Revista Internacional de Educación y Análisis Social Crítico
Mañé, Ferrer & Swartz.
ISSN: 2990-0476
Vol. 3 Núm. 1 (2025)

The attention advantage: How Internet companies profit from the uninformed consumer

La ventaja de la atención: cómo las empresas de Internet se aprovechan del consumidor desinformado

A vantagem da atenção: como as empresas da Internet se aproveitam do consumidor desinformado

Olivia Llanio
B.A. Internet, Cultures and Social Evolutions and Political Science (Rollins College, Florida, USA)
https://orcid.org/0009-0009-0751-6409
ollanio@rollins.edu

Abstract

This paper presents an analysis of the role of a consumer in a social internet. It reviews privacy and data collection practices, modern media companies, digital advertising, and the impacts consumers and users face in the current digital landscape. It explains the landscape of data brokerage and the role modern technology companies have in the digital economy. This analysis draws connections between how informed consumers are and how they behave online, arguing that mixed media companies benefit from uninformed consumers. The paper provides the critical context of large, for-profit internet companies within an ecosystem that the majority of the global population operates within. This understanding sets the foundation for research related to digital economies and media engagement online and can equip users with an opportunity for more informed decision making at the individual and policy levels.
Keywords: Media companies, social media, digital privacy, data brokerage, attention, data, internet.

Resumen

Este artículo presenta un análisis del papel del/a consumidor/a en una internet social. Repasa las prácticas de privacidad y recopilación de datos, las empresas modernas de medios de comunicación, la publicidad digital y las repercusiones a las que se enfrentan los/as consumidores/as y usuarios/as en el actual panorama digital. Explica el panorama de la intermediación de datos y el papel que desempeñan las empresas tecnológicas modernas en la economía digital. Este análisis establece conexiones entre lo informados que están los/as consumidores/as y cómo se comportan en línea, argumentando que las

empresas que poseen diversos medios se benefician de los/as consumidores/as desinformados/as. El documento proporciona el contexto crítico de las grandes empresas de internet con ánimo de lucro dentro de un ecosistema en el que opera la mayoría de la población mundial. Esta comprensión sienta las bases de la investigación relacionada con las economías digitales y la participación en los medios de comunicación en línea, y puede brindar a los/as usuarios/as la oportunidad de tomar decisiones más informadas a nivel individual y político.
Palabras clave: Empresas de medios de comunicación, medios sociales, privacidad digital, intermediación de datos, atención, datos, Internet.

Resumo

Este artigo apresenta uma análise do papel do consumidor numa Internet social. Passa em revista as práticas de privacidade e de recolha de dados, as empresas modernas de comunicação social, a publicidade digital e as implicações que os consumidores e os utilizadores enfrentam no atual panorama digital. Explica o panorama da intermediação de dados e o papel das empresas tecnológicas modernas na economia digital. Esta análise estabelece ligações entre o grau de informação dos consumidores e o seu comportamento em linha, argumentando que as empresas proprietárias de meios de comunicação social beneficiam de consumidores desinformados. O documento fornece um contexto crítico para as grandes empresas de Internet com fins lucrativos num ecossistema em que opera a maioria da população mundial. Esta compreensão lança as bases para a investigação relacionada com as economias digitais e a participação nos meios de comunicação social em linha, e pode dar aos utilizadores a oportunidade de tomarem decisões individuais e políticas mais informadas.
Palavras-chave: Empresas de comunicação social, redes sociais, privacidade digital, intermediação de dados, atenção, dados, Internet.

Introduction

The internet has evolved drastically in a few short decades. An underbelly resource has turned mainstream, migrating from open access towards a landscape of commercialization and paywalls. Throughout this time, many major companies in this space have risen and fallen, and few have remained as leaders in their industries. In today's age, the digital frontier is all but monopolized. The few companies leading the industry are referred to as the 'Big Five'. 'The Big Five' refers to Alphabet (the parent company of Google), Amazon, Meta (previously Facebook), Apple and Microsoft. They are the tycoons of their time, amassing record levels

of wealth, power and industry control. These companies have numerous approaches to making their billions, with several in common. Together, they set the industry standards and enforce them through their market control.

The degree of control they exert over their industries make them a critical study. This article focuses on the non-hardware, data oriented facets of these companies' operations. Specifically, industry areas of social media, online search and cloud services. These sectors generate massive profits while providing free access for users. Their common profit methods are not well known for their transparency, and are generally at least partially obscured to the average reader. This paper will explain the social landscape, its economies, and how the major companies in the digital services market benefit by their consumers being uninformed about the reality of how these free services operate.

The Modern Digital Landscape

To be online today is to be surrounded by noise. The successful digital company holds user attention for as long as possible, through increasingly engaging content and platform design. With the reality of that landscape, it is easy to understand the overflow of information. This overflow, coupled with the informational silos users often inhabit, is delicately designed to nurture a consumer to enjoy without many questions. This is both driven and exemplified by the social media tycoons of today. Focusing on the social media services offered by these actors in the 'Big Five' will allow specific inter-company parallels to be drawn across platforms.

This paper focuses on Meta (Facebook, Instagram), Google, and Twitter. Both Meta and Google -two juggernauts in their respective tech corners- are included here because, while their software portfolio differs from one another, they have revenue streams which, for the scope of this paper, are reasonably similar. The focus is on companies whose primary function is in the social media space, where the relevant research applies to their media and/or advertising arms. Twitter and Meta are leaders in the social media space, with their vast user bases and social capital. Google's best known social media platform is YouTube, a pioneer in the 2010's social media marketing space. Google also houses advertisements across their digital services, including Gmail and Google Maps.

All of these companies produce varied media content for their users. Media content for the purpose of this article includes visual, audial and written content, encompassing movies, shows, podcasts and music, news articles and short form images and videos. Contemporarily, any of these types of media can be found across social media sites. This generally generates and maintains user activity on the platforms. More traditionally

customers used to pay for access to the media itself. Newspapers, CDs, and cable television are examples of that practice. The revenue generated from the media itself is a commodity model known as the “media content model” (Fuchs, 2020). Fuchs considers the media content model to be one of several “capital accumulation models” (2020, p. 152) and is integral to modern social media companies’ sales strategies.

Walking hand in hand with the media content model is the advertising model. The advertising model’s commodity defined by Christian Fuchs are “advertising, attention, and personal data” (2020, p. 136). Where the media content model sells content at the consumer’s request, the advertising model presents content to the consumer without request. While both models are rooted in sharing information, the advertising model’s role is to drive awareness to products and services in the hopes of successfully convincing a consumer that they want or need what is presented to them (Fuchs, 2020). Advertisers spend tremendous amounts of money with the hope that the money spent will return in the form of consumers then buying what is being advertised to them. Media companies earn money from advertisers buying ad space to hold the attention of the individuals who spend their time on said platforms. Attention is the thing really being sold, via the eyes, ears and dollars of millions (or billions) of users.

Companies generating revenue by advertising on their platforms is not new. Neither is the overlap between these content and advertising models. The merging of these sales models is best described by what Fuchs refers to as a “mixed media company” (2020). Mixed media companies sell, or commodify, more than one sales approach:

> Mixed media companies have at least a dual form of the commodity: Audience attention (C’2) is sold to ad clients. At least one other commodity (C’1) is sold to customers. C’1 is often content, but can also be some other communication commodity such as communication technologies (Fuchs, 2020, p. 145).

Mixed-media companies (MMC) combine different business models to generate multiple revenue streams at the same time. Mixed media companies are more nuanced and complex than any of the aforementioned models standing alone because of their compounding services. MMC are not always composed of strictly media and advertising content models, but the platforms studied here are. A past example is cable channels (and streaming services) generally charge a fee to customers subscribing to their channels or services, in addition to selling advertising space on those channels. All mainstream social media sites (e.g. Instagram, Facebook, Twitter) are modern examples of these mixed media companies, as are several contemporary media conglomerates (e.g. Disney).

ISSN: 2990-0476
Vol. 3 Núm. 1 (2025)

Social media sites are the most salient example of a contemporary mixed media company. In contrast to traditional media production, much of the access to content across social media is free to consumers. Necessarily, this shifts the core of profit away from user contribution to advertising dollars. Advertisements are littered within the audiovisual and written content found across social media, both overtly and covertly. They show up in Instagram posts, tweets on Twitter, float to the top of online search results and even find home in their own tab in Gmail. With an increased role on the part of advertisements, companies have a renewed need for marketability among advertisers themselves. To better understand the role the advertisements have across social media, the concept of advertising itself must be better elucidated.

The heart of advertising is to sell something a consumer has not asked for. In order for those sales to occur, advertisements must buy and sell attention. Attention sales, or advertisements, are a primary profit method for these companies. To make this effort as effective as possible, advertisers harness user data. Users enter the digital economies of these platforms at every part of their online journey, well before they make any purchases. To understand profits and advertising practices across these platforms, there are two basic concepts which apply to the consumer, on any platform. Companies either sell a product *to* a consumer or sell the consumer *as a* product (Rahman-Jones, 2024). To sell a product *to* a consumer is the traditional practice of advertising explained above. The advertisement itself recommends a product advertisers hope to convince you that you want or need. Here, the ultimate commodity is attention. The second method, which operates with significantly less transparency, makes the consumer the commodity. In this case, the information companies sell -like users' traits, habits and behaviors- is the profit making machine. In this area of the market, the commodity is data.

Data Collection Practices

Within these companies, they use both attention and data to generate profit. The exchange related to profit through attention can be referred to as the attention economy. The attention economy is a concept first introduced in the 1970's by Herbert Simon (1971), and has been expanded and updated for the internet age by various scholars. When companies sell the information they collect, it contributes to the data economy. The data economy integrates real-time insights and individual digital footprints to tailor internet experiences (Shukla et al., 2023). The data economy thrives off of information generated by the users of the sites and platforms.

The specific details of what is included when user data is collected varies from app to app, site to site. Across research, however, most, if not all, digital spaces are collecting similar archetypes of information. Some companies are well known for having a more intimate and vast reach of data than others. Meta, the parent company of Instagram, is infamous for such practices. An analysis of Instagram's Privacy Policy by a third party grouped their data collection as follows: "Account and Profile Information," "Content Interaction Data," "Device and Connection Information" (UpGrow, 2024). These terms seem relatively innocuous, but include a vast amount of information, including everything from your email address, age and gender to how long you watched a specific video or the precise time and location of the picture you upload to the platform.

The labels provided in most privacy policies and terms of service documents can generally be understood by three aggregate terms. They collect "Personally Identifiable Information (PII)", "Behavioral Information" and "Metadata" (Singh, 2024). PII refers often to the information needed to create an account, like a name, contact details and sometimes things like gender and age (Singh, 2024). Behavioral Information includes the data related to individual activity on the platform (how and when the services are used, what is liked or shared, what accounts users follow, etc.) and Metadata is data about your device or browsing patterns that would not be included in behavioral data (Singh, 2024). Behavioral data and metadata often work in conjunction, and can include things on and off the app or site. Information like your device details, location, time and date of posts, browsing patterns (even across various apps or websites) and, depending on the application, various other data stored across the device you use to access the platform (Heiligenstein, 2023). This data is not limited to the platform or site the user is currently browsing, but is rather an aggregate profile synced across sites and devices, using repeating account details, IP addresses and browsing habits to build a 360 degree view of each consumer (Tau, 2024).

An example of the depth of this reach is in 'location data.' When a company refers to collecting 'location data,' an average user might assume a given service might collect somewhat broad location data, like your city or state. In actuality, location data is usually highly specific, referring to your real-time location determined by IP addresses or GPS (Tau, 2024). It can also encompass historic or future location data, depending on the terms of service. It can also continue to collect said data, meaning a user might approve a specific app using their location for a single session while the app might track their location for a much longer period of time — across days, weeks or more (Klosowski, 2021). This ensures that the data being sold continues to update, being more accurate to your location and thus, your advertising preferences (Keegan and Ng, 2021).

The data is all encompassing, and its collection does not go unutilized. Some of these data points are necessary to open and maintain an account on social media, an email provider, or many website 'memberships.' Much of the data collected is much more specific and in a greater volume than an average user grasps. A 2024 journal concludes, "understanding the explanations of the collection and use of personal data typically requires expertise beyond the comprehension of most data subjects" (Ding and Huang, 2024, p. 3). The palatable, industry-specific language used in these terms and conditions agreements is a strategic choice on the part of the companies, for various reasons.

I would also note that, while vast, this lists only the data points publicly available from various online services. Various lawsuits and articles have suggested more data collection than this might occur in some cases. In 2024, the US Federal Trade Commission fined Facebook a record-setting $5 billion USD for their reported violation of a 2012 FTC order by "deceiving users about their ability to control the privacy of their personal information." This is coupled with a Justice Department complaint alleging that Facebook "repeatedly used deceptive disclosures and settings to undermine users' privacy preferences" (Nguyen, 2024). A year earlier (in 2023), Facebook was hit with a 1.2 billion euro fine from the EU for similar offences of user privacy right violations (EDPB, 2023). Google also settled a lawsuit in 2022 for $392 million over allegations that the company "tracked people through their devices after location tracking had been turned off" (Allyn, 2022), suggesting that even if companies develop these privacy policies, their potential for profit might incentivize breaking those privacy commitments.

Data: Bought and Sold

Byron Tau, in his book *Means of Control: How the Hidden Alliance of Tech and government is creating a new American Surveillance State* (2024), elaborates on the data sales environment. He explains the practices of 'anonymizing' data, something done before it is sold. Data is scrubbed of legally protected details before buyers receive it. When user data is 'anonymized' an individual's name is replaced with a 'user ID' composed of letters and numbers while all the patterns and data points remain the exact same (Tau, 2024). While this removes the legal identifiers from the user profile, an advertiser has little use for a name when they have the entire rest of a user's online presence (Tau, 2024). Anyone with access to that same information could reasonably digest all of a person's preferences and practices and, with as little as three GPS location points, quickly uncover the redacted information (Tau, 2024).

Tau leads with an example of such a story involving US government officials at the beginning of his book. In this example, he highlights the technical vulnerabilities regarding 'anonymized' location data collected

from Grindr, a dating app for gay men. The high-level officials could be pinpointed via real-time location data shared within the app; an individual with a small amount of tech-savviness could exploit that location sharing and retain the live location tracking data even when the user closes the app (Tau, 2024). This example highlights some of the ample security concerns regarding this practice, as well as the sale and purchase of such data in general. Some websites have 'opt-out' designed to give users some choice over the data collection and tracking on the site and beyond, and Apple and Google offer increasing opt-out tracking options on their devices. Currently, a user is not guaranteed access to a given site or app if they choose to reject the tracking.

After this data is collected, it is sold. This industry is known as data brokerage. Data brokers make up billions of dollars of the annual market share, and, according to market research, their influence is only growing. According to Sharma and Chandola, "The global data broker market size was over 374 billion USD in 2023 and is likely to reach almost 672 billion dollars by 2032" (2024). This is a market which reaches far beyond the major social platforms. Data brokers predate the internet, and while the specifics of the data have changed drastically over time, 'data' remains highly valued by many industries.

Data brokerage has a long history, entwined with advertisers and security industries alike. Data brokers before the internet were much more restricted as to what information they could collect. The predecessors of modern day data brokerage were reserved to some of the most basic information, often limited to the type of information that could be found on a census. National security and surveillance limitations were also strict, limited to what could be found "on the outside of an envelope" (Tau, 2024). Since the days of print, data brokers have benefited most by giving the most detailed and far-reaching information possible, but were limited by what individuals chose to share outside their private spaces. The evolution of data collection and privacy attitudes greatly shifted after 9/11 and moved the mark of what is allowed.

Advertisers and companies want to market their products and services as effectively as possible across wide ranges of the consumer market, and data brokers help in that process. The depth of information private companies have access to has increased in stride with the evolution of a social internet. As people practice sharing more details about their lives across a large-scale 'town square,' the legal protections of past decades have become insufficient. Modern laws have not kept pace with the sprint of the social media revolution, and as a result, data brokers are selling every megabyte of data billions of people share about themselves and their lives to be assessed by private and government contacts alike.

Modern data brokers are selling all the data points they can gather in real time. The information collected while a user interacts with a platform, after being ascribed with the 'user ID' attached to a user's digital profile, is sent instantly to a slew of companies who pay top dollar for access (Tau, 2024). Most often, this is sent into an advertising pipeline, where the most pertinent use of the information is to aid in the development of more effective and precise advertising campaigns. This means it is not only the amount of data that is valued, but the specificity of the data as well.

At present, the range of 'specific' data can go so far as what accounts you follow, which ones you look at the most, and where you are at any given moment. The 'anonymizing' of this data may not include your name, but it ensures that a company or data broker can analyze your entire digital presence (across platforms and websites too, in many cases) to then curate the most effective and specifically applicable advertisements across the entirety of your online identity. Contemporary marketing practices suggest that a company benefits from a highly tailored audience. Before one can be an informed consumer, they must understand the landscape of data brokerage.

While the digital services profit largely from the exchange of data, they also profit from the subsequent increase of user attention. As the CEO of 'attention technology company' Lumen said, "attention almost exactly predicts profit" (Stewart, 2025). Companies can receive a portion of sales from successful ad campaigns on a given site or platform, and they can charge higher rates for ad space when they have higher rates of engagement. Engagement, in the social media space, encompasses the time spent using and interacting with a given app or service (CLRN, 2024). This engagement is both desired and analyzed, internally and externally. The engagement is presented as 'user data' and in both data and attention economy, user data is relevant and utilized.

Engagement is the ultimate metric by which the attention economy is measured. From time spent browsing, to how long users spend on a post, or share and interact with it, engagement encompasses all activity data (CLRN, 2024). It can be measured across a single account, post, topic or any other margin. The aforementioned engagement is also a major factor in determining the ad rates of various individuals or accounts who make profits from posting on the platforms. 'Ad rates,' a shorthand for 'advertising rates,' refer to how much a certain platform charges for its various kinds of advertising space. This can refer to companies and platforms as well as digital 'influencers,' a term used to refer to people who make profit from sharing content across the web. The most common place for influencers is on Instagram, Tiktok, Youtube and Facebook, the same platforms which prioritize this form of engagement and attention from users. On

both sides of this larger mixed media market, there is direct benefit from keeping users engaged on the platform.

Advertising rates vary widely per entity, with some traditional celebrities getting paid alleged sums of over a million dollars for a single post on Instagram (Influencer Marketing Hub, 2025). To advertise through the platforms themselves, rates change depending on the type of advertisement, the audience and more. Advertisement rates are estimated by industry analysts to range between roughly $0.40-0.70 USD per click on a single advertisement (DeFazio, 2025). The specific algorithms used to determine ad rates are trade secrets, and can only be estimated based on data in the public sphere. Either way, by any measure, this digital advertisement economy is one with a massive amount of money in circulation. The global digital ad spend was over 790 *billion* USD in 2024 (Kemp, 2025) -all hinging on the promise of eyes and clicks across the web. The cyclical process here utilizes eyes on advertisements to generate product sales and data from users which continually promises better ad and revenue returns- whether or not they purchased a product.

Most people have a general expectation that the exchange for accessing a platform or website for free is that companies will make profits through advertising. The shorthand for this phenomenon is referred to as ‘consent or pay’ (Rahman-Jones, 2024), which references the idea of paying for access or giving consent to data tracking for profit. Consumers may have that general understanding of this sales process but the gap between traditional advertising practices and advertising practices on social media is vast. Traditional media targeting is much less individualized, and the average consumer does not have a strong grasp on what it takes in order to produce the handpicked advertisements they see on their social media feeds. These companies benefit largely from consumers not understanding how much data it takes to generate those types of advertisements. In real-time, an advertisement is selected for them as a result of various companies having access to a well of their own personal information and digital habits. The misunderstanding is a large issue. The control companies have in shaping and directing how users spend both their money and time, however, is an even greater threat.

The Uninformed Consumer

As discussed above, digital service companies, at large, profit from increasing the time and engagement activities of users on their platforms. Within the industry, engagement metrics are considered one of the primary determinants for how companies and influencers alike can increase their rates for various types of advertisements (DeFazio, 2025). This creates a self-sustaining machine of more people posting and advertising, increasing profits and the movement of this market as a whole. Social media companies have

the data that explains what kinds of posts and content engage consumers at the highest rate. Everyone who benefits from any kind of advertisement in circulation online benefits from better, more detailed and accurate statistics on users. All parts of the money-making side of the equation -which notably, does not include the users- are continually searching for ways to better increase their profits, which incentivizes companies to not only procure but present and share more detailed versions of user data. This was, in part, a major element of the Cambridge Analytica scandal of the late 2010s (Chomanski, 2025).

The central event of the Cambridge Analytical scandal was the uncovering that, in conjunction with Facebook, Cambridge Analytica, a private company for hire, could influence user activity on social media so drastically that they were able to successfully sway multiple elections and voting events around the world. A Guardian article quotes a former Cambridge Analytica employee who says

> the company could craft adverts no one else could: a neurotic, extroverted and agreeable Democrat could be targeted with a radically different message than an emotionally stable, introverted, intellectual one, each designed to suppress their voting intention – even if the same messages, swapped around, would have the opposite effect. (Hern, 2018).

The understanding that, with enough data points -data points being any information that can be gleaned from how you use the internet- a company can craft a deft and specific message that could incite you to act in a specific way can be daunting. It is also a proven reality. The Cambridge Analytica example serves to remind us that this access is not understood and does not have public approval when users are adequately informed. A CBS News article published after the scandal broke quotes one user saying “Facebook has increasingly given me reasons not to trust them;” it explains he cut his usage from about 30 minutes daily to about 10 minutes every other day and would “happily flee altogether if a viable alternative emerged” (CBS, 2018).

Facebook (Meta)’s involvement in this subterfuge was significant for a few reasons. Politically, this scandal shows how much influence and change can be wielded with the personal information that is bought and sold online every single day. While the political and cultural influence is far from limited to the US 2016 presidential election, the research and data from this event is vast and is a strong example. In an analysis done at the University of North Carolina at Chapel Hill, researchers conducted interviews during the election cycle. They found that “these firms [Facebook, Google, Microsoft, Twitter] are more active intermediaries in U.S. electoral politics than is conventionally recognized in the literature” (Kreiss and McGregor, 2017). This collusion, particularly in the 2016 US election example, was not only deeply effective for their most heavily

involved campaigns, but proved beneficial for their bottom line as well. The employees of these various sites who took up work, in effect, for the political campaigns, provided a strong return on investment: “These technology firm staffers, in turn, generated larger returns for both these companies and campaigns… For technology firms, this meant more revenue” (Kreiss and McGregor, 2017). The revenue increase is the ultimate priority for these technology companies, even if it comes at the cost of user misinformation.

The engagement in electoral politics increased over time, which, in conjunction with sales to various data brokers, created an environment for a company like Cambridge Analytica to flourish. Facebook has been cited as having knowledge of the increased polarization and volatility on its site and in the landscape, often as a result of these deeply targeted content pieces (Horwitz, 2023). Facebook did not, however, make any serious attempts to curb these concerns after becoming aware of them. In fact, some of this activity helped to increase engagement on the platform (Horwitz, 2023). With engagement in the position of a critical metric, many companies were able to angle this polarization and dissonance as a success, citing increased ad circulation, user engagement and ad sales for those correlating sales periods (Team, 2017).

While the consequences of Cambridge Analytica and other similar firms' work are significant and widespread, it is of the most significance here as it relates to the core of this work: an uninformed consumer. To be ‘uninformed’ is a concept which far predates the internet, an idea which has many applications but has been heavily studied through politics. James Kuklinski, a political scientist, first elaborated on people being informed and uninformed within a political context. He explained that to be informed, people must have factual beliefs on an issue, and those beliefs must be accurate. If people do not hold factual beliefs, they are uninformed (Kuklinski et al., 2000). Elina Lindgren, a more contemporary political scientist, draws an important distinction to the reality of human nature: making choices rooted in fallacy. She claims, “this division of citizens as being either informed or uninformed ignores the fact that people might believe in the wrong answer – something which should be considered distinct from a lack of knowledge and beliefs” (Lindgren et al., 2022). These concepts have been discussed readily in political contexts but their relevance to the attention and consumer economies cannot be overstated.

The consequence of an uninformed user is severe. Users must navigate an increasingly relevant social sphere while not understanding its actual function. Pew Research Center data explains, “the public increasingly says they don’t understand what companies are doing with their data. Some 67% say they understand little to nothing about what companies are doing with their personal data” (McClain et al., 2023a). Not only do consumers not feel they have a grasp on what their information is being used for, but often that lack of understanding influences how they interact with the platforms. A 2021 study by Sigitas Urbonavicius

et al. explained, “[social media users’] willingness to disclose personal data was negatively impacted by the perceived lack of control” over data collected (p. 82). There is a correlation with increased awareness of data collection practices and perceived loss of control. That lack of control over users’ own data collection often drives users to minimize their disclosure, if given an opportunity. A Consumer Reports survey from 2024 supports this, finding that 78% of respondents were in favor of regulation and the limiting of data collection by various companies (Medintz, 2024).

In recent years, especially in the wake of scandals and lawsuits revolving around how these tech giants utilize user’s data, mistrust in the companies (and many governments) are on the rise. As news and information continues to circulate around various actors mishandling personal data, trust continues to decline across ages, political affiliations and identities. From 2019 to 2023, we see the percentage points raise 7 or more percent for multiple trust-centric questions, including the lack of trust Americans have in how the government is using their data and how little they understand about how their data is used (McClain et al., 2023a). The co-development of these sentiments suggests that, when having a true and fair grasp of how their information is used and shared, people are less trusting of the companies and platforms which claim their information. individuals who are better informed about possible misuse of personal data have a higher probability of opting out and choosing not to disclose such information. A 2020 study explains, “when deciding whether to disclose information, people will consider the amount of privacy collection occurring” (Lee and Yuan, 2020).

When users across age groups have an increased understanding of malevolent practices, their disillusion heightens. After the immediate breach of the Cambridge Analytica scandal, “Facebook had lost $50 billion in market capitalization in two days” (Richter, 2019). The rapid sharing of this information, by journalists, media outlets and individuals alike, gave users a better idea of their digital landscape. Almost immediately Facebook lost public favor and, consequently, public funds. As this example shows, an informed consumer is a threat to the profits of these major media juggernauts.

We also see this discrepancy illustrated by the correlation of where the best privacy legislation exists and the subsequent profit of those regions. The profit margins for US users is drastically higher than that of EU users. 46% of the total revenue of Alphabet, Google’s parent company, comes from the US alone, and 44% of Meta’s almost 115 billion dollar advertising revenue comes from the US and Canada, according to Visual Capitalist (Ang, 2022). The US is the largest profit market for these companies and also has the weakest data protection legislation, in comparison to the EU. The European Union has implemented the General Data Protection Regulation (GDPR) as of 2018 and, according to the EU, is “the strongest privacy and

security law in the world" (*The General Data Protection Regulation,* 2024). This regulation increases the control citizens have over their data, and places the obligation on the companies engaging with users in the EU. Critically, this regulation requires a "right to erasure," or the right for individuals to request their personal data be deleted, something not guaranteed everywhere. In the United States, the legislation is not comparable and, as a result, corporations have a much more access to Americans' online data.

There is also the subject of privacy policies for the sites and companies themselves. A report by the *New York Times* shares a synthesis of several privacy policies, which they also put into Lexile, a software designed to understand reading levels of text; Litman-Navarro explains,

> to be successful in college, people need to understand texts with a score of 1300. People in the professions, like doctors and lawyers, should be able to understand materials with scores of 1440, while ninth graders should understand texts that score above 1050 to be on track for college or a career by the time they graduate. Many privacy policies exceed these standards. (2019).

This coincides with reports that users do not have an understanding of what they are agreeing to in said privacy policies. Dr. King, the director of consumer privacy at Stanford's Center for Internet and Society, is quoted by the Times as saying, "these documents were created by lawyers, for lawyers. They were never created as a consumer tool" (Litman-Navarro, 2019). The legal jargon and low readability scores littering these policies is effective in making it difficult to for consumers to comprehend these policies.

Separate from the issue of clarity, most users do not read the terms and conditions at all. The tone evoked from the terms used by these companies are meant to not set off any alarms in an average user, but rather aid in maintaining an even-toned reaction from users *if* they read the terms they are agreeing to. It should be mentioned, however, that most users do not read the terms and conditions of apps and platforms they use. Nili Steinfeld explains that when users have the option of accepting website terms and conditions without reading a policy, they will generally forgo reading the document… even when users decide to click a non-obligatory link to read the policy, they spend much less time and effort actually reading the document (2016).

These policies are also generally designed to technically relay accurate information in such a way that if a user does not have a strong grasp of the terminology, they are unlikely to understand the full scope of the term. This only worsens the uninformed consumer problem. Users are constantly being fed privacy policies that are intentionally vague and difficult to understand (Parker, 2024). Over time, users are less likely to

read the policies and more likely to be confused if they do attempt to read them. In the document, still, there is mystery. The vague language is designed to “protect companies” (Litman-Navarro, 2019) and provides legal room for the corporations behind these services, giving them broad access and users limited control. The less specific the language, the less likely companies are to receive backlash, legally or publicly.

While the EU’s GDPR had a positive impact on some privacy policies, there is much left to be desired. There remains the issue of poor user comprehension as it relates to what data is being collected, and how it is used. About Google’s privacy policy specifically, *The Times* says, “the policy became more readable at the expense of brevity after the introduction of the General Data Protection Regulation…The regulation includes a clause requiring privacy policies to be delivered in a ‘concise, transparent and intelligible form, using clear and plain language’” (Litman-Navarro, 2019). It does not help that, when viewing the policies directly from the source, a user could come away with little understanding of the policy consented to.

A 2024 study on the efficacy of online privacy policies explains, “even if individuals can easily access information, high understanding cost might prevent individuals from making informed choices” (Ding and Huang, 2024, p. 13). Companies are advantaged when users seek more information “direct from the source” as a result of said low comprehension and high time commitment of reading the policies in their entirety. Ding and Huang touch on this, stating

> subjects must spend considerable time reading all the privacy policies to which they have to consent… [The] content of privacy policies is too complex for individuals to understand. Understanding the explanations of the collection and use of personal data typically requires expertise beyond the comprehension of most data subjects. (2024, p. 3).

Often the source information, if digested at average comprehension, leaves a user with a minimal understanding of the consent they are giving. It is not easy for users to understand how their time and information is being used online, and companies benefit. When users do become informed, their behavior changes. An earlier study from the Pew Research center provides an example:

> After National Security Agency contractor Edward Snowden disclosed details about government surveillance programs starting in 2013, 30% of adults said they took steps to hide or shield their information and 22% reported they had changed their online behavior in order to minimize detection. (Rainie, 2018).

Additional studies, like one from Christine Prince in 2018 conclude, “individuals who are better informed about possible misuse of personal data have a higher probability of opting out and choosing not to disclose such information” (p. 30). Within the economic landscape of data brokerage, a decline in user disclosure has a negative economic impact on social media companies.

The most informed populations are the ones who tend to take the strongest action to protect their privacy. Across Pew’s data privacy related research, younger populations are consistently more informed and have a higher confidence in their understanding of the digital privacy landscape when compared to older generations. These are the same populations who have the highest percentage of action when it comes to prioritizing data privacy for themselves. We see this through research from the Pew Research Center,

> 76% of social media users under 50 say they have changed their privacy settings on social media sites. 49% … say they have used a browser or search engine that doesn’t keep track of what they’re doing. 42% … say they have used messaging apps or services that encrypt their private communications. (McClain et al., 2023b).

Lee and Huang’s research agrees, stating that students used various strategies for managing their privacy, including limiting access and information to their profile through information exclusion and strategic friending decisions (2020). Young people have more familiarity, comprehension and privacy practices online.

In addition to a decline in user trust, companies have seen financial loss in the aftermath of scandals rooted in data collection and privacy issues. There has been a growth in both users and governments seeking stronger protections and more privacy across their browsing and a growing disillusion with the social media landscape as it exists today. A Gartner survey of 263 consumers between July and August of 2023 found 53% of consumers believe the current state of social media has decayed compared to either the prior year or to five years ago. The top reasons for this perceived decline were the spread of misinformation, toxic user bases and the prevalence of bots. A perceived decay in the quality of social media platforms was expected to drive 50% of consumers to abandon or significantly limit their interactions with social media by 2025 (Gartner, 2023). A decline in use across these platforms is detrimental for the actual revenue of these companies, a fate avoided whenever possible –even if that means sowing divisive or ‘bad’ information in order to maintain engagement.

With the threats of legislation and user decline, it is easy to imagine companies are more desperate than before to maintain these high levels of profit and engagement. In the aftermath of scandals and political

upheaval, and with many users looking to deprioritize their social media use, the companies referenced here are under increasing pressure to maintain an environment palatable to their ultimate customers– advertisers. If use declines, the mixed media economy withers. There is less data to be sold, less engagement with ads. While social media has been trading in the dark, users have been fighting against their unknowing. Users want more choice and more transparency even if it hurts advertisers.

Just this year (2025) Meta did a complete overhaul on their privacy policy, one of the fundamental aspects of which is improved clarity (UMA Technology, 2025). According to UMA Technology, Meta aims to "rebuild user trust that has eroded following various scandals and regulatory pressures" (2025). It is not easy for users to understand how their time and information is being used online, and companies benefit. These changes come at the cost of this 'trading in the dark,' as massive fines and legal ramifications rack up for these companies. Their profits were best before users wanted a better understanding of their practices, and now they are adjusting to expectations of various governments in the way of disclosure and policy adherence.

Conclusion

Part of the success of these companies lies in making it difficult for a consumer to have a true grasp on their digital environment. The obscuring of information occurs online in many ways. First, the policies and practices of these companies are vague and not transparent. That inherently shields any less-than-determined consumers from a high understanding of the company operations as defined by themselves. There is also an influx of data across platforms, which both oversaturates and overwhelms the average consumer. This aids in dissuading many consumers from active investigation into the functioning of their favorite apps. Lastly, companies have been proven to act outside the terms and conditions outlined by their own internal and external bodies. These broad examples craft a clear understanding of the uphill battles faced by a consumer desiring to be informed. The task is made more difficult by the endless stream of platform and policy changes. These are fundamental elements of the profit models used by these social media companies.

This article elucidates the truth of how incentivized these companies are to keep consumers at a minimum comprehension of the way their data is scraped, bought and sold. When users are more present -more *engaged*- on the platforms and services these companies provide, their profit margins increase. They are able to sell more expensive advertising at a higher volume. They are able to sell increasingly accurate data to more and more data brokers. When consumers are uninformed about how this data is used and sold, the

companies, in effect, make their trades in the dark. Users interact at high rates, with little to no understanding about how these companies generate their profits.

When users are more informed, they tend to want different rights and procedures for their data and their privacy. When there is a strong understanding of how their data is collected, users tend to try and adjust their privacy settings in their digital spaces. When users have a grasp of how their data is sold, they tend to limit data collection where possible. More threateningly, they limit their usage. As more scandals and understanding breach into the mainstream surrounding the realities of data surveillance and privacy breaches, the weariness grows and trust falls, across user audiences.

The biggest threat to these companies is that the lack of attention ends, and that people care about their data. It is ultimately at the benefit of said companies for users to have little to no understanding of what they are doing on the other side of their algorithms. This problem is not new to today, but is one that has and continues to worsen, even in spite of governmental and institutional attempts to curb the data collection. The takeaway from this research is, as companies continue to profit, the users themselves must become active in their own digital lives, in the interest of the self and the collective.

Bibliography

Allyn, B. (2022, November 14). Google pays nearly $392 million to settle sweeping location-tracking case. *NPR*. https://www.npr.org/2022/11/14/1136521305/google-settlement-location-tracking-data-privacy

Anderson, J. and Rainie, L. (2017, October 19). The Future of Truth and Misinformation Online. *Pew Research Center*. https://www.pewresearch.org/internet/2017/10/19/the-future-of-truth-and-misinformation-online/

Ang, C. (2022, April 25). How Do Big Tech Giants Make Their Billions? *Visual Capitalist*. https://www.visualcapitalist.com/how-big-tech-makes-their-billions-2022/

CBS/AP. (2018). Can Facebook restore public trust after Cambridge Analytica scandal? *CBS News*. https://www.cbsnews.com/news/facebook-cambridge-analytica-restore-public-trust-after-privacy-scandal/

Chomanski, B. (2025). The challenge of regulating digital privacy. *Critical Review of International Social and Political Philosophy, 0*, 1-25. https://doi.org/10.1080/13698230.2025.2478725

CLRN. (2024, December 9). What are social media engagements? *California Learning Resource Network*. https://www.clrn.org/what-are-social-media-engagements/

DeFazio, A. (2025, April 4). How Much Do Instagram Ads Cost? (+How to Make the Most of Your Budget). *WordStream*. https://www.wordstream.com/blog/ws/2021/02/08/instagram-ads-cost

Ding, X. and Huang, H. (2024). For whom is privacy policy written? A new understanding of privacy policies. *Computer Law & Security Review*, *55*, 1-13. https://doi.org/10.1016/j.clsr.2024.106072

EDPB. (2023, May 22). 1.2 billion Euro fine for Facebook as a result of EDPB binding decision. *European Data Protection Board*. https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

Fuchs, C. (2020). *Communication and Capitalism. A critical theory*. University of Westminster Press. https://doi.org/10.2307/j.ctv12fw7t5

Gartner Inc. (2023, December 18). Gartner Predicts 50% of Consumers Will Significantly Limit Their Interactions with Social Media by 2025. *Gartner*. https://www.gartner.com/en/newsroom/press-releases/2023-12-14-gartner-predicts-fifty-percent-of-consumers-will-significantly-limit-their-interactions-with-social-media-by-2025

Heiligenstein, M. (2023, August 8). How companies track you online – the definitive guide. *Firewall Times*. https://firewalltimes.com/how-companies-track-you-online/

Hern, A. (2018, May 6). Cambridge Analytica: How did it turn clicks into votes? *The Guardian*. https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie

Horwitz, J. (2023). *Broken code: Inside Facebook and the fight to expose its harmful secrets*. Doubleday.

Influencer Marketing Hub. (2025, March 21). 20 of Instagram's highest paid stars in 2024. *Influencer Marketing Hub*. https://influencermarketinghub.com/instagram-highest-paid/

Keegan, J. and Ng, A. (2021, September 30). There's a multibillion-dollar market for your phone's location data*. The Markup*. https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data

Kemp, S. (2025, March 23). Digital 2025: Global Overview Report - DataReportal – Global Digital Insights. *DataReportal*. https://datareportal.com/reports/digital-2025-global-overview-report

Klosowski, T. (2021, May 6). We checked 250 iphone apps-this is how they're tracking you. *The New York Times*. https://www.nytimes.com/wirecutter/blog/how-iphone-apps-track-you/

Kreiss, D. and McGregor, S. C. (2017). Technology firms shape political communication: The work of Microsoft, Facebook, Twitter, and google with campaigns during the 2016 U.S. presidential cycle. *Political Communication*, *35*(2), 155–177. https://doi.org/10.1080/10584609.2017.1364814

Kuklinski, J. H., Quirk, P. J., Jerit, J., Schwieder, D. and Rich, R. F. (2000). Misinformation and the Currency of Democratic Citizenship. *The Journal of Politics, 62(3)*, 790-816. https://www.jstor.org/stable/2647960

Lee, Y.-H. and Yuan, C. W. (2020). The Privacy Calculus of “Friending” Across Multiple Social Media Platforms. *Social Media + Society*, *6*(2), 1-10. https://doi.org/10.1177/2056305120928478

Lindgren, E., Damstra, A., Strömbäck, J., Tsfati, Y., Vliegenthart, R. and Boomgaarden, H. (2022). *Knowledge Resistance in High-Choice Information Environments*. Routledge. https://doi.org/10.4324/9781003111474-10

Litman-Navarro, K. (2019, June 12). 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

McClain, C., Faverio, M., Anderson, M. and Park, E. (2023a, October 18). 1. Views of data privacy risks, personal data and Digital Privacy Laws. *Pew Research Center*. https://www.pewresearch.org/internet/2023/10/18/views-of-data-privacy-risks-personal-data-and-digital-privacy-laws/

McClain, C., Faverio, M., Anderson, M. and Park, E. (2023b, October 18). How Americans View Data Privacy. *Pew Research Center*. https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

Medintz, S. (2024, November 20). Americans Want Much More Online Privacy Protection Than They’re Getting. *Consumer Reports*. https://www.consumerreports.org/electronics/privacy/americans-want-much-more-online-privacy-protection-a9058928306/

Nguyen, S. (2024, August 20). FTC imposes $5 billion penalty and sweeping new privacy restrictions on Facebook. *Federal Trade Commission*. https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook

Parker, K. D. (2024, August 12). The hidden dangers of privacy laws like the GDPR and CCPA. *Forbes*. https://www.forbes.com/councils/forbestechcouncil/2020/11/25/the-hidden-dangers-of-privacy-laws-like-the-gdpr-and-ccpa/

Prince, C. (2018). Do consumers want to control their personal data? empirical evidence. *International Journal of Human-Computer Studies*, *110*, 21-32. https://doi.org/10.1016/j.ijhcs.2017.10.003

Rahman-Jones, I. (2024, August 23). Should you have to pay for online privacy? *BBC News*. https://www.bbc.co.uk/news/articles/c93599ejdeno

Rainie, L. (2018, March 27). Americans’ complicated feelings about social media in an era of privacy concerns. *Pew Research Center*. https://www.pewresearch.org/short-reads/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/

Richter, F. (2019, May 11). Wall Street Has Moved On From Cambridge Analytica Scandal. *Statista*. https://www.statista.com/chart/13822/facebook-share-price/

Sharma, R. and Chandola, V. (2024). Data broker market. *Dataintelo*. https://dataintelo.com/report/data-broker-market

Shukla, S., Bisht, K., Tiwari, K. and Bashir, S. (2023). *Data Economy in the Digital Age*. Springer. https://doi.org/10.1007/978-981-99-7677-5_1

Simon, H. A. (1971). Designing Organizations for and Information-Rich World. In M. Greenberger (Ed.), *Computers, communications, and the public interest* (pp. 37-72). Johns Hopkins University Press. https://gwern.net/doc/design/1971-simon.pdf

Singh, B. (2024, October 11). The Privacy Policy of Social Media Platforms. *The Law Communicants*. https://thelawcommunicants.com/the-privacy-policy-of-social-media-platforms/

Steinfeld, N. (2016). "I agree to the terms and conditions": (how) do users read privacy policies online? an eye-tracking experiment. *Computers in Human Behavior*, *55*, 992-1000. https://doi.org/10.1016/j.chb.2015.09.038

Stewart, T. (2025, April 3). Driving engagement: How attention delivers profits. *New Digital Age*. https://newdigitalage.co/advertising/attention-profits-uber-advertising-lumen-research-paul-wright-mike-follett/

Tau, B. (2024). *Means of control: How the Hidden Alliance of Tech and government is creating a new American Surveillance State*. Crown.

Team, T. (2017, October 30). Facebook's Strong Ad Revenue Growth to Continue. *Forbes*. https://www.forbes.com/sites/greatspeculations/2017/10/30/facebooks-strong-ad-revenue-growth-to-continue/

The General Data Protection Regulation - Consilium. (2024, June 13). https://www.consilium.europa.eu/en/policies/data-protection-regulation/

Tremblay, A. (2024, February 27). *2024: The Year of Disengagement from Social Media*. Tink. https://www.tink.ca/en/insights/2024-year-disengagement-social-media

UMATechnology. (2025, January 27). Meta Rolls Out Privacy Policy Update for Instagram and facebook. *UMA Technology*. https://umatechnology.org/meta-rolls-out-privacy-policy-update-for-instagram-and-facebook/

UpGrow. (2024, October 25). What data does Instagram collect. *UpGrow*. https://www.upgrow.com/blog/instagram-data

Urbonavicius, S., Degutis, M., Zimaitis, I., Kaduskeviciute, V. and Skare, V. (2021). From social networking to willingness to disclose personal data when shopping online: Modelling in the context of social exchange theory. *Journal of Business Research*, *136*, 76-85. https://doi.org/10.1016/j.jbusres.2021.07.031

