire pop-ups listing terms and conditions. Long paragraphs filled with legal terminology encourage neither reading nor understanding the risks associated with allowing one's data to be collected. Thus, Internet users routinely agree (tacitly consent[5]) to what they do not comprehend, what can disadvantage them, and what no federal law systematically regulates (Turow et al., 2023). In what follows, I define terms important to ensuing discussion about regulations governing personal data exchanges online.

[5] Tacitly, that is without full awareness. Informed consent requires complete information and comprehensive understanding. The question of whether customers are sufficiently knowledgeable about data practices in the current digital landscape will be taken up in Chapter 2.

APPROACHES TO PRIVACY PROTECTION

Background

Privacy, separated from its role in any specific context, is commonly considered to be a broad right. This means that it is limited neither in scope – it applies to a wide range of situations – nor in application – it is flexibly exercised and enforced. It can even be seen as a fundamental right if one considers its inclusion in the International Declaration of Human Rights (United Nations, 1948). At times defined simply as "the right to be let alone," (Warren & Brandeis, 1890) privacy is a constitutionally protected freedom, safeguarding individuals from infringements such as, in the language of the Fourth Amendment, "unreasonable searches and seizures" (U.S. Const. amend. IV). Given the growing reliance on digital record-keeping for storing personal information, the risk of falling prey to a data breach, and thus potentially suffering harm to one's person or reputation, is increasing. In 2022, 422 million people were affected by data compromises in the United States alone[6] (Petrosyan, 2023). Between 2017 and 2023, an estimated 2 million people became victims of fraud conducted with data bought from the recently seized Genesis Market, a dark web marketplace (Sandford, 2023). As such, the importance of privacy and the necessary protections it provides can hardly be overstated.

At the same time, it takes little to notice that people are selective in their privacy choices. Their preferences for keeping things to themselves or sharing them with others vary primarily depending on the relationship to the other party, the type of information, the potential harm that sharing may bring upon its beholder, and the potential benefit that it may create for one or both sides of the exchange. There is certainly a host of other factors involved, such as lived

[6] Some may have been impacted multiple times and in a variety of ways (e.g., data breaches, leakages, exposures), which this data set treats as separate instances, defining "individuals impacted by data exposures" as "number of records exposed" (Petrosyan, 2023). The reported number can thus exceed the U.S. population.

experience of sharing information with others. However, let us concentrate on these basic determinants for the purposes of evaluating approaches to privacy protection.

Conceptualizing privacy as a protection following the seminal work of Warren and Brandeis (1890) points to security from interference that personal data exchanges might lack. For example, a company may use a consumer's personal data to create a detailed profile of the consumer's interests and behaviors, and then use that profile to show them personalized ads or make decisions about their eligibility for certain products or services. These mechanisms do not usually imperil the consumers in any serious way. Nonetheless, a worrisome situation can arise when a detailed user profile generated from conduct that can range from web searches and ad clicks to engagement with various types of content exposes sensitive information such as political views, medical history, or financial status. The use or transfer of these data (be it the user profile constructed or the information comprising it) to a third party may conceivably affect consumers' lives by leading to "personalized" insurance costs, loan denials, or job rejections, depending on the motivations of the party in whose hands the user's information lands. In this case, privacy is to act as a barrier of sorts, designating personally identifiable information[7] (PII) as something that may not be infringed upon without the beholder's permission.

Taking a different approach to privacy – seeing it primarily as a value enabling control over the information comprising one's self or the narrative one wishes to project to others – suggests other kinds of potential problems arising in its absence (Moore & Katell, 2016; Nissenbaum 2009; Rachels, 1975). Namely, incomplete agency over controlling access to one's image, or arguably to oneself, might impose limitations on the liberty to informational self-

[7] Most government agencies define Personally Identifiable Information as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means" (Ferraiolo et al., 2015).

determination (Mulligan et al., 2016). It may also have consequences for the freedom to selectively form relationships (Rachels, 1975). Intimate relationships are such because they are characterized by the sharing of information kept confidential in most other contexts (Fried, 1970). If to others we are what they know about us, and thus principally what we have chosen to share with them, then collecting personal data without informed consent has repercussions for who we are perceived to be, how we define ourselves, and how we define our relationships.

Further, technologically enabled deduction of unshared personal data risks the erosion of meaningful control over one's information (Mulligan et al., 2016). Such control over access is essential for individual well-being (Moore & Katell, 2016). The focus here is on the potential risks arising from data breaches and knowledge of private information built through inference (e.g., deducing that someone is at risk of a given disease based on their search history of specific symptoms or medical professionals), combining datasets (e.g., supplementing the data that an individual shared with one entity, such as their name and age, with data that they shared with another, such as their zip code), de-anonymizing information (i.e., linking the person to information they shared thinking that it would not be used to identify them, such as a donation made anonymously), and others. These practices, comprising big data analytics, are particularly difficult to combat because control over PII is insufficient to protect oneself from exploitation (Mulligan et al., 2016; Crawford & Schultz, 2013).

On one hand, generating personal data from other sources, such as online behaviors and social network activity, may not qualify as a privacy invasion under a narrow conception of the phenomenon. No unauthorized access to the person occurred – at least not in a straightforward way that would be easy to isolate. On the other hand, generating data using powerful analytics leads to the (re)creation of a highly accurate picture of the user, often without their realization

(Crawford & Schultz, 2013). As far as they are concerned, they never shared their diagnosis with anyone. They just searched Google to find doctors, added specific medicine to their Amazon cart, and reviewed a relevant book on Goodreads. Without disclosing their health status to anyone, they left digital traces leading anyone with internet access right back to the diagnosis.

The above example may sound accusatory, as if the person enabled those who collect user data to learn what was to remain private. While that is not the case – it should not be possible to access personal information so easily – it nonetheless encourages considering one more view of privacy itself: privacy as duty. Anita Allen (1988), defining privacy as a value that moderates access to persons and, in line with previously discussed scholarship, a requirement for liberty, elsewhere discusses its character as a duty (2016). Acknowledging the libertarian stance that one cannot have a duty to oneself, she nevertheless advances a view that individuals have a moral obligation to protect their information (Allen, 2016). The obligation stems from the interrelation of privacy to well-being and autonomy (Allen, 2016). Denying a duty to protect access to information about oneself would deny a duty to protect one's safety, agency, and happiness (Allen, 2016). It follows that liberal governments, concerned with enabling individuals to pursue lives of well-being, should uphold privacy as an ethical good (Allen, 2013).

Taken together, viewing data privacy as a safeguard, a right, a control, a freedom, and a duty can lead to various perceptions of its importance for individual well-being. Regardless of its perceived significance, the view that privacy is a value exposed to risk of being disregarded implies that it necessitates protection. This chapter will engage with three possible approaches to protecting personal information privacy: aligning the involved parties' incentives (as informed by the principal-agent problem), imposing formal duties on the entity handling another's

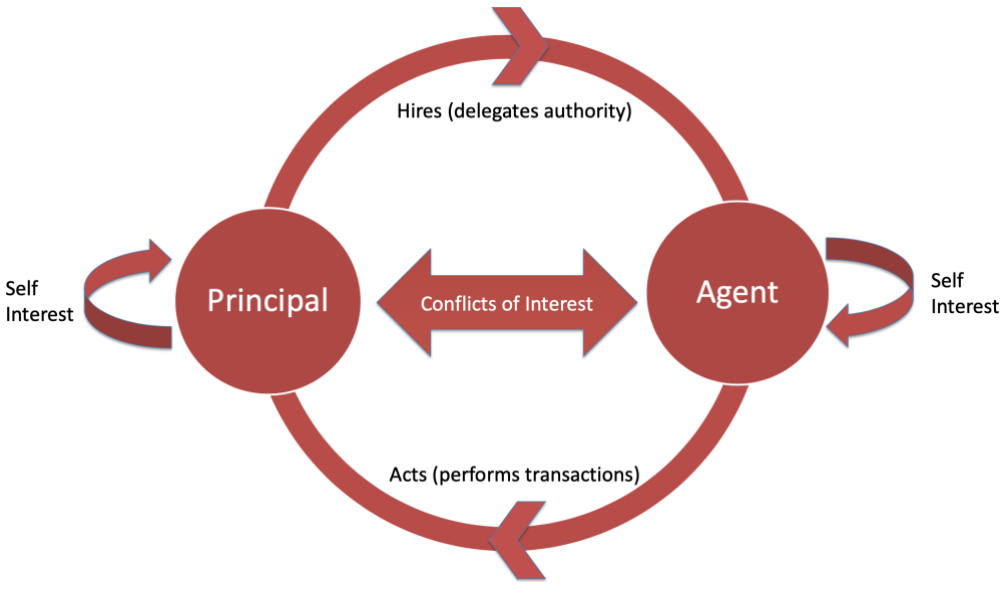
personal information (under the information fiduciary framework), and engendering more competition (with antitrust law).

Principal-Agent Problem

The principal-agent problem arises when one entity (the principal) contracts with another entity (the agent) to act on their behalf, but the latter has interests that might not align with those of the former. Such misalignment, combined with incomplete information, may create a conflict of interest between the two parties and subsequently lead to harmful outcomes. In this case, incomplete information is the unavailability of full knowledge about other participants in the transaction. For instance, the parties might not know each other's preferences or budget constraints. The basic framework of the principal-agent problem, as shown in Figure 1, can be applied to personal data exchanges online where consumers (principals) share PII with companies (agents).

Figure 1

Diagram of the Principle-Agent Problem



The problems arising from this delegation of handling private information will be broken down into two sections: moral hazard and adverse selection. In this context, moral hazard describes a situation in which the principal cannot observe the agent's actions after entering a trust-based relationship with the agent. For instance, the consumer cannot see what companies do with their personal information (how they "act" with it)—to whom they sell it, how they analyze it, etc. Adverse selection describes a situation in which one party (either the principal or the agent) cannot observe the other party's "type." For instance, the consumer does not know whether the company to which they are transferring their data has appropriate data management systems in place. Similarly, the company does not know whether a particular user's data are worthy of collecting and analyzing in terms of the behavioral insights they may or may not yield. However, our focus will be on concerns about the consumer's, rather than the firm's, well-being.

In both situations, moral hazard and adverse selection, the principal might like to know (1) the agent's actions once they have entered a commercial relationship with the agent so that they can informedly choose to remain in the relationship or leave it if their trust is violated. Further, the principal might like to know (2) the agent's type before they enter a relationship that requires trusting them, i.e., placing them in control of private information. Knowing the agent's type—characteristics—can inform the principal's perception of the agent as trustworthy or not, and thus empower the principal to make an informed decision about contracting with the agent in the first place.

Moral Hazard

When consumers entrust a company with their personal data, they naturally expect the company to use the data in their (the consumers') best interest – to provide a better user

experience, personalized recommendations, and the like.[8] At the same time, the company may have financial incentives to use the data for other purposes, for instance, targeted advertising, data brokerage (selling the data to third parties), or research and development. Such incentives may give rise to a conflict of interest between the two parties, putting consumers at risk of harm if their data are used in ways that violate their privacy, imperil their reputation, or otherwise do not align with what they believe to be consenting to in the exchange.[9]

This conflict of interest is, of course, predictable. It is the reason regulators require companies to share privacy notices with customers and to respect laws limiting data collection and use. However, moral hazards arise after the contract – in most cases of data exchange, a standard privacy notice[10] – comes into effect (Rauchhaus, 2009). As such, agents may take action violating the agreement or exploiting its vague terms after entering into it. Clearly, violating a contract is grounds for legal action and the monetary and reputational costs that come with it. As such, it is generally avoided. Less costly ways of deriving maximum value from personal data exist.

Specifically, a contract may be designed in such a manner that it serves one side without really benefiting the other. Indeed, privacy notices generally shield the service provider from liability while offering little benefit to the user, who is supplying personal data. Following the standard Notice and Choice model (also referred to as Notice and Consent), corporate agents state what information they collect, how they store it, and how they might use it (Sloan & Warner, 2014). Although companies are the ones who acquire valuable personal data in this

[8] Pertinently, these expectations may be changing, as consumers grow increasingly skeptical of the agency they have over their data and over decisions to share personal information in digital interactions with online vendors (Turow et al., 2023).

[9] The notion of informed consent in personal data exchanges will be discussed in Chapter 2: Corporate Moral Obligations.

[10] For the purposes of illustrating the argument, we will assume that a privacy notice constitutes a contract. This assumption will be addressed later in this chapter and in subsection *Law* in Chapter 3: Policy.

exchange, they also dictate the terms on which such collection occurs. Users are given a binary choice: to use or not to use the service; at times followed by options that allow them to communicate and preserve some preferences pertaining to data collection.[11]

Moreover, a contract may be written in vague terms that are incomprehensible or that hardly limit permissible conduct. Privacy policies tend to pose significant challenges to most non-experts, and users without postgraduate education more broadly, as they require very good reading comprehension skills (Litman-Navarro, 2019). Such policies have generally grown increasingly complex over the past two decades (Amos et al., 2021; Fabian et al., 2017; Reidenberg et al., 2015). Additionally, the inclusion in notices of "third parties" with which data collected may be shared does not make it easier for consumers to envision what exactly they consent to upon clicking "I agree." Consider, for instance, Facebook. Upon reading and agreeing to Facebook's Terms and Conditions, consumers may still be unaware of the specific entities that Facebook makes their data available to under the Facebook Privacy Policy (Meta Platforms Inc., 2023). No agreement was made between the user and those third parties. Hence, allowing one's data to be transferred to them is inherently hazardous.

Given these shortcomings of mandated privacy notices, a possible avenue for improvement immediately comes to mind: renegotiation. If consumers do not see the agreement as adequate, they should, in a competitive market, have the ability to either (a) choose a different provider or (b) renegotiate the agreement with the current provider.

Ad. (a). The market in products such as search engines and social networks is characterized by economies of scale, network effects, high switching costs, and (other) barriers to entry. Hence, it is not particularly competitive. Emerging alternatives tend to simply be

[11] See, for example, Google's Privacy Policy, which instructs users on exercising controls over information sharing (Google Inc., 2022).

acquired by dominant companies, as was the case with, for example, Instagram's acquisition by Facebook. Consumers are thus in a bind if they want the benefits of using popular products and services but find themselves wary of the protections accorded to them or to their data. Direct network effects experienced by social media platforms actively discourage consumers from searching for alternatives. With pressure to participate in online communities and tangible risks, if not harms, of opting out, Meta, TikTok, and the like have leveraged these effects, along with high switching costs, to the point where respect for consumer privacy can descend to the background with little risk to client retention. Importantly, actively seeking out alternatives is not just an inconvenience for customers. It can be considered unfair to require consumers to part with still more data or to entrust yet another entity with their privacy.

Ad. (b). Being able to renegotiate an agreement requires, at the very least, being informed about its terms. This is difficult for most consumers as data analytics and other use cases are quickly evolving. Most recently, the explosion of machine learning – large language models (LLMs) in particular – has proven how foreign the workings of complex algorithms are to most. Given lacking education and awareness, consumers effectively face an even starker information asymmetry. They can hardly be expected to feel empowered in initiating a renegotiation effort. Additionally, privacy policies may be seen as little but statements of company policy, and thus not give rise to contract claims, which puts customers at a further disadvantage in seeking adequate protection or damages through the legal system should the policy be violated.[12]

As was just mentioned, data exchange relationships are characterized by information asymmetry between the company and the consumer (Pavlou et al., 2007; Balkin, 2020). This phenomenon is not limited to differences in education which become relevant when advanced

[12] See, for instance *Dyer v. Northwest Airlines Corporations*, 2004.

technologies come into play. Taking a step away from the technology to evaluate the basic principal-agent relationship as a whole, it is evident that while companies have detailed knowledge about how PII is used and what risks that involves, consumers frequently lack a complete understanding of the implications of data sharing (Turow et al., 2023). This can make it easier for companies—agents—to take advantage of consumers'—principals'—wanting awareness and to use PII in ways that are not in accord with the latter's interests. In consequence, data brokers come into the possession of vast amounts of information together with its potential for generating insights hidden therein. It is primarily this knowledge-producing capability of data analytics that accords corporations amassing PII an enormous competitive advantage over firms without direct access to a bottomless source of profitable information (Zuboff, 2019). As such, this constitutes an anti-competitive characteristic of the market in data-intensive products.

The information asymmetry (which, by itself, is simply a situation in which the transacting entities have different information) identified above is at the foundation of the power dynamic in the company—consumer relationships discussed. However, important to note is also a further complication of information asymmetry. While the parties can signal – convey credible information to one another – in order to collaboratively minimize the harms of incomplete information, they can also signal in an effort to misrepresent themselves. For example, the agent may paint a positive picture of themselves, posing as a privacy-concerned company, while pursuing actions that are not in accordance with this set of values. The signals used to achieve that are, among others, public assertions that the company is extraordinarily dedicated to consumer wellbeing. Consider, for instance, Apple's campaign targeted against Meta, Google, and other benefactors of the between-app tracking feature present in iPhones and other Apple (and non-Apple) devices.

In 2021, Apple unveiled its App Tracking Transparency (ATT) framework with the public-facing goal of giving users more control over how their data are collected by third parties (Apple Inc., 2021). The marketing campaign positioned the company as a visionary among tech giants, its billboards stating plainly: “Privacy. That’s iPhone.” (Figure 2).

Figure 2

Frame from Apple’s Privacy-Centric Advertisement[13]

This outward image, was accompanied by Apple CEO Tim Cook’s statements at the Computers, Privacy and Data Protection conference, such as “technology does not need vast troves of personal data (...) in order to succeed” (Rogers, 2021). At the same time, the company’s earnings surged, largely due to increased revenue from advertising (see, for instance, Apple’s earnings reports[14]). ATT only blocked third party tracking, hence Apple retained unchanged, virtually unlimited access to user data, and gained an uncontestable advantage in delivering

[13] The ad, which was part of a larger international marketing campaign, is publicly available on YouTube (*Privacy on iPhone | Data Auction | Apple*, 2022).

[14] In an annual report for fiscal year 2022 submitted to the Securities and Exchange Commission, Apple stated that “services net sales increased during 2022 compared to 2021 due primarily to higher net sales from advertising, cloud services and the App Store” (Apple Inc., 2022). Similar statements can be found in the firm’s quarterly earnings reports, which are available at *https://investor.apple.com/investor-relations/default.aspx*.

targeted advertising. Its Privacy Policy evidences extensive tracking inherent to many of the company's products and services while maintaining the veneer of empowering consumers. For instance, the section entitled "Safari Search & Privacy" begins with the following subheading: "Safari Search is designed to protect your information and enable you to choose what you share," but goes on to outline far-reaching surveillance of user activities (Apple Inc., 2022). Consider, for instance, the following excerpt:

> When you use Siri Suggestions or Look Up, or type in Search, Spotlight, Safari search or #images search in Messages, any information sent to Apple does not identify you and is associated with a 15-minute random, rotating device-generated identifier. *Your device may send information such as location, topics of interest (for example, cooking or football), your search queries, suggestions you have selected, apps you use and related device usage data to Apple* [emphasis added]. (Apple Inc., 2022)

It is reasonable to assume that more people will internalize the marketing campaign than the Privacy Policy.[15] As such, misleading signalling is likely to succeed and exacerbate the harms stemming from information asymmetry. In consequence, a lack of knowledge or awareness translates into limited agency as users struggle to exercise meaningful control over data sharing. Zuboff (2019), building on Durkheim's work, argues that it has become possible for companies to monopolize how they are perceived, thus successfully masking surveillance practices amounting to exploitation of users.

[15] Perhaps consumers should not even be expected to read the latter given the immense cost of the time that it would take to read such agreements for every product they use (McDonald & Cranor, 2008).

Adverse Selection

Another part of the principal-agent problem may be adverse selection. It is most commonly found in insurance contexts (Akerlof, 1970). Adverse selection "appears (or at least is possible) whenever the individual or group insured has freedom to buy or not to buy, to choose the amount or plan of insurance, and to persist or to discontinue as a policy holder" (Denenberg et al., 1964, p.446 cited Akerlof, 1970, p.493). In the case of personal data exchanges, companies have freedom to collect consumers' information, but they do not know how much value any particular person's data have until after they collect them. As such, incomplete information is present, but not necessarily adverse selection. Instead of pre-selecting customers whose PII they will collect, which would be costly, firms do not discriminate, collect widely, and parse through so-constructed detailed datasets afterward. The power of big data lies primarily in volume and is not reduced by consumers' preferences for information disclosure. However, the value of PII that companies recognize but users often fail to realize constitutes an asymmetry that gives rise to moral hazard.

Important to note is also that adverse selection might occur when users have a better understanding of the risks associated with the ways in which companies use their personal data, while companies have limited knowledge of users' preferences and behaviors. The problem, then, might be that users who are not as concerned about their privacy may be significantly more likely to accept a privacy agreement with a given company than users who are more concerned with their privacy. At the same time, the "privacy-unconcerned"[16] probably cannot understand what the consequences of agreeing to such a policy entail. If this is so, companies have access to

[16] Alan Westin was the first scholar to propose characterizing consumers as privacy pragmatists, privacy fundamentalists, or privacy-unconcerned (Hoofnagle & Urban, 2014). It is likely that, with more education, a larger proportion of users will become one of the first two kinds, developing some or serious concerns with excessive data collection.

a disproportionate amount of personal data from users who are less concerned about privacy than those who are more concerned (as the latter are much more likely to refrain from using the services of a company who does not adequately protect data privacy than the former).

In sum, conceptualizing the under-regulated state of personal data exchanges between private individuals and (usually corporate) actors as a principal-agent problem (a) highlights the tension stemming from the conflict of interest to which little regulatory oversight is currently applied; (b) facilitates creating solutions to address the elementary components of an overwhelmingly wide-spread set of practices; and (c) questions implicitly accepted business practices that may exploit consumers and put their rights at risk.

Solving this problem requires more than aligning incentives on the surface, which the public can easily scrutinize. Admittedly, however, solutions such as signalling company reputation can be a powerful tool for increasing market efficiency (Saeedi, 2019). Still, to be effective on a large scale, the prevention of unfair PII collection practices must be rooted in moral principles made enforceable by regulatory or legal tools. One proposed framework for incorporating ethical duties to commercial data exchanges is the information fiduciary framework.

Information Fiduciary Framework

Approaching the problem of personal data exchange with distinct focus on the increasingly complex relationship between individuals and entities that collect and manage their data, Jack Balkin (2020) introduced the information fiduciary framework as a potential solution. The framework proposes that companies and organizations handling personal information assume the role of fiduciaries toward the individuals whose data they manage (Balkin, 2020). Drawing parallels between firm-client interactions and professional relationships such as those

between doctors and their patients or attorneys and their clients, the information fiduciary model emphasizes trust and responsibility in data handling practices. This approach could lead to a shift in the way privacy and data governance are approached by prioritizing the welfare of individuals and holding data custodians accountable for it. What follows is a discussion of the arguments and assumptions underpinning the information fiduciary framework, as well as its potential to reshape data protection policies and practices.

First, Balkin (2020) establishes that certain entities who use personal data have asymmetric power over their customers. This imbalance arises upon the transfer of sensitive information from the customer to the company, as it enables the latter to harm or otherwise disadvantage the former, for instance, by sharing said information publicly (Balkin, 2020). There is significant vulnerability in allowing data points such as one's location to be collected. However, disclosing them has become standard practice in recent years (Selinger & Rhee, 2021). The rapid adoption of data collection and analysis practices and the wide, uninformed acquiescence to these "default settings" on consumers' part quickly led the explosion of surveillance to become normalized (Selinger & Rhee, 2021). This leads back to concerns about eroding agency in protecting one's privacy and liberty.

Individuals using the products or services provided by data-collecting entities often find themselves with few or no alternatives. In Balkin's (2020) words, they are increasingly dependent on these companies. As was discussed earlier with respect to the network effects and high switching costs associated with popular Big Tech[17] products, customers may feel uneasy about handing over access to themselves without clear information about how it will be

[17] In this paper, "Big Tech" refers to the dominant technology companies that have extensive influence and control over various aspects of the digital landscape, such as Google, Amazon, Facebook, Apple, and Microsoft.

protected. Nevertheless, they tend to ignore such worries. They feel they have little choice but to click “I agree” and proceed (Turow et al., 2023).

Third, it is in the companies’ direct interest to provide assurance rather than list risks accompanying PII disclosure (Zeng et al., 2022). Returning for a moment to the doctor-patient relationship for comparison, one can imagine a medical professional informing their ‘client’ about the risks and benefits associated with a recommended surgical procedure. While the doctor may, within reason, encourage the patient to focus on the advantages to be gained from successful surgery, she must nevertheless ensure that the patient understands what he is submitting to prior to signing the consent form. The doctor, of course, wants those who she interacts with to do what is best for their health. However, she will not be (financially) harmed[18] regardless of the patient’s decision to use or refuse her services. The situation is understandably dissimilar in firm-consumer interactions. Companies have a vested interest in attracting and retaining customers regardless of whether engaging in the relationship is in the latter’s interest.

Based on these three main concerns – about power asymmetry, restricted agency, and disingenuous signaling – Balkin (2020) argues that entities handling sensitive personal information should have special fiduciary duties toward their users. Namely, duties of care, loyalty, and confidentiality. Adopted together, they would obligate firms to act with the best interest of their customers in mind. This interest is, of course, unlikely to be aligned with the best interest of the company. Thus, legal standards and independent enforcement mechanisms must co-evolve with the proposed information fiduciary framework.

In similar vein, Shoshana Zuboff (2022) argues that emerging regulation, such as the recently introduced Digital Services Act in the European Union, should aim to promote greater

[18] Let us assume that the doctor’s compensation is not dependent on the number of patients choosing to undergo risky medical procedures.

trust and confidence in the digital economy by means of protecting individuals' privacy and autonomy. Considering the broader landscape of data exchanges, Zuboff (2019) outlines possible privacy-promoting changes on both the firm and the consumer side. In addition to requiring companies to act in line with promoting individuals' well-being, which is heavily emphasized by Balkin (2020), she highlights the need to collectively resist exploitative commercial exchanges that drive "digital dispossession" (Zuboff, 2019). This phenomenon is a cycle whereby a company invades a business vertical, normalizes its newly established dominance, adapts to public critique (which, given the scale of disruption, is likely), and, lastly, redirects public attention away from the core issue (Zuboff, 2019). This series of events drives dispossession as civil society feel less and less capable of protecting individual liberties (Zuboff, 2019). Couldry and Mejias (2019) also highlight the profit-maximizing use of data for influencing behaviors in a population. It is in companies' interest to nudge consumers toward purchasing their products and services, sometimes to the extent of attempting to mold prevailing norms and values by shaping trends. As such, "surveillance capitalists" can be seen as undemocratic in their rapaciousness.

Further, considering the relational rules proposed by fiduciary models, Hartzog and Richards (2022) emphasize the promise of the traditional duty of loyalty as a powerful supplement to the current regulatory toolkit. They suggest that loyalty can be significantly strengthened as a responsibility and, in effect, disrupt the unprecedented power of contemporary platforms (Hartzog & Richards, 2022). It is their focus on the power asymmetry between firms and consumers that allows Richards and Hartzog (2022) to take a relationship-centric approach to privacy protection. Advocating a move away from regulating data management practices themselves (i.e., data collection, use, transfer, etc.) and toward dismantling the inequities that

characterize information capitalists' relationships with their clients, they make a strong case for reevaluating the current approach to privacy law (Richards & Hartzog, 2022).

Informational capitalism is, in fact, another scholar – Julie Cohen's (2019) – term. She uses it to describe the present state of capitalism that relies on the accumulation of nonmaterial assets and the race to develop increasingly complex technologies to process them, thus enabling knowledge production, among other capacities. But Cohen's contribution to the privacy literature is far greater than that. In considering various approaches to privacy protection, fiduciary duties in particular, she expresses skepticism toward excessive reliance on traditional methods for reshaping distinctively modern institutional shortcomings (Cohen, 2019*).* Engaging with her account merits its own thorough analysis, but important to this thesis is the insight that the account offers on the risks associated with the emergence and rise to dominance of platforms that are two-sided markets (Cohen, 2019). Such markets are intermediary platforms for exchange where both sides' decisions, i.e., the buyers and the sellers' choices, impact the outcomes of the exchange. For instance, Airbnb matches people who have extra living space with tourists and other individuals looking for a place to stay. Through the generation of network effects and employment of monopolistic practices, these platforms – think, for example, of Google, Amazon, and Uber – have begun to restructure economic exchange (Cohen, 2019). This restructuring is evidenced in the financial sector's growing independence as it increasingly relies on highly complex, underregulated trades that are displacing established markets, such as that for securities (Cohen, 2019).

Cohen's is also a sobering narrative about the reality of partial freedom. Specifically, when companies allow consumers to exercise agency in one area, they retain control over consumers' choices in another (Cohen, 2019). As such, countering pervasive exploitative

practices in a global economy based on user-generated data must entail more than disconnected laws and regulations that fixate on the specifics of data collection. At the same time, technical solutions such as growing adoption of blockchain databases are promising in terms of the security they accord to individual data points. For instance, user profiles and financial transactions are assigned unique identifiers protected by private tools (termed keys), which can only be used by the original owner to access their data.

Returning for a moment to the broader discussion about the information fiduciary model, it is worth pointing out concerns about Balkin's framework. Some oppose it altogether, arguing that private law solutions may be insufficient to address the structural and systemic issues underlying data privacy and protection, especially Big Tech's market dominance achieved largely by acquiring competitors (Khan & Pozen, 2019). Khan and Pozen (2019) propose departing from imposing traditional fiduciary structures on online platforms, pointing out that said platforms hold much more power over their end-users and society than professional fiduciaries, like doctors or lawyers. Reform, they posit, should address the power imbalance at least in part by leveraging antitrust challenges (Khan & Pozen, 2019).

Despite these criticisms, the information fiduciary framework has gained traction as a promising approach to address some of the main challenges to privacy posed by the digital economy. Some scholars – Julie Cohen (2019) in particular – go far beyond the framework to argue that multifaceted reforms to governance are needed on top of protections for individual consumers. More consumer and government scrutiny is called for where market dominance and surveillance capabilities endanger individual autonomy and democratic values.

Antitrust Law

So far, this chapter has discussed two potential approaches to privacy protection. The first one was informed by the principal-agent problem and focused on aligning distinct actors' incentives. The second one concentrated on the imposition of formal duties on the entity handling another's personal information. A third approach will now be discussed: using antitrust law to engender competition.

Why might more competition be relevant to fostering a better environment for consumers and society? Big Tech, as discussed earlier, achieved the power it currently holds by locking customers in with high switching costs,[19] direct network effects, and limited availability of alternatives. Further, users have to pay for services with information about themselves (Cooper, 2013). There usually is no monetary payment option offered as an alternative. Additionally, given that restricting the emergence of new companies was a strategy actively employed by technology giants, primarily via acquisitions, Big Tech can be considered to have monopolistic tendencies (Khan & Pozen, 2019).

In the United States, the agency tasked with implementing laws designed to prevent monopolization is the Federal Trade Commission (FTC). Its mission is twofold: to protect competition and to protect consumers. It is a way into the private sphere, especially when it does not espouse adequate self-regulation. FTC's current chair, Lina Khan, has been a vocal advocate of improving privacy protections. She sees the power asymmetries characterizing personal data exchanges as harmful to the market and individuals alike (Khan, 2022). Consumers are not knowledgeable about information gathering practices, and thus susceptible to (potentially

[19] Consider, for instance, how difficult it would be to switch from using Facebook to using a new platform, where dozens, if not hundreds, of 'friend' connections are yet to be made. Or, to use a concrete, recent example, think about the failure of many Twitter users' efforts to move to Mastodon after Musk's acquisition of the former.

deceptive or clandestine) efforts to effectively limit their agency. Hence, they require protection from the harmful effects that Big Tech's dubious endeavors may have.

Indeed, Khan's (2022) discontentment with current regulations stems primarily from the inadequacy of existing enforcement mechanisms to address the privacy risks posed by dominant technology companies. She advocates addressing deficiencies in consumer protection by requiring companies to obtain explicit consent from users before collecting their personal data and to provide greater transparency and control over how data are used; enhancing the FTC's and other agencies' enforcement methods, e.g., by imposing steeper fines for violating consumer privacy rights; and crafting more uniform policy measures across industries (Khan, 2022).

Moreover, antitrust regulation has the potential to restructure the industry, including the primary axes of competition for consumers. Since their inception, Silicon Valley companies have relied on establishing barriers to entry with inventiveness and resolve to outcompete contenders for market domination. Garnering the potential of big data analytics was a breakthrough in achieving and retaining said control. Therefore, if stringent requirements for data handling and outsized acquisitions limit opportunities for exploitative practices, and if consumers become more concerned with privacy, competition should shift to other domains, such as quality and cost of service. Once those changes are underway, entry into the market should no longer be as difficult for new actors. They will nevertheless face the challenge of building reputation as trustworthy agents of privacy protection. However, with adequate regulation and enforcement mechanisms in place, standards will be higher and distinguishing oneself as particularly careful with data handling can gain in significance as an attractive feature.

Businesses competing on this axis already exist. For instance, DuckDuckGo is a search engine that does not collect user data. Branding itself as "the Internet privacy company for

everyone who's had enough of hidden online tracking," it now performs more than 3 billion search queries per month (DuckDuckGo Inc, 2023). Modeling the implementation of privacy protections that are more stringent than those offered by other players, the literature finds implementing them to be a promising strategy for developing a competitive advantage (Lee et al., 2011; Adjerid et al., 2019).

Fostering more competition, ideally in tandem with empowering consumers by means of providing accessible education about data exchanges and privacy protection to the public, can thus indirectly lead to improved alignment of incentives and greater confidence in PII management safeguards. The FTC has to overcome powerful opposition to its work in order to be effective, but it may have a better chance of enacting positive change for consumers than does Congress, many of whose members coincidentally hold equity in Big Tech companies (Green, 2022). Irrespective of individual members' interests, the political economy of regulating online privacy is not favorable to Congress stepping in to take substantial action (Hoofnagle, 2016).

CORPORATE MORAL OBLIGATIONS

Acknowledging that user data-driven companies have extensive influence over market exchanges and social relations is the first step toward advocating for regulation that would impose adequate checks and balances on their power. However, for consumer protection to be warranted, a need for it should be clearly established. On one hand, some might consider it evident: exploitative datafication disempowers individuals while equipping corporate agents with increasing, underregulated power (Weber, 2015). On the other hand, some might consider such a need to be unexpressed: consumers seem complacent about data security. Although the latter claim can be objected to on the grounds that uninformed acquiescence should not be taken as consent, and that a lack of awareness and power to protect one's security merits (government) interference into the private sector, we will first entertain the objection materialized by the privacy paradox.

Privacy Paradox

The privacy paradox is the phenomenon of expressing concern with one's privacy but taking little to no action to protect it (Brown, 2001). It is commonly found among Internet users (Adjerid et al., 2019; Smith et al., 2011). Its pertinence here is clear. If consumers do not appear to care for personal data overuse, how can it be established as a policy priority? Evidently, the spurious variable is lacking knowledge. Were consumers more aware of the threats associated with PII disclosure and equipped with tools to evade related risks, they would not feel powerless trying to protect their privacy (Turow et al., 2023). Yet, the issue is more complex than it might seem when focus is limited to the pronounced role of awareness, or rather its dearth, in aggravating it.

Acquisti and colleagues (2015) offer three themes encompassing key behavioral findings pertinent to privacy protection behaviors. First is uncertainty; people are sure neither of their own preferences nor of the consequences of privacy-related behaviors (Acquisti et al., 2015). Second is context-dependence; privacy concerns are heavily dependent on various situational factors (Acquisti et al., 2015). For instance, Keith and colleagues (2012) found that intentions to disclose vary with relative increases and decreases in perceived risk. Third is malleability; privacy preferences and behaviors are susceptible to influence, such as context manipulation (Acquisti et al., 2015). For example, in a different study, Acquisti and colleagues (2012) discovered that merely reordering questions so that they become increasingly intrusive increases the likelihood of disclosure. These three behavioral themes are interdependent. Consider how uncertainty amplifies context-dependence and malleability as underinformed consumers search for understandable cues in the environment, including in the (potentially manipulated[20]) choice architecture, to guide their actions (Acquisti et al., 2015).

Consequently, tools such as Notice and Choice privacy policies are inadequate systems for privacy decision-making (Norton, 2016; Solove, 2013). Uncertainty, context-dependence, and malleability render consumers' choices insincere expressions of their true preferences (Acquisti et al., 2015). Importantly, those preferences and concerns are adaptive, which makes the normalization of excessive tracking a worthy endeavor for actors with a vested interest in controlling willingness to disclose personal information (Acquisti et al., 2015).

Do these findings constitute a suitable basis for an argument for increased government investment in consumer protection? In the context of imposing duties of care on corporations, do governments have grounds to build a strong moral case for such requirements? If individuals

[20] See page 27 for a discussion of designing privacy policies to highlight benefits rather than address risks (Zeng et al., 2022). Also relevant is Zuboff's (2019) opposition to using nudges to elicit specific choices from users.

cannot (know to) appropriately protect their well-being, and are therefore relatively powerless, the state should indeed support them (without unreasonable infringement on their liberties).

Consider an analogy to the regulation of harmful substances, such as tobacco and alcohol. At the very least, they come with warnings, so that buyers can make an informed decision about risking their health and their sober judgment, seeing that consumption can easily develop into addiction. Addiction, in turn, tends to override reasoned decision-making that prioritizes long-term well-being. Further, the sale of harmful substances is regulated. For instance, they cannot be sold to underage customers, and they are distributed with information about risks associated with their use on the packaging. Some information privacy laws already mimic these regulations. The Children's Online Privacy Protection Act imposes higher restrictions on young users' data collection, while privacy notices are, in theory, like the etiquettes informing consumers of risks associated with using the product.

As such, there is a case to be made for government intervention in the private sphere based on the established risks to consumer autonomy and health. A more exhaustive discussion of this interference will follow in the Policy chapter. However, worth observing in this context is that such solutions are incapable of making more than a minor dent in the asymmetric power structure characterizing firm-consumer relationships in the modern, datafied world. If nearly all digital products collect PII now, and many do so without making data gathering clear to their users, limiting those practices slightly in hopes of sparing the most vulnerable demographic from harm will not suffice as a counter mechanism to continually expanding influence.

Informed Consent

Perhaps technology companies, or any private entities for that matter, can be assumed to have no obligations to promoting consumer well-being. Without explicit social obligations,

however, they can still have ethical obligations, if not in the form of deontological duties, that is duties stemming from the nature of the actions and persons associated with them, then in the form of consequentialist duties arising from the outcomes of said actions. Ensuring that consumers with whom companies transact can meaningfully consent to those interactions is not just right because (I) it is fair. It is right also because, in line with utilitarianism, (II) it promotes the greatest good for the greatest number.

(I) In order to conclude that there is fundamental unfairness to unethical data practices, which, for our purposes, can be simplified to breaches of privacy, we must first establish the deontological basis for making a normative statement of this kind. First, let us determine the values at risk. Three principles feature prominently in the literature on informed consent: respect for autonomy, beneficence, and justice (Faden & Beauchamp, 1986). If violated, they cease to protect the teleological soundness of an action.

Consumers' autonomy, that is, freedom of choice, is undermined with every attempt to manipulate their decision-making. Privacy policies may purposefully obfuscate unethical data practices or prompt the expression of consent by belying the risks associated with privacy forfeiture (Pollach, 2005). Beneficence, the value of seeking the principal's welfare, is at minimum equivalent to inflicting no harm (Faden & Beauchamp, 1986). As such, exploitative PII gathering that either exposes or subjects consumers to harms stemming from privacy invasion and choice limitation neglects beneficence. Lastly, justice, broad and contested as it is as a term, will here be narrowly treated as the principle of enabling all persons to exercise their rights without undue burdens (Faden & Beauchamp, 1986). In the privacy context, it would be unjust to make information owed to consumers – information concerning the handling of their personal data – difficult to obtain. It would prevent them from exercising their right to privacy in

an informed way. Moreover, perpetuating the power asymmetry present in personal data exchanges requires putting oneself (or one's enterprise, which then becomes a proxy for one's actions) above those whose information privacy is violated for one's benefit. This stands in conflict with the view of justice as equality.

With the values of autonomy, beneficence, and justice in mind, we can draw inferences about the doctrine of informed consent. It should be guaranteed in personal data exchanges because it enables consumers to exercise their right to privacy as they wish—as they are entitled to do.

(II) Shifting away from basic principles[21] to evaluating the morality of actions based on their consequences, we will determine the applicability of utilitarianism to imposing the duty of promoting informed consent on companies transacting with private individuals. Clearly, there is at least as much utility to be gained from respecting consumers' right to privacy as there are consumers.[22] But much more is attainable. Given the cycle of dispossession characterized as authoritarian by Zuboff (2019), empowering individuals to control how much data they transfer to corporate entities simultaneously empowers civil society to safeguard itself from private sector's influence. The tradeoff is the companies' ease of data acquisition and knowledge production, both of which drive profit, which can be seen as utility. As such, utilitarianism would advocate prioritizing consumer protection in the form of bolstered privacy standards only if consumers and civil society's gains exceeded the losses of the private sector.

[21] "Basic" rather than "first" because to formally treat values—such as autonomy—and rights—such as that to privacy—as first principles would be an oversimplification even if they were considered inalienable; they would still stem from qualities determined about persons.

[22] The gain to each likely depends on how much they value privacy. This variable, while important for determining total utility gains, is not necessary for the argument at hand. All can benefit from stronger privacy protections as privacy enables the pursuit of other liberties and personal projects. In short, privacy can advance well-being.

Another way to think about informed consent is through the lens of data literacy, that is, users' understanding and control of datafied systems (Pangrazio & Sefton-Green, 2019). Equipping consumers with more knowledge about information privacy can assist them in meaningfully expressing their sharing preferences through adjusting product settings. The notion of informed consent must thus encompass educating users about their rights as well as the avenues for exercising them. Once again, the assumption is that the costs associated with transitioning to stronger privacy protections will not exceed the benefits to be drawn from the envisioned ensuing state. It is conceivable that the positive externalities resulting from bolstered data exchange regulations will, indeed, compensate for the private sector's losses (Cohen, 2012). Even if they do not, that is, even if the ethical duty to foster informed consent cannot be defended on utilitarian grounds, there might be a moral obligation to co-creating sustainable social structures. That discussion, however, belongs in a separate paper, dedicated entirely to it.

Personal Agency

While much has already been said about agency and autonomy in reference to privacy preferences, behaviors, and duties, let us briefly return to these ideas to conclude this chapter. Freedom to pursue well-being implies the liberty to exercise individual rights, such as one's right to privacy. We have previously seen that the burden to enable the pursuit of happiness might lie with the government.[23] The government, in turn, may effectuate this responsibility by requiring companies to have stronger default privacy protections and reduced data collection capabilities. Accordingly, the baseline option for users of a data-driven product could be established as no personal information tracking. This is a simple, if stark, contrast with the currently prevalent

[23] As a reminder, the determinant of that responsibility was the consumers' incomplete ability to protect their rights.

default of opt-out settings (Acquisti et al., 2015). These settings are doubly problematic as users struggle to exercise the privacy choices that websites claim to provide (Habib et al., 2020).

A supplementary approach to burdening data brokers with ensuring adequate privacy protection is seeing the autonomous user as, fittingly, responsible for controlling access to themselves. This duty is not an alternative to company or government protection, but it is a necessary responsibility nevertheless (Allen, 2016). Ascribing it to individuals indicates that there are moral limits to what should be shared (Allen, 2011). Drawing on Kant's deontological concern with individuals' duty to protect themselves from harm, Allen (2016) suggests that limiting information disclosures shields ourselves and our reputations, thus facilitating other responsibilities we have to ourselves, including the pursuit of happiness. Hers is a view that offers an enriched perspective on regulating personal data exchanges. It lends itself well to regulatory frameworks that could benefit from grounding in normative ethics (that is nevertheless pragmatic).

POLICY

Existing Frameworks

The current set of laws and policies demands fundamental changes. It is based on outdated information about data analytics, and it benefits one side—data-collecting enterprises—more than the other—consumers. Its deficient state is, in part, the effect of Big Tech's successful lobbying to pursue profit maximization under the guise of benefiting the public interest (Popiel, 2018). Aforementioned negative externalities include disempowering users to the extent of undermining their personal agency (Zuboff, 2019).

Simultaneously, regulatory efforts seem out of touch with technological advancement and pragmatism. Required Notice and Choice policies, for instance, cannot be thought of as adequate, not least because the cost of reading them every time one visits a new website would be outlandish (McDonald & Cranor, 2008). Data breaches are too common, not taken seriously enough (most consumers do not comprehend the risks associated with having their data intercepted by a malicious third party), and expected to occur. Companies neglect to proactively avoid them by failing to enact stronger cybersecurity measures (Schneider, 2009).

Given that data-handling corporations have acquired immense power by designing systems for PII collection and use, they cannot be expected to self-regulate away from it. The risks – suppressed revenues and the loss of competitive advantage – are too great. If, however, all firms were required to curb their data collection practices, other axes on which to compete with one another would take precedence. To guide such coordination, a strong state—of the coercive, Leviathan[24] kind—is needed.

[24] Following Hobbes' (1651/1968) seminal work, I, too, accept the premise that the social contract must ultimately be enforced by a sovereign with absolute power if it is to be respected.

Regulation

Given the rapid evolution of data analytics and machine learning, as well as the growing dependance on data-intensive products and services, one would expect to see policy efforts to proactively regulate segments of the technology industry. However, policymakers and the public alike may lack a strong grasp of the evolving elements comprising digital products and solutions (Kang & Satariano, 2023). In addition, emerging advances, which few experts understand relatively well, are difficult to conceptualize and subject to existing legal frameworks. As such, it may be helpful to use established guidelines as a point of departure. For instance, likening data – a concept that is difficult to isolate as a physical object or phenomenon – to personal property or speech lends itself well to potential applications to rule-making efforts in already established regulatory fields.

A range of laws and policies have been enacted in the United States to safeguard consumer privacy in online personal data exchanges. These regulations tend to be industry-specific, as distinct sectors manage various data types, each associated with unique risks and varying levels of perceived significance. Key regulatory acts that contribute to shaping the privacy-protection landscape include:

a. The California Consumer Privacy Act of 2018 (CCPA). CCPA is a privacy law that applies to companies operating in California and collecting personal data about the state's residents. It requires these companies to disclose – to consumers as well as to regulators – what personal information they collect and how they use it, and it gives consumers the right to access their personal information or request its deletion.

b. The Children's Online Privacy Protection Act of 1998 (COPPA). COPPA is a federal law regulating those websites and online services that are either directed to the youngest group of consumers – children under the age of 13 – or that have actual knowledge that they are collecting personal information from children under the age of 13. It requires obtaining verifiable parental consent before any collection of personal information from children, and it prohibits sharing such information with third parties without parental consent.
c. The Electronic Communications Privacy Act of 1986 (ECPA). The ECPA is a federal law that governs the interception of electronic communications, such as emails and instant messages. It requires law enforcement agents to obtain a warrant before accessing the contents of individuals' electronic communications.
d. The Health Insurance Portability and Accountability Act (HIPAA). HIPAA is a federal law that regulates the use and disclosure of health information. It requires healthcare providers and other agents handling personal health data to protect the privacy and security of that data, and it gives individuals the right to access and control them.
e. The Federal Trade Commission Act of 1914 (FTC Act). The FTC Act is a federal law that gives the FTC the authority to carry out its mandate of protecting consumers (and the market at large) from unfair and deceptive trade practices. Its uses have spanned the enforcement of data privacy and security standards, including bringing enforcement actions against companies that violate consumers' rights to privacy or imperil fair competition by means of obtaining access to staggering volumes of consumers' personal information.

f. The Gramm-Leach-Bliley Act (GLBA). The GLBA is a federal law that requires financial institutions, such as banks and credit unions, to provide notice about their privacy practices to consumers and to give consumers the right to opt out of certain information sharing practices. Moreover, it dictates comprehensive standards for information security programs maintained by the institutions in question.

Furthermore, sector-specific regulations and standards that apply to specific types of data, such as credit card information, exist and operate internationally. For example, the Payment Card Industry Data Security Standard (PCI DSS) is a set of security benchmarks that apply to corporations who process credit card payments (PCI Security Standards Council, n.d.). The standards require companies to implement security measures such as encryption and access controls.

Notwithstanding the implementation of various regulations, the current state of personal data protection remains inadequate considering increasing reliance on technology, which goes hand-in-hand with sharing ever more personal data with machines and the companies that own them. Increasingly pertinent types of data exchanges remain underregulated. For instance, ChatGPT's Terms of Use state that users' input may be used to develop the model (OpenAI, 2023). This clear disclosure of data collection, which is nevertheless made less transparent by Privacy Policy provisions allowing PII transfers to other parties, can help users make somewhat informed decisions (OpenAI, 2023). But potential problems associated with a machine learning model and the team behind it having access to tens of millions of users' conversations with it are numerous and, if AI continues advancing anywhere near as fast as it has been in recent years, such data can become leverage. It is not implausible that an advanced AI could use knowledge

deduced about a given person from all the information it finds on said person online to convince them to perform tasks it cannot perform itself, such as reCAPTCHA verifications. OpenAI has put safeguards in place, but it has also made API access easy to obtain by anyone (OpenAI, 2023). And not every developer will put safety first.

The under-regulation of certain types of data and their uses is in part due to their swift rise in importance, and in part due to the relatively slow operation of legislative bodies, who may also be dissuaded from passing laws that will impose additional rules on business by powerful lobby groups. It is not in companies' immediate interest to subject themselves to more scrutiny or to adopt stricter privacy protections. Tighter regulations and increased oversight usually impose additional costs, both in terms of compliance and potential fines for violations. As such, the approach to policymaking itself, not just its aim – the final policy product – may need restructuring to evade the pitfalls of lobbyists who have prevailed in the past.

The first and only comprehensive (that is, not sector-specific) law against privacy violations passed by Congress was the Privacy Act of 1974. 25 years later, in 1997, the Clinton Administration introduced A Framework for Global Electronic Commerce, which called for minimal regulation of electronic commerce. "Governments should avoid undue restrictions on electronic commerce," it read (Clinton & Gore). Indisputably, things have changed in the few decades since. The current state-by-state, sector-specific, patchwork approach to privacy protection is insufficient for confronting both established and swiftly emerging challenges in personal data protection calls for reform.

Law

In similar vein, the legal system does not fully recognize that the entire market structure needs changing (Zuboff, 2019; Cohen, 2019). Questions concerning bolstering consumer

protection merit revisiting precedents that stifled past efforts for formal recognition of individuals' right to privacy. In a remarkable clash of logical reasoning between different branches of the state with respect to privacy, the court in *Dyer v. Northwest Airlines Corporations* (2004) ruled that privacy policies did not give rise to contract claims absent of allegations that passengers relied on these policies. Of course, the judiciary is completely distinct from the legislative bodies of the government. They need not align on all matters. Still, it is telling that regulations (in this case, the requirement to post privacy policies in the interest of consumer protection) are, at times, not strong enough to stand in a court of law.

Should such policies translate into legal rights? Considering that they would then provide consumers with grounds on which to claim damages even in the absence of government regulation, this could strengthen consumers' position. In *Meyer v. Christie* (2007), where a bank violated the terms of its privacy policy by disclosing confidential financial information about the plaintiff to a third party, the court recognized that the privacy policy constituted more than "a mere unilateral statement of company policy." The plaintiff relied on the bank's privacy policy in conducting business with the bank, and thus said policy was part of the plaintiff's bargained-for exchange with the financial institution (*Meyer v. Christie*, 2007).

Moreover, recognition of agreements between users and online service providers as contracts could empower consumers to enact change by means of collective action suits. For instance, when Canadian coffeehouse-donut chain Tim Hortons was found to be tracking granular geolocation data of millions of its customers without their knowledge or consent, four separate class action lawsuits were filed across Canada (Bundale, 2022). The chain's parent company, Restaurant Brands International, covertly recorded the movements of clients who had

downloaded the Tim Hortons App in the background, receiving an average of 10 events[25] per user per day, while its FAQ erroneously claimed that the app used the customer's location only when they had the app open (*Joint Investigation into Location Tracking by the Tim Hortons App*, 2022). While the class action lawsuits were settled with coffee and donuts,[26] Tim Hortons also agreed to comply with user data deletion and privacy management recommendations produced by the investigation (*Joint Investigation into Location Tracking by the Tim Hortons App*, 2022).

More recently, Meta committed $725 million to settling a class action lawsuit that claimed that Facebook negligently disclosed users' personal information to third parties (*Facebook, Inc. Consumer Privacy User Profile Litigation*, 2023). Among the instances of the platform's failures to protect consumers' privacy between May 2007 and December 2022 (this was the period specified by the lawsuit) was the infamous Cambridge Analytica scandal, in which data from over 87 million accounts were harvested.

Challenging exploitative personal information practices time and again may induce companies to shield themselves from legal costs by means of granting clients increased protection. However, so long as the law remains ambiguous[27] and privacy policies—abstruse—opportunities for consumer privacy mismanagement abound.

[25] The location data was processed to "generate an entry or exit "event" whenever the User visited a location of any of nine competitors identified by Tim Hortons, visited major sports venues and stadiums, or returned to their inferred home or place of work" (*Joint Investigation into Location Tracking by the Tim Hortons App*, 2022).
[26] The compensation for damages to members of the class action lawsuits (all affected users, unless they had opted out of the proceedings) was decided to be a voucher granting each eligible member one free beverage and one free pastry (*Transaction Agreement*, 2022).
[27] The view that the language of statutes constituting privacy law is ambiguous or imprecise is commonly found in extant literature (see, for instance: Amos et al., 2021; Bamberger & Mulligan, 2015; Culnane & Leins, 2019; Krotoszynski, 2016).

Proposed Reform

Three paths for the future develop from the discussion. First, informing rules governing personal data exchanges by looking to behavioral economics insights, which may be underexplored in the literature (Lin, 2022). Second, making privacy protection the axis on which firms compete. Third, fostering equitable distribution of burdens[28] to protect one's own and others' privacy and, in line with that, protecting democratic values. The three will be discussed with reference to one kind of data gathering and use: targeted advertising.

Micro-targeting is the practice of crafting and delivering highly personalized messages to a specific audience based on its demographics, interests, behaviors, and other characteristics. This practice has become a widespread tool for customer acquisition and profit maximization. It easily affects tens of millions of people every day. Undeniably, existing privacy and data protection regulations enumerated earlier can indirectly impact data-driven marketing practices and micro-targeting for non-marketing purposes – such as influencing political sentiments. Although these regulatory acts do not address data-driven marketing or micro-targeting explicitly, they do influence how businesses collect, use, and share personal information for marketing purposes. Nevertheless, they are not a satisfactory means of consumer protection.

While micro-targeting does not necessarily target individual users per se, it does target very small, well-defined segments of users with similar characteristics. These narrow segments are constructed from a combination of demographic (age, gender, location), psychographic (interests, values, lifestyle), and behavioral information (browsing habits, purchase history). Leveraging it enables identifying patterns and preferences among users and subsequently

[28] Currently, minorities suffer more liberty restrictions due to excessive surveillance and other privacy-evading practices (Allen, 2011).

creating tailored content that appeals to them. These capabilities present ethical concerns that merit scrutiny and tailored regulatory intervention.

Firstly, micro-targeting can infringe upon individual privacy if the collection, analysis, and utilization of personal data proceeds without adequately informing users about the risks, i.e., obtaining their informed consent. Importantly, the problem lies not in the sale of data to third parties, which regulation generally does not allow regardless. Rather, it lies in the immense potential of knowledge generation from behaviors that individuals rarely realize are observed and harvested (Zuboff, 2019). As standard Notice and Choice practices have been identified as insufficient (Balkin, 2020), regulation should specify methods of communicating with users transparently. In practice, consumers should be able to restate the general risks associated with data sharing and know how they can revoke consent. Ideally, they should also have meaningful control over the actors to whom insights about their preferences and behaviors are being sold by data brokers such as social media sites and search engines. This, however, would be a difficult contractual agreement to implement, not least because it exposes the primary model of profit-making for many Big Tech companies.

Secondly, data-driven marketing can inadvertently or intentionally lead to discriminatory practices, perpetuating or exacerbating social inequalities and biases. For instance, lenders can identify narrow segments of the population who frequently search for payday loans or short-term financial solutions, suggesting that they might be struggling to make ends meet. Further, they can seek to label those who also have limited financial literacy or face other challenges that make them even more susceptible to predatory lending practices.

Clearly, targeting vulnerable individuals, who are often from low-income or marginalized communities, may reinforce existing disparities and disproportionately trap certain demographics

in cycles of debt. As such, regulations on data-driven marketing should go beyond provisions to prevent the use of personal data for discriminatory targeting. This is likely the area of consumer protection where law enforcement has the highest effectiveness for promoting equity.

Thirdly, the high degree of personalization enabled by micro-targeting allows advertisers to manipulate users' decision-making, raising concerns surrounding autonomy. For instance, marketers can tap into users' cognitive biases, such as social proof (Cialdini et al., 1999). By presenting content that shows others, especially peers or authority figures, engaging with a product or service, companies can create a perception that the product is popular or valuable, and influence targeted consumers to purchase it. In extreme cases, these practices may be outright deceptive, capitalizing on paid fake reviews of products (Wu et al., 2020). Regardless of whether deception is used (perhaps the influencers employed really do endorse the product), one can argue that by capitalizing on social proof, advertisers can nudge consumers towards decisions that may not be aligned with their genuine preferences, needs, or values. However, whether this amounts to a violation of personal autonomy depends on one's views on government's role in far-reaching consumer protection. Good advertising has always tapped into biases, social norms, and convincing rhetoric. It does not seem to have posed a great risk to individuals or populations thus far. With that in mind, however, it is still important to protect vulnerable populations and limit the advertising of risky activities, such as smoking or gambling. We will, once again, draw parallels between existing regulatory acts limiting the advertising of addictive substances and those that would limit micro-targeting.

In the case of harmful substances, regulation counteracts misleading or manipulative marketing tactics. Regulatory measures like the Family Smoking Prevention and Tobacco Control Act of 2009 recognize that promoting highly-addictive, health-harming substances may

expose vulnerable individuals to the risk of acting irrationally, against their better judgment. Compulsive users tend to eschew awareness of the associated health risks, which marketing messages could further downplay or even belie as less severe than they are. Young users are impressionable and can be easily manipulated by persuasive advertising, and it is thus in their best long-term interest to be shielded from it.

In the context of micro-targeting and, more broadly, personal data use for advertising, regulation seeks to ensure that individuals maintain control over their personal information and are not subjected to intrusive or discriminatory marketing practices. Hence, both types of regulation aim to preserve individual autonomy and promote informed decision-making in the absence of undue influence. This is especially important when disparities in education may make some more susceptible to manipulation than others.

Therefore, individuals and societies can gain from enacting regulation that enforces ethical, transparent practices in data-driven advertising. Responding to objectors who might claim that this is overblown, I will concede that preferences informing, e.g., retail practices, do not constitute as risk-laden of a dataset as credit card information, the collection of which is stringently restricted. However, as has been demonstrated above, seemingly unrelated interests and behaviors revealed online can expose vulnerabilities, such as addiction, or be analyzed in tandem to infer information about political leanings in a population. Thus, data can enable those who wield them to act in ways that imperil public health or democratic processes.

For instance, in the run-up to the 2016 US Presidential Election, aforementioned Cambridge Analytica harvested personal data from millions of Facebook users without their consent, leveraging psychological profiling and micro-targeting techniques to manipulate voter behavior and opinions through tailored political advertisements (Digital, Culture, Media and

Sport Committee, 2018). This incident demonstrated the vast potential of exploiting seemingly value-laden personal information, such as online shopping history (in this case narrowed down to merchandise purchased), media outlets followed, and the kind (Cadwalladr & Graham-Harrison 2018; Digital, Culture, Media and Sport Committee, 2018).

Given the inequitable distribution of risks and burdens to individuals, as well as the potential social harms stemming from the abuse of insights generated from large quantities of personal data, multilevel reform is not only justified but necessary. Mine is but a preliminary sketch focusing on practices that should be departed from or regulated more scrupulously first.

CONCLUSION

Based on the preceding multilayered discussion of personal data exchanges, we are justified in drawing some conclusions about addressing the problems associated with them. There is reason to encumber excessive personal data collection and brokerage with broad enforcement of consumer-first principles. Governments are justified in redesigning the landscape of PII exchange based on behavioral science insights that legitimize a consumer protection-based approach to thwarting outsized power. Additionally, the means of accessing valuable resources at virtually no cost, at the expanse of vulnerable individuals, certainly merits a reconsideration of what comprises fair and ethical business practices. Further, the expansion of antitrust law into the sphere of privacy protection is warranted insofar as data exploitation facilitates the rise of monopoly-like structures. Congress, the Federal Trade Commission, and the judicial system should expeditiously evaluate the current state of personal data exchanges. Consumers have much to gain from the introduction of checks and balances into the prevailing system. If executed well, such change should also benefit the market at large. More regulation on one side may enable more competition where freedom to innovate is preserved.

REFERENCES

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*, 509–514. https://doi.org/10.1126/science.aaa1465

Acquisti, A., John, L. K., & Loewenstein, G. (2012). The Impact of Relative Standards on the Propensity to Disclose. *Journal of Marketing Research*, *49*(2), 160–174.

Adjerid, I., Acquisti, A., & Loewenstein, G. (2019). Choice Architecture, Framing, and Cascaded Privacy Choices. *Management Science*, *65*(5), 1949–2443. https://doi.org/10.1287/mnsc.2018.3028

Akerlof, G. A. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, *84*(3), 488–500.

Alan E. Meyer, et al., Plaintiffs, v. David J Christie, et al., Defendants, Case No. 07-2230-JWL (United States District Court, D. Kansas Ocotber 2007).

Allen, A. L. (1988). *Uneasy Access: Privacy for Women in a Free Society*. Rowman and Littlefield. https://philpapers.org/rec/ALLUAP

Allen, A. L. (2011). *Unpopular privacy: What must we hide?* Oxford University Press.

Allen, A. L. (2013). An Ethical Duty to Protect One's Own Information Privacy? *Alabama Law Review*, *64*(4), 845–866.

Allen, A. L. (2016). The Duty to Protect Your Own Privacy. In *Privacy, Security and Accountability: Ethics, Law and Policy*. Rowman & Littlefield International Ltd.

Amazon Information Request Report (p. 3). (2016). Amazon Web Services. https://d1.awsstatic.com/certifications/Information_Request_Report_June_2016.pdf

Amos, R., Gunes, A., Lucherini, E., Kshirsagar, M., Narayanan, A., & Mayer, J. (2021). Privacy Policies over Time: Curation and Analysis of a Million-Document Dataset. In

Proceedings of the Web Conference 2021 (pp. 2165–2176). Association for Computing Machinery. https://doi.org/10.1145/3442381.3450048

Annual Report 2012. (2012). Facebook, Inc. https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB_2012_10K.pdf

Apple Inc. (2021, April 26). *IOS 14.5 delivers Unlock iPhone with Apple Watch, more diverse Siri voice options, and new privacy controls*. Apple Newsroom. https://www.apple.com/newsroom/2021/04/ios-14-5-offers-unlock-iphone-with-apple-watch-diverse-siri-voices-and-more/

Apple Inc. (2022a). *Annual Report pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 for the fiscal year ended September 24, 2022* (No. 001–36743). Apple Inc. https://s2.q4cdn.com/470004039/files/doc_financials/2022/q4/_10-K-2022-(As-Filed).pdf

Apple Inc. (2022b, September 12). *Safari Search & Privacy*. Apple Legal. https://www.apple.com/uk/legal/privacy/data/en/safari-search/

Ashley Sitko and Ashley Cadeau v. Restaurant Brands International Inc., No. CV-20-00643263-00CP (Ontario Superior Court of Justice 2022).

Balkin, J. M. (2020). The Fiduciary Model of Privacy. *Harvard Law Review Forum, 134*(1), 11–33.

Bamberger, K. A., & Mulligan, D. K. (2015). *Privacy on the ground: Driving corporate behavior in the United States and Europe*. MIT Press.

Bhatia, J., Breaux, T. D., Reidenberg, J. R., & Norton, T. B. (2016). *A Theory of Vagueness and Privacy Risk Perception*. IEEE International Conference on Requirements Engineering. https://www.cs.cmu.edu/~breaux/publications/jbhatia-re16.pdf

Brown, B. (2001). *Studying the Internet Experience* (HPL-2001-49; User Studies & Design Group, DMSD, p. 24). Hewlett Packard. https://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf

Children's Online Privacy Protection Act of 1998, S. 2326, United States Senate, 105th Congress 2nd Session.

Bundale, B. (2022, July 29). Tim Hortons offers coffee and doughnut as proposed settlement in class action lawsuit. *CTV News*. https://www.ctvnews.ca/business/tim-hortons-offers-coffee-and-doughnut-as-proposed-settlement-in-class-action-lawsuit-1.6007455

California Consumer Privacy Act of 2018, Assembly Bill No. 1680, California Legislature, 2017-2018 Regular Session, Civil (2018).

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Cialdini, R. B., Wosinska, W., Barrett, D. W., Butner, J., & Gornik-Durose, M. (1999). Compliance with a Request in Two Cultures: The Differential Influence of Social Proof and Commitment/Consistency on Collectivists and Individualists. *Personality and Social Psychology Bulletin*, *25*(10), 1242–1253.

Clinton, W. J., & Gore, A. (1997). *A Framework For Global Electronic Commerce*. The White House; National Archives. https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html

Cohen, J. E. (2012). *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. Yale University Press.

Cohen, J. E. (2019). *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford University Press.

Cooper, J. C. (2013). Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity. *George Mason Law Review*, *20*(4), 1129–1146.

Couldry, N., & Mejias, U. A. (2019). *The Costs of Connection: How Data is Colonizing Human Life and Appropriating it for Capitalism*.

Crawford, K., & Schultz, J. (2014). Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review*, *55*(93), 93–128.

Cukier, K., & Mayer-Schoenberger, V. (2013). The Rise of Big Data: How It's Changing the Way We Think About the World. *Foreign Affairs*, *92*(3), 28–40.

Culnane, C., & Leins, K. (2019). Misconceptions in Privacy Protection and Regulation. *Law in Context*, *36*(2), 49–60.

United States of America v. Meta Platforms, 1:22-cv-05187 (Office of Administrative Law Judges June 21, 2022). https://www.justice.gov/opa/press-release/file/1514026/download

Digital, Culture, Media and Sport Committee. (2018). *Disinformation and 'fake news': Interim Report* (HC 363). House of Commons. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf

DuckDuckGo Inc. (2023). *DuckDuckGo: About Us*. Your Personal Data Is Nobody's Business. https://duckduckgo.com/about

Dyer v. Northwest Airlines Corporations, 334 F. Supp. 2d 1196 (D.N.D. 2004) (US District Court for the District of North Dakota September 8, 2004).

Electronic Communications Privacy Act of 1986, Pub. L. No. Public Law 99-508, 1848 (1986).

Fabian, B., Ermakova, T., & Lentz, T. (2017). Large-scale readability analysis of privacy policies. In *Proceedings of the International Conference on Web Intelligence* (pp. 18–25). Association for Computing Machinery. https://doi.org/10.1145/3106426.3106427

Facebook, Inc. Consumer Privacy User Profile Litigation, 18-MD-2843-VC (United States District Court for the Northern District of California 2023).

Faden, R. R., & Beauchamp, T. L. (1986). *A History and Theory of Informed Consent*. Oxford University Press.

Federal Trade Commission Act of 1914, 41–58 15 U.S.C. (2006).

Ferraiolo, H., Chandramouli, R., Ghadiali, N., Mohler, J., & Shorter, S. (2015). *NIST Special Publication 800-79-2. Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-79-2

Fried, C. (1970). *An Anatomy of Values*. Harvard University Press. https://www.hup.harvard.edu/catalog.php?isbn=9780674332485

Google Inc. (2022, December 15). *Privacy Policy*. Privacy & Terms. https://policies.google.com/privacy?hl=en-US

Gramm–Leach–Bliley Act, 106–102, Senate, 106th Congress, U.S.C. (1999).

Green, J. (2022, January 27). Congress's Big Tech Stock Stakes Make Regulation Awkward. *Bloomberg*. https://www.bloomberg.com/news/articles/2022-01-27/congress-s-big-tech-stock-trading-makes-antitrust-regulation-awkward#xj4y7vzkg?leadSource=uverify%20wall

Habib, H., Pearman, S. K., Wang, J., Zou, Y., Acquisti, A., Cranor, L. F., Sadeh, N., & Schaub, F. (2020). "It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion

Choices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1–12). Association for Computing Machinery. https://doi.org/10.1145/3313831.3376511

Hartzog, W., & Richards, N. M. (2022). The Surprising Virtues of Data Loyalty. *Emory Law Journal*, *71*(5), 985–1034.

Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 1936 (1996).

Hill, K. (2012, February 16). 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/

Hobbes, T. (1968). *Leviathan*. Penguin Books. (Original work published 1651)

Hoofnagle, C. J. (2016). *Federal Trade Commission Privacy Law and Policy*. Cambridge University Press.

Hoofnagle, C. J., & Urban, J. M. (2014). Alan Westin's privacy homo economicus. *Wake Forest Law Review*, *49*(2), 261–318.

Joint Investigation by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Office of the Information and Privacy Commissioner of Alberta, and the Office of the Information and Privacy Commissioner for British Columbia into The TDL Group Corp.'s (the operator and franchisor of Tim Hortons in Canada) compliance with Canada's Personal Information Protection and Electronic Documents Act, Quebec's Act Respecting the Protection of Personal Information, Alberta's Personal Information Protection Act, and British Columbia's Personal Information Protection Act (PIPEDA Findings #2022-001). (2022). Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du

Québec, the Office of the Information and Privacy Commissioner of Alberta, and the Office of the Information and Privacy Commissioner for British Columbia. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2022/pipeda-2022-001/#toc7

Kang, C., & Satariano, A. (2023, March 3). As A.I. Booms, Lawmakers Struggle to Understand the Technology. *The New York Times*. https://www.nytimes.com/2023/03/03/technology/artificial-intelligence-regulation-congress.html

Kearns, M., & Roth, A. (2019). *The Ethical Algortihm: The Science of Socially Aware Algorithm Design*. Oxford University Press.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, *71*(12), 1163–1173. https://doi.org/10.1016/j.ijhcs.2013.08.016

Khan, L. M. (2022, April 11). *Remarks of Chair Lina M. Khan as Prepared for Delivery* [Conference Remarks]. IAPP Global Privacy Summit, Washington, D.C. https://www.ftc.gov/system/files/ftc_gov/pdf/Remarks%20of%20Chair%20Lina%20M.%20Khan%20at%20IAPP%20Global%20Privacy%20Summit%202022%20-%20Final%20Version.pdf

Khan, L. M., & Pozen, D. E. (2019). A Skeptical View of Information Fiduciaries. *Harvard Law Review*, *133*(2), 497–541.

Krotoszynski, R. J. (2016). *Privacy Revisited: A Global Perspective on the Right to be Left Alone*. Oxford University Press.

Lee, D.-J., Ahn, J.-H., & Bang, Y. (2011). Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection. *MIS Quarterly, 35*(2), 423–444. https://doi.org/10.2307/23044050

Lin, T. (2022). Valuing Intrinsic and Instrumental Preferences for Privacy. *Marketing Science, 41*(4), 663–681.

Litman-Navarro, K. (2019). We Read 150 Privacy Policies. They Were an Incomprehensible Disaster. *The New York Times*. https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html

McDonald, A. M., & Cranor, L. F. (2008). The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society, 4*(3), 543–568.

Meta Platforms Inc. (2023, January 1). *Privacy Policy*. Meta Privacy Center. https://www.facebook.com/privacy/policy/

Meta Reports Fourth Quarter and Full Year 2022 Results (Financial Statements, p. 11). (2023). [Earnings Release]. Meta Platforms Inc. https://s21.q4cdn.com/399680738/files/doc_financials/2022/q4/Meta-12.31.2022-Exhibit-99.1-FINAL.pdf

Moore, A. D. (2003). Privacy: Its Meaning and Value. *American Philosophical Quarterly, 40*, 215–227.

Moore, A. D., & Katell, M. A. (2016). Introduction. In *Privacy, Security and Accountability: Ethics, Law and Policy*. Rowman & Littlefield International Ltd.

Mulligan, D. K., Koopman, C., & Doty, N. (2016). Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal*

Society A: Mathematical, Physical and Engineering Sciences, *374*(2083), 20160118. https://doi.org/10.1098/rsta.2016.0118

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press. http://www.sup.org/books/title/?id=8862

Norton, T. B. (2016). The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model. *Fordham Intellectual Property, Media and Entertainment Law Journal*, *27*(1), 181–210.

OpenAI. (2023a, March 14). *Terms of Use*. https://openai.com/policies/terms-of-use

OpenAI. (2023b, April 5). *Our approach to AI safety*. https://openai.com/blog/our-approach-to-ai-safety#OpenAI

OpenAI. (2023c, April 7). *Privacy Policy*. https://openai.com/policies/privacy-policy

Pangrazio, L., & Sefton-Green, J. (2020). The social utility of 'data literacy.' *Learning, Media and Technology*, *45*(2), 208–220. https://doi.org/10.1080/17439884.2020.1707223

Parent, W. A. (1983). Privacy, Morality and the Law. *Philosophy & Public Affairs*, *12*(4), 269–288.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective. *MIS Quarterly*, *31*(1), 105–136. https://doi.org/10.2307/25148783

PCI Security Standards Council. (n.d.). *About Us*. Retrieved March 22, 2023, from https://www.pcisecuritystandards.org/about_us/

Petrosyan, A. (2023, February 24). *Cyber crime: Number of compromises and impacted individuals in U.S. 2005-2022*. Statista. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

Pollach, I. (2005). A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent. *Journal of Business Ethics*, *62*, 221–235. https://doi.org/10.1007/s10551-005-7898-3

Popiel, P. (2018). The Tech Lobby: Tracing the Contours of New Media Elite Lobbying Power. *Communication, Culture and Critique*, *11*(4), 566–585. https://doi.org/10.1093/ccc/tcy027

Privacy on iPhone | Data Auction | Apple. (2022, May 18). [YouTube Video]. https://www.youtube.com/watch?v=K_i4odTSTvg&t=1s

Rachels, J. (1975). Why Privacy is Important. *Philosophy and Public Affairs*, *4*(4), 323–333.

Raice, S., Das, A., & Letzing, J. (2012, May 17). Facebook Prices IPO at Record Value. *The Wall Street Journal*. https://www.wsj.com/articles/SB10001424052702303448404577409923406193162

Rauchhaus, R. W. (2009). Principal-Agent Problems in Humanitarian Intervention: Moral Hazards, Adverse Selection, and the Commitment Dilemma. *International Studies Quarterly*, *53*(4), 871–884. https://doi.org/10.1111/j.1468-2478.2009.00560.x

Reidenberg, J. R., Bhatia, J., Breaux, T. D., & Norton, T. B. (2016). Ambiguity in Privacy Policies and the Impact of Regulation. *Journal of Legal Studies*, *45*(3), 8.

Reidenberg, J. R., Breaux, T., Cranor, L. F., French, B., Grannis, A., Graves, J. T., Liu, F., McDonald, A., Norton, T. B., Ramanath, R., Russell, N. C., Sadeh, N., & Schaub, F. (2015). Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding. *Berkeley Technology Law Journal*, *30*(1), 39–88.

Richards, N. M., & Hartzog, W. (2020). A Relational Turn for Data Protection? *European Data Protection Law Review*, *6*(4), 492–497. https://doi.org/10.21552/edpl/2020/4/5

Rogers, C. (2021, January 29). Apple's Tim Cook: Business cannot turn a blind eye to data exploitation. *MarketingWeek*. https://www.marketingweek.com/apple-data-privacy/

Saeedi, M. (2019). Reputation and Adverse Selection: Theory and Evidence from eBay. *The RAND Journal of Economics*, *50*(4), 822–853. https://doi.org/10.1111/1756-2171.12297

Sandford, D. (2023, April 5). Genesis Market: Popular cybercrime website shut down by police. *BBC News*. https://www.bbc.com/news/uk-65180488

Schneider, J. W. (2009). Preventing Data Breaches: Alternative Approaches to Deter Negligent Handling of Consumer Data. *Boston University Journal of Science & Technology Law*, *15*, 279–303.

Selinger, E., & Rhee, J. H. (2021). Normalizing Surveillance. *Northern European Journal of Philosophy*, *22*(1), 49–74.

Sloan, R. H., & Warner, R. (n.d.). Beyond Notice and Choice: Privacy, Norms, and Consent. *Journal of High Technology Law*, *14*(2), 370–414.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 989–1015. https://doi.org/10.2307/41409970

Solove, D. J. (2013). Introduction: Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, *126*(7), 1880–1903.

Steve Holcman v. Restaurant Brands International Inc., Restaurant Brands International Limited Partnership and The TDL Group Corp., No. 500-06-001081-203 (Quebec Superior Court 2022).

Transation Agreement between Restaurant Brands International Inc., Restaurant Brands International Limited Partnership and The TDL Group Corp. (The Defendants) and BK Canada Service ULC and Steve Holcman and William Jung and Wai Lam Jacky Law and

Ashley Sitko and Ashley Cadeau. (2022). https://lpclex.com/wp-content/uploads/2020/07/Tim-Hortons-Settlement-Agreement.pdf

Turow, J., Lelkes, Y., Draper, N. A., & Waldman, A. E. (2023). *Americans Can't Consent to Companies' Use of Their Data: They Admit They Don't Understand It, Say They're Helpless to Control It, and Believe They're Harmed When Firms Use Their Data—Making What Companies Do Illegitimate* (p. 24). Annenberg School for Communication, University of Pennsylvania. https://dx.doi.org/10.2139/ssrn.4391134

United Nations. (1948). *Universal Declaration of Human Rights*.

U.S. Constitution, § Amendment 4.

Wai Lam Jacky Law v. Restaurant Brands International Inc. And Radar Labs, Inc., No. VLC-S-S-207985 (British Columbia Supreme Court 2022).

Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193–220. https://doi.org/10.2307/1321160

Family Smoking Prevention and Tobacco Control Act of 2009, no. Public Law No. 111-31, 111th Congress (2009).

Weber, R. H. (2015). Internet of things: Privacy issues revisited. *Computer Law & Security Review*, *31*(5), 618–627. https://doi.org/10.1016/j.clsr.2015.07.002

William Jung v. Restaurant Brands International Inc., Restaurant Brands International Limited Partnership, The TDL Group Corp., BK Canada Service ULC and Radar Labs, Inc., No. CV-20-00648562-00CP (Ontario Superior Court of Justice 2022).

Wu, Y., Ngai, E. W. T., Wu, P., & Wu, C. (2020). Fake online reviews: Literature review, synthesis, and directions for future research. *Decision Support Systems*, *132*, 113280.

Zeng, F., Ye, Q., Yang, Z., Li, J., & Song, Y. A. (2022). Which Privacy Policy Works, Privacy Assurance or Personalization Declaration? An Investigation of Privacy Policies and Privacy Concerns. *Journal of Business Ethics*, *176*, 781–798. https://doi.org/10.1007/s10551-020-04626-x

Zuboff, S. (2019). *The Age of Surveillance Capitalism*. Profile Books.

Zuboff, S. (2022, May 11). *Europe Is Saving Democracy from Big Tech, Says the Author of Surveillance Capitalism* [Magazine Article]. https://time.com/6174614/shoshana-zuboff-twitter-surveillance-capitalism/