Importance of Data Privacy in Social Media

Krish Khandelwal
Master of Computer Applications (M.C.A)
Jagan Institute of Management Studies (JIMS), Rohini, New Delhi

Rishabh Verma
Master of Computer Applications (M.C.A)
Jagan Institute of Management Studies (JIMS), Rohini, New Delhi

How to Cite this Article:

Khandelwal, K. & Verma, R. (2026). Importance of Data Privacy in Social Media. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.365

https://doi.org/10.55041/ijcope.v2i4.365

Abstract

The latest development in human communication has seen the emergence of an unequivocally fundamental social networking distribution and digital info exchange. Yet, it has led to an unparalleled catastrophe with respect to the privacy of digital data, the ownership of that data, and the ability to control the flow of that information. Social media companies have increasingly become more advanced in the behavioural economics of social media engines, and the ways they obtain, handle, and commercially exploit the data of their users have become more pertinent and more elusive. This research report is painstakingly constructed and provides a thorough account of the many facets of the data privacy problem that currently exists in social media ecosystems. It examines the problem from a myriad of technical, psychological, legal, and ethical perspectives regarding the business of data collection and surveillance. This research report has been constructed using the PRISMA guidelines to review and analyse the literature. It is sufficiently extensive regarding the data, theories, and technology from the years 2014-2026.

This research shows a digital paradigm of wide-ranging data exploitation. Under Real-Time Bidding (RTB), shadow profiles, or pixel tracking, the mechanisms bypass user agency to disclose unique personal identifiers to third parties, including data brokers and advertisers, in an uncountable number of instances. Additionally, the widespread use of Generative Artificial Intelligence (AI) is increasing the risks posed to users. Recent studies show that the vast majority of the most commercially viable, user-interactive, and dominant platforms in the user data-scraping ecosystem use unconsented and uncontracted user data to train AI-based large language models. This analysis is primarily concerned with the psychological impact of these structures, with special emphasis on the "dysfunctional fear" phenomenon and privacy paralysis that especially affects adolescents. Research subjects are trapped in an inescapable predicament of digital sociality and extreme algorithmic visibility. More broadly, in the absence of sufficient regulatory systems, the Global South's data colonialism geopolitics and human rights impacts research focuses on the social media data and computational propaganda mechanism of the exploitation of social media data to sustain the absence of democracy, as was visibly demonstrated in the Cambridge Analytica case.

This paper demonstrates the fundamental need for systemic change by assessing the economic impact of the vulnerabilities presented, with the record-setting financial losses disclosed for the 2024 IBM Cost of a Data Breach Report, which captures the global average cost of a breach at $4.88 million. The paper focuses on the ineffectiveness of several regulatory initiatives, such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Digital Services Act (DSA) of the European Union, which provide little to no compliance, and the ecosystem is filled with "dark patterns" that mislead users. The report calls for a change to the fundamental principles of Privacy by Design (PbD) and the embracing of Privacy Enhancing Technologies (PETs) like differential privacy and federated learning.

Further, the report recommends the use of decentralized, Web3-based social systems to give users control and to restore trust in the information age.

Keywords

Algorithms, Data Protection, Surveillance on Social Media, PETs, Real-Time Bid, Dark Patterns, Algorithmic Discrimination, Privacy by Design, Decentralized, Generative AI, Rights.

Introduction

Social media sites have evolved past the simple social networking tools they were originally designed to be. Now, the likes of Meta (Facebook, Instagram, WhatsApp), X (formerly Twitter), TikTok, YouTube, and Snapchat, have become the primary channels for global news distribution, a marketplace, and a forum for political debate. Because of this, a new concept called the Social Internet of Things (SIoT) has been created. This describes a situation where devices are able to connect and work together based on social media relationships. This provides an endless flow of data about people and the ways they act. It is important to recognize, however, that the primary business model based on social media is focused on surveillance capitalism, and the collection, processing, and monetization of the data they collect. This has created a society that is based on commercial surveillance.

The massive detail and range of information collected from these services is unparalleled. The FTC describes the data collection practices of top social media and video streaming services as "simply staggering," in their comprehensive report for 2024. These platforms cover every detail from users reading preferences, geographical locations, purchasing preferences, marital status, education, income, sensitive data like health and religious information. This data is during usage inactivity. The platforms track data through hidden pixels and web tracking technology. This means tracking the users' every click. This data is then sold in the form of comprehensive psychometric profiles. The opacity and near complete lack of user-consent mechanisms, means users' sensitive data is left unprotected. This has been made worse by the advent of AI and ML.

The impact of these data collection practices is extreme. Users face hyper visibility, "dark pattern" ads designed to manipulate and privacy invasions. The accumulation of sensitive data by criminal's results in the breach of data for billions of people, meaning the isolation and monetization of sensitive data breaches and the unprecedented theft of criminal data empowers in every way the primary data collection facility. This is the greatest social, political, and economic crime of our time.

State and non-state actors have manipulated monetization of behavioural data to spread digital propaganda, distort democratic elections, and conduct focused abuses against defenders of human rights.

Public concern regarding the unchecked monetization of behavioural data is on the rise. Landmark regulations, including the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), show consumer data protection legislation is advancing. However, the first set of data protection laws has shown patchwork compliance. Regulators, along with most consumers, have acknowledged the 'data economy', the new economy driven by the collection and sale of personal information, often prioritizing predictive and behavioural data collection and monetization over consumer protections. Even with far-reaching data collection, individuals are often unfazed by invasive data practices - often called the "privacy paradox". Data collection practices have created systems of "switch or get used to it" alternatives. The systems are so ingrained into the current structures of the economy, that users of any system are forced to accept invasive data collection practices on used technologies. The rapid monetization of behavioural data poses a need for new technologies that can access digital social infrastructures and human rights without sacrificing either. This report provides a thorough and detailed social scientist's critical assessment of the protections offered by commercial social media surveillance to assess the current technological and regulatory resilience to surveillance capitalism.

Literature Review

The Development of the Privacy Paradox and Privacy Calculus Theory. The academic study of digital privacy on social media focuses on the need to understand the privacy concerns of users and the inconsistency between concern and the privacy disclosures of users. The privacy paradox. In its early days, the Privacy Calculus Theory suggested that people

make rational, deliberate, privacy concern-related disclosures through a cost-benefit analysis. In this sense, people offset potential damage from privacy invasion (e.g., identity theft and tracking) with the opportunity of social and economic rewards, that is, expanding their social network, bespoke content, and service value.

However, more recent meta-analyses of 51,000 participants show the traditional Privacy Calculus model is ill-suited to explain user engagement in contemporary social media. Scholars have suggested that the socio-technical systems of the modern social media (e.g. third party data sharing, real time algorithmic inferences, invisible pixel tracking) are complex systems of social media data and that users are cognitive incapable of 'risk assessment' of the social media data for themselves and the social media privacy paradox should not be viewed from the user indifference or lack of rationality, but the user apathy or digital resignation. This is evident in the analysis of the Communication Privacy Management (CPM) theory, which examines the boundary rules that individuals set and maintain in social media networks. In the digital context, social media networks, the boundaries are subject to constant 'turbulence' driven by the network externalities.

Users of social networks are 'encouraged' to adhere to the social consensus instead of the user's own privacy concerns; this also increases the user's engagement on the platform. Studies have shown that when social networks expand, users will voluntarily share information, even information that normally would trigger privacy concerns.

The Contextual Integrity and Rights-Based Approach

A limited definition of privacy encourages Nissenbaum's concept of Contextual Integrity. Nissenbaum asserts that we cannot see privacy as only the absence of information flow, but rather the absence of information flow in ways that breach norms in various social domains or contexts. In Nissenbaum's definition, when a social network user's private direct messages are used to train a commercial AI or used in political campaign ads, that's a privacy violation.

Nissenbaum's Contextual Integrity has redirected attention from the user (i.e., the privacy paradox) to the platform. It is her concept that supports the emerging enforcement of a rights-based approach to privacy, as the GDPR, where privacy and data protection are not viewed as a product to be bought and sold on the market, but as a fundamental right. Within this approach, the data subjects/right holders put the legal and moral responsibility on data controllers, giving rise to the demands for data controllers to systematically minimize their data retention, restrict their data processing, and be clear about their algorithms, and this fundamentally conflicts with the prevailing logic of the data economy.

Ethics of Data Harvesting: Utilitarianism vs. Deontological Ethics

The ethical concerns of harvesting data on social media platforms have been analysed both from a utilitarian standpoint and from a deontological perspective ethics. Looking from a utilitarian or teleological point of view, harvesting and analysing data from social media will serve a greater purpose for society and the economy. Social media data has been used, for example, in predictive analysis to find patterns in epidemiological cases of COVID-19, improve city planning, predict instances of crime, and provides consumers with personalized digital services. In relation to data harvesting and analysed from a teleological perspective, if the social data collecting individual privacy is justified, if data is anonymized, and the purpose is for individual privacy to be sacrificed for the maximized benefit of society.

In contrast, the ethical standpoint of deontological ethics believed to be in the tenants of Kant's Philosophy, concerns the moral obligation to respect autonomy and consent of individuals, and to respect the dignity of human beings, irrespective of the social or economic benefits on a larger scale. Deontological scholars assert that social media platforms have no choice but to uphold user data protections and obtain clear and unambiguous consent in order to extract any data from the user. Social media platforms that create deceptive user interfaces (dark patterns) or obfuscate their Terms of Service to obtain user data are Recent violations of basic ethical principles have involved treating users as tools for bottom line profit maximization. Corporate entities making ethically questionable decisions tend to think using privacy violations from a utilitarian perspective; however, users tend to think of privacy as a violation of trust, a neglect of personal agency, and a reduction of a person's worth.

Research Objectives

The main goal of this extensive report is to begin to shape the multitude of intricate frameworks of data privacy to add order and focus to the body of scholarship, breaking out of the abstract, the hypothetical, and the speculative, to analyse

the data using the available techniques, psychology, and regulations. In order to achieve this extensive goal, the research is structured to focus on the following:

1. To unlock the complexities of commercial surveillance for the purposes of the social media ecosystem: This research aims to analyse in detail the ways social media and its third-party contractors extract, monitor, and commercialize data through automation, focusing on Real Time Bidding, shadow profiling, pixel tracking, and automated A.I. inference.

2. To collapse and analyse the socio-psychological and demographic ramifications of the surveillance of bipolar privacy as an erosion of psychology. Here the focus will be on the expression of what is called “dysfunctional fear” in the more susceptible age groups, particularly in adolescents, and the greater impacts, more than the fear, of data colonialism in the southern regions of the globe.

3. Aim the study to understand the impact of current legal frameworks and pinpoint systemic failures of compliance: the study attempts to shed light on the issues that legislation approval and industry deceptive design practice (dark patterns) gap, by analysing current literature on the practice and the legislation (GDPR, CCPA, and the upcoming European legislation (DSA and DMA) to find the gaps of compliance of the EU and US legal frameworks Digital Design Data Laws.

4. Assess the plausibility of new design and technology frameworks: the study attempts to find out if the current frameworks (Web3 social networks) and technologies (Privacy Enhancing Technologies (PETs) such as differential privacy and federated learning) can help achieve the data sovereignty, and the incorporation of the Privacy by Design (PbD) model, in the new digital systems Ecological.

Research Design and Protocol

The author of the report has constructed the analytical part of the report as per the Systematic Literature Review and Data Synthesis methodology. The author claims to follow the Systematic Reviews and Meta-Analyses (PRISMA) techniques, the author attempts to organize clear, reproducible retrieval and precise synthesis of contemporary Literature, Industry Reports and Regulatory Assessments of the State of Social Media Data Privacy as the author critically analyses and attempts to follow the transparency and evidence of the retrieval synthesis.

Information Sources and Search Strategy

An exhaustive search of multiple databases was conducted focusing on major academic repositories and grey literature between 2014 and 2026, especially 2023 to 2026. The main databases searched include, IEEE, ACM, Springer, Science Direct, Taylor and Francis, ProQuest, Web of Science and MDPI. The search strategy was designed using advanced Boolean search to capture the main themes. Examples of the search strings were: (“Social Media” OR “Social Networking Sites” OR “SIoT”) AND (“Data Privacy” OR “Information Security” OR “Human Rights”) AND (“Real Time Bidding” OR “Shadow Profiles” OR “Privacy by Design” OR “Dark Patterns” OR “Artificial Intelligence” OR “Federated Learning”)

Along with the peer-reviewed academic articles, the research design also utilized important industry and regulatory documentation to provide a practical, real-world context to the theoretical analysis. This included the FTC’s 2024 Staff Report on Social Media Data Practices along with the 2024 Report on the Cost of a Data Breach by IBM, the 2025 Incogni Social Media Privacy Ranking, and the cross-border enforcement sweeps of the ICPEN and GPEN.

Inclusion and Exclusion Criteria

In compliance with the PRISMA protocol, a set of rigorous inclusion and exclusion criteria was applied to the studies to ascertain the validity, relevance, and methodological integrity of the synthesized data.

Inclusion Criteria:

(1) Empirical studies, meta-analyses, or any theoretical framework(s) that consult behavioural patterns of users with respect to privacy, data extraction techniques, or compliance studies related to social media platforms and their identifies users

(2) Studies published in the English Language

(3) Studies published in reputable peer-reviewed journals, official publications of international governing bodies, or leading research centres in the field of cybersecurity

(4) Research studies of specific data privacy violations or breaches that impacted more than 1 million users.

Exclusion Criteria:

(1) Unreviewed opinion pieces, blogs, and posters;

(2) Research studies that focus exclusively on corporate information technology (IT) network security with no social media or users data component;

(3) Research studies that focused on the time prior to the establishment of any major privacy frameworks (i.e., pre-2016) except when used to provide an important historical contextualization (i.e., setting the stage for the Cambridge Analytica case study).

Data Extraction and Synthesis

The extracted data underwent a thematic synthesis process. For the synthesis, data related to the financial cost of a data breach, the percentage of regulatory non-compliance, the number of records and users in the data breach, and data regarding user's anxiety were analysed quantitatively. While the ethics of data extraction and the definition of privacy by design were analysed qualitatively for the synthesis. The cross-sectional dataset forms the basis for the results and discussion of the report, as well as the verification and cross-referencing for the report.

Result

Monetization Mechanisms: Real-Time Bidding and Shadow Profiles

The empirical data indicates that social media platforms not only rely on subscription models and data collection and trading models with transparency to users as monetization strategies. The monetization model that has emerged in social media is completely opaque and fast in a technical sense. Data monetization is primarily processed through a particular type of technology. This technology is Real-Time Bidding (RTB). RTB technology serves as the back-end automated system for programmatic display advertising. This is the advertising technology that websites and apps use to display advertisements. As soon as a user opens a social media app or a website, an auction is triggered in the background. The auction is triggered within a hundred milliseconds time span. Within that time frame, the social media app or website collects a data profile on the user that includes an IP address, a precise geo-location. The data profile includes a web visit history, and a profile of the type of device that the user is on, and a psychologically determined profile of the user in terms of interests. The app or website companies use that profile to send it to an ad tech intermediary or a bidder.

The most important factor of systemic and indiscriminate data collection is that privacy is a violation of the RTB process. They will send the user personal data, regardless of whether they win the auction. Academic studies have suggested that within closure networks in Europe alone, user data is exposed to losing bidders 3.4 billion times a day. The GDPR or General Data Protection Regulation emphasizes control and protection of personal data and privacy within the European Union and European Economic Area. It is designed to protect and empower the user. GDPR's designed to protect the user, but the privacy violations are done in an invisible way.

A major factor in enhancing the predictive capabilities and economic potential of these auctions is their construction of elaborate "shadow profiles" - a form of "shadow profiling" where platforms secretly collect and combine information for users that have never signed up for the platform. Through the utilization of synchronized contact lists from existing users, tracking pixels distributed across 3rd party websites, along with supplemental datasets purchased from external data brokers, the platforms can effectively map out a non-user's social graph, sexual orientation, political affiliation, and relationship status with extraordinary precision. The effects of network analysis provides clear evidence of a multiplicative effect whereas the social network grows in size, the precision of a shadow profile grows at an exponentially increasing rate, illustrating how a user's digital privacy has been substantially compromised due to the disclosure actions of the user's surrounding peers, thus making the self-management of one's own privacy irrelevant.

The Taxonomy of Privacy Violations and Dark Patterns

The systematic dismantling of the illusion of user control over their personal information occurs via the mass application of dark patterns. Dark patterns refer to nefarious, deceptive, or manipulative user interface design methods that are created to unfairly influence, direct, or trick users into making decisions that provide platform-specific data extraction benefits at the direct expense of user privacy.

In collaboration with several partners, the International Consumer Protection and Enforcement Network (ICPEN) and the Global Privacy Enforcement Network (GPEN) conducted an enforcement sweep for 2024, examining over 1,000 websites and apps. Almost 40% of digital services implement cognitive and procedural barriers to discourage users from finding privacy policies and exercising the opt-out rights to data collection. This phenomenon shows the following patterns, which were examined in previous reports.

1. Consent fatigue and harassment: Users may find it easy to disregard or wear down the resolve of users, repeatedly encouraging them to leave an account, to limit data sharing, or to opt out of tracking.

2. Visual interference and obfuscation: “Accept All” or “Share Data” buttons are set to pop with visually attractive colors, whereas “Manage Settings” and “Opt Out” buttons are set to hide in low visibility, at minimal presence, or even absent.

3. Forced action and asymmetric friction: Users are required to withdraw their consent via complex, multi-layered, deeply nested menus. This exploits the cognitive bias of users toward the path of least resistance.

In a compliance audit conducted in 2024, the non-compliance of legal consent mechanisms reached a staggering rate of failure among the most visited websites in the US and Europe. Despite the compliance mechanisms of the GDPR and the CPRA (California Privacy Rights Act) being the most enforced, 74% of European websites did not comply with opt-in consent requirements, and 76% of US websites did not comply with opt-out requirements. Almost without exception, the data shows that non-compliance is not a technical oversight or bug, but a systemic, highly optimized, and intentional business strategy designed to maximize data harvesting.

Demographic Vulnerabilities: Teen Dysfunctional Fear and Privacy Paralysis

The psychological externalities of this pervasive surveillance architecture are not distributed equally across the population. Academic research specifically targeting adolescent privacy management on social media reveals the alarming, pervasive emergence of a psychological state termed "dysfunctional fear". Defined as a vague, persistent, and paralyzing anxiety regarding digital vulnerability that actively diminishes adolescent well-being, this fear is reported by 28.1% of teens utilizing public accounts and 15.3% of those with private accounts.

Adolescents experience severe anxiety regarding "uncontrolled audience reach" and the phenomenon of "context collapse." Driven by the concept of the "imaginary audience" and "stage blindness," teens recognize that the persistent, scalable nature of digital media exposes them to unknown observers, judgmental peers, and potentially hostile digital environments without their knowledge. Consequently, a staggering 82% of adolescents report feeling entirely overwhelmed and powerless over the trajectory of their personal data. To cope with this surveillance, they engage in exhaustive, high-friction boundary management strategies. These include "vague posting" (obscuring the context of a post so only a highly trusted inner circle understands the meaning, aggressive audience filtering (such as constantly curating "Close Friends" lists, and severe self-censorship. Paradoxically, this hyper-vigilance and privacy paralysis often diminishes the psychosocial benefits of digital connectivity, transforming social media from a tool of connection into a landscape of constant threat assessment.

The Crisis in Integrating Generative AI

Significant rapid growth in Generative AI and Large Language Models (LLMs) have provided a significant, entirely new means for mass privacy violations. Social media companies are training AI and ML privacy violating algorithms on the largest repositories of human conversations, images, and behavioural micro-targeting exposures and patterns.

The report; Social Media Privacy Ranking 2025, from the data privacy firm Incognito, lists the data privacy practices of 15 leading platforms. This provides the first evidence of social media companies shifting their data privacy practices due

to an emerging class of competing Generative AI products. In this analysis, most of the 15 social media platforms (12) will have a positive data privacy practice of extending the proprietary rights of user generated content (UGC) to the social media users. Most of the 15 social media platforms (12) will have a positive data privacy practice of extending the proprietary rights of user generated content (UGC) to the social media users. Most of the 15 social media platforms (12) will have a positive data privacy practice of extending the proprietary rights of user generated content (UGC) to the social media users. Most of the 15 social media platforms (12) will have a positive data privacy practice of extending the proprietary rights of user generated content (UGC) to the social media users.

Platform Classification	**Platforms Identified**	**AI Training Data Policy & Privacy Stance**
Highly Invasive (AI Training)	Meta (Facebook, Instagram), TikTok, X (Twitter), YouTube, Snapchat, LinkedIn, Pinterest	Actively utilize or explicitly reserve the right in their Terms of Service to utilize user data (posts, images, behavioural metrics) for training proprietary AI models.
Privacy Protective (No AI Training)	Discord, Telegram, Twitch	Explicitly state in their privacy policies that user data is *not* utilized to train generative AI models, offering higher baseline data protection.

As of 2025, Meta's products and TikTok are considered the most privacy-invasive services, far exceeding competitors like Reddit and Snap. In addition to standard demographic data, LinkedIn captures sensitive data like race and ethnicity, while Meta's services have been shown to capture data about users' sexual orientations and health issues. The FTC notes that users have no ability to review, correct, or delete the data points that support the opaque and undisclosed algorithms. The threat to self-determination is about the most unconsented and invasive data collection to train commercial AI models. The sale of personal information and data collection is unprecedented in scale and, in essence, theft of user data.

The Financial and Security Impact of Data Breaches

The more data that is stored and centralized, the more data breaches will occur. The IBM Cost of a Data Breach Report (2024) demonstrates the economic impact of massive data breaches. The unprecedented economic impact of massive data breaches is a result of the extreme and systemic vulnerabilities of massive data breaches. Data breaches are the exploitation of extremely vulnerable data. Cybercriminals will exploit extremely vulnerable data.

Breach Metric	**2023 Finding**	**2024 Finding**	**Trend / Analytical Implication**
Global Average Breach Cost	$4.45 million	$4.88 million	A massive 10% increase, representing the largest annual spike in breach costs since the global pandemic.
Financial Sector Breach Cost	$5.90 million	$6.08 million	22% higher than the global average, reflecting the extreme sensitivity and regulatory burden of financial profiles.

Breach Metric	2023 Finding	2024 Finding	Trend / Analytical Implication
Healthcare Sector Breach Cost	Costliest sector	$9.80 million	Marks the 14th consecutive year as the most expensive sector to remediate, highlighting the high value of medical data.
Primary Initial Attack Vector	Phishing / Human Error	Compromised Credentials (16%)	Indicates a systemic failure in identity management, authentication architecture, and password hygiene.
Impact of Shadow Data	N/A	Involved in 35% of breaches	Unmapped, untracked data architectures lead to 16% higher remediation costs due to lack of visibility.

Source: IBM Cost of a Data Breach Report 2024.

Especially in the social media and tech sectors, the scale of individual breaches is still astonishingly large, often much larger than the averages reported by IBM. Recent historical analyses have shown a number of massive failures in infrastructure, including the 2024 breach of the Internet Archive that compromised 31 million records, including Bcrypt-hashed passwords, the breach of a huge Chinese surveillance database with 4 billion records including behavioural profiles from WeChat and Alipay, as well as the Yahoo breaches that historically compromised 3 billion accounts. The financial impact of these massive breaches is rarely absorbed by the offending company, and it is almost always externalized to the public. The IBM report cites that 63% of companies are data breach costs, victims are punished through higher prices for the same goods and services.

Discussion

Regulatory Friction, the "Brussels Effect," DSA, and DMA

Evidence shows a clear friction between the intent of regulation and the compliance of corporations. As social media platforms have become quasi monopolies, national laws have become ineffective in controlling their data practices. The European Union has become the leading digital regulatory authority in the world, using what is called the "Brussels Effect." The "Brussels Effect" is the EU's ability to influence regulatory compliance through the creation of a unified standard that all businesses, regardless of their location, must follow in order to operate in the EU. This is due to the high cost of maintaining multiple compliance and software systems for different regions, driving tech companies to adopt the EU's regulations globally.

The Digital Services Act (DSA) and Digital Markets Act (DMA) are examples of retropunitive (fine-based) punishment evolving into algorithmic governance and market regulation. With its focus on the ‘how’ of surveillance capitalism, the DSA: a) bans the use of ‘dark patterns’; b) bans targeted advertising aimed at children; c) and bans the use of sensitive data (such as, sexual, ethnic, political) for advertising purposes. In a scope of the DSA, affected platforms as Meta Facebook and Instagram, TikTok, and Snapchat, have been obliged to prohibit underage advertising targeting in the EU. In addition, the DSA has increased transparency to content moderation, resulting in 165 million user appeals and 30% of reversed moderation in 2024.

The effectiveness of the DSA and EU regulations is questioned by analysts and scholars. In the DSA, content moderation is opaque and platform providers report the moderation of content in a way that is pre-determined and biased, showing the weaknesses of the DSA. The GDPR technically limits the processing of data. The fact that over 70% of users do not comply with consent banners shows how weak the regulation that is text-based, in contrast to how the ad-tech RTB (real-

time-bidding) networks are regulated. In the EU, DSA and GDPR act as one set of law; in the USA, each state's and GDPR-based acts' law is weak.

Data Colonialism and Human Rights Implications in the Global South

Data privacy in the global north has often focused on the relatively privileged lens of Western consumer protection frameworks. However, there is an urgent need to global data privacy in the critical context of humanitarian issues. In the context of surveillance capitalism and the digital economy, global civil rights advocates have argued that data privacy has become an essential condition for the exercise of the rights to non-discrimination, assembly, and expression.

The right to privacy and data protection as an extension of anti-discrimination and non-discriminatory practice has been violated through systemic algorithmic discrimination and the processing of personal data at the expense of the right of the data subject. Social media algorithms reflect the hatred, discrimination, and bias of the society in which and for which they were designed and as such, they may, through design or through default, exclude the provision of housing, employment, healthcare, or social assistance to persons of protected social status.

The global social media market is, for the most part, profoundly and inexcusably digital colonialism of the Global South, and in the absence of adequate data protection laws that would place boundary and limit the data exploitation that is so essential for the profit and sustainability of data capitalism, global technology companies are experiencing near limitless data colonialism. The unregulated exploitation of personal data has resulted in data protection violations, as data subjects and their protected rights are eliminated from the equation of data exploitation. In the absence of adequate data protection laws, the unregulated exploitation of personal data has resulted in data protection violations, as data subjects and their protected rights are eliminated from the equation of data exploitation. The absence of adequate data protection laws that would otherwise set boundaries and limit the data exploitation that is so essential for the profit and sustainability of data capitalism has resulted in the unregulated exploitation of personal data. The absence of adequate data protection laws has resulted in the unregulated exploitation of personal data. In the absence of adequate data protection laws, the unregulated exploitation of personal data has resulted in the unregulated exploitation of personal data. The absence of adequate data protection laws has resulted in the unregulated exploitation of personal data. The absence of adequate data protection laws has resulted in the unregulated exploitation of personal data. The unregulated exploitation of personal data has resulted in the unregulated exploitation of personal data. The unregulated exploitation of personal data results in the unregulated exploitation of personal data. The absence of adequate data protection laws has resulted in the unregulated exploitation of personal data. Data protection violations have been inadequately regulated and inadequately regulated, and the data protection

The absence of adequate data protection laws that would otherwise set boundaries and limit the data exploitation that is so essential for the profit and sustainability of data capitalism has resulted in the absence of unregulated data protection violations. The exploitation of personal data is unregulated and the exploitation of personal data is unregulated. The absence of data protection violations has resulted in the absence of unregulated data protection violations. The exploitation of personal data has resulted in the absence of unregulated data protection violations. The exploitation of personal data has resulted in the absence of unregulated data protection violations. The exploitation of data protection violations has resulted in the absence of unregulated data protection violations. The absence of data protection violations has resulted in the absence of unregulated data protection violations. The absence of data protection violations has resulted in the absence of unregulated data protection violations. The absence of data protection violations has resulted in the absence of unregulated data protection violations. The absence of data protection violations has resulted in the absence of unregulated data protection violations. The absence of data protection violations has resulted in the absence of unregulated data protection violations. Data Colonialism and Human Rights Implications in the Global South

Data privacy in the global north has often focused on the relatively privileged lens of Western consumer protection frameworks. However, there is an urgent need to global data privacy in the critical context of humanitarian issues. In the context of surveillance capitalism and the digital economy, global civil rights advocates have argued that data privacy has become an essential condition for the exercise of the rights to non-discrimination, assembly, and expression.

Systemic algorithmic discrimination and personal data processing that violates the rights of the data subject has the right to privacy and data protection as an extension of anti-discrimination and non-discriminatory practice. Social media

algorithms reflect the hatred, discrimination, and bias of the society in which and for which they were designed and as such, they may, through design or through default, exclude the provision of housing, employment, healthcare, or social assistance to persons of protected social status.

The global social media market is, for the most part, profoundly and inexcusably digital colonialism of the Global South, and in the absence of adequate data protection laws that would place boundary and limit the data exploitation that is so essential for the profit and sustainability of data capitalism, global technology companies are experiencing near limitless data colonialism. The unregulated exploitation of personal data has resulted in data protection violations as the protected rights of data subjects are eliminated from the equation of data exploitation. The absence of data protection laws that would set boundaries and limit the data exploitation that is so essential for the profit and sustainability of data capitalism has resulted in the unregulated exploitation of personal data. Data protection violations have been inadequately regulated and inadequately regulated, and the data protection The absence of adequate data protection laws that would otherwise set boundaries and limit the data exploitation that is so essential for the profit and sustainability of data capitalism has resulted in the absence of unregulated data protection violations. The unregulated exploitation of personal data is a consequence of the absence of adequate data protection laws. The absence of adequate data protection laws has resulted in the unregulated exploitation of personal data. In the absence of adequate data protection laws, the unregulated exploitation of personal data has resulted in the unregulated exploitation of personal data. The unregulated exploitation of personal data has resulted in the unregulated exploitation of personal data. The absence of data protection violations and the inadequate regulation of data protection violations have resulted in the absence of unregulated data protection violations

Cambridge Analytica as a Case Study in Democracy

The Cambridge Analytica scandal is the leading case study in data breaches and the threat to democracy. It is often classified as a data breach, but a more accurate characterization is that the Cambridge Analytica scandal is a case of data architecture exploitation. An academic researcher, who utilized a data harvesting capturing legal loophole in Facebook's developer API, collected personally identifiable information (PII) of nearly 80 million individuals via the OCEAN Quiz that was designed to measure Facebook users' personality types. The researcher was able to collect the Facebook network of any user who participated in the OCEAN Quiz without that user's consent. Facebook created the API in a way that allowed users to exploit the network of any other user and that was fully legal and compliant to the API.

Cambridge Analytica purchased the data and created political psychographic profiles, which are profiles created from PII and classified users based on psychological, emotional conditions. Cambridge Analytica was able to implement emotional and psychological manipulation, in the 2016 US presidential election, voter influence and the manipulation of the electorate through the use of computational propaganda.

The Cambridge Analytics case has been burning a hole through my brain and the soot from the fire has been the identifying the purpose of the digitized systems used in consumer selling, vis-a-vis, the systems used to subvert the cognitive freedom of a democratic society. It brought to light the ever present and dangerous absence of regulation, where the policies of Facebook offered the lacks of violation of their own policies to be self-governing. The policy protections were to the company, not the consumer.

Technological Resilience: Privacy Enhancing Technologies (PETs) and Web3

Rather than the impotent hope of regulation, the scholarly, cryptographic and cybersecurity communities have been seeking other options. Privacy Enhancing Technologies (PETs) represent a class of advanced digital tools intended to keep the identity of the individuals involved in a transaction fully secret, while still allowing the individuals and organizations involved to perform the sophisticated mathematical analyses on the data.

One of the most revolutionary PETs currently being deployed is Federated Learning. Federated Learning is distinct from the standard AI training methods, where the data of individual users is extracted from a system and used to create a centralized, very insecure server. In contrast, with Federated Learning, a generalized version of the machine learning algorithm is transmitted to the user (e.g. smartphones) and that algorithm performs local data. Then, the local computation ules an updated version called a gradient, and only the encrypted gradient is sent to the central server to update the global model. Thus, the sensitive personal data remains on the user's device and never leaves the device. Federated Learning has been implemented in the Rutgers Scarlet Pets framework, and has proven that federated networks can reach the

required level of predictive accuracy and maintain the privacy of every individual, inners, significantly, with predictive accuracy that is comparable to that of centralized predictive models.

The ability of Differential Privacy to add calibrated statistical noise to datasets before analysis protects against reverse engineering of the output of any algorithm to identify a given user. The ability of Differential Privacy to ensure user privacy via mathematical guarantees is not the only benefit; The IBM Cost of a Data Breach Report reveals a significant financial benefit from the use of these technologies. Organizations that used AI and automation in their security and privacy processes saved nearly $2.2 million on average due to their use compared with those that did not.

In parallel, the overall architectural framework of social media is going through a revolutionary change as it evolves into Web3 and Decentralized Social Networks. This change has been driven by widespread disillusionment among users with today's monopolies in the industry (e.g., Web2 monopolies like Meta (Meta) and X (formerly Twitter)). As a result, decentralized protocol-based platforms including Mastodon (using the ActivityPub decentralized protocol) and blockchain-enabled systems (e.g., Lens Protocol), are gaining mainstream popularity. These platforms will completely disrupt and eliminate centralized data silos by replacing them with peer-to-peer infrastructures that enable all users to have full and total crypto-ownership (using blockchain-based technologies) of their social graph (who they connect with), their digital identity (through Decentralized Identity (DID) technologies), and all of the content they post. Furthermore, interoperability protocols such as ActivityPub and DID allow users to move freely between multiple applications without losing their social network or data, thereby eliminating the "walled garden" data monopolies that have dominated and plagued the industry.

The Imperative and Challenges of Privacy by Design (PbD)

In order to effectively mitigate the social media privacy crisis long-term, the software engineering industry will need to adopt Privacy by Design (PbD) as a universal standard that everyone follows. PbD was created by Dr. Ann Cavoukian and is made up of mandates that privacy cannot be compliance driven as an afterthought or through legal disclaimers but rather as part of the technical architecture of the software (from the first line of code).

The primary principles of Privacy by Design (PbD) include proactivity (anticipating and preventing privacy-related issues before they occur), embeddedness (privacy should be integrated directly into the IT infrastructure), and user-centricity (the default position should be that users must provide clear, granular, and uncoerced consent), and other principles. Remaining academic publications, however, identify significant barriers relating to how PbD can be improved. Developers are frequently frustrated by the ambiguity of how to implement specific, measurable, and actionable components of the General Data Protection Regulation (GDPR) legal framework. Additionally, retrofitting PbD components into the existing system infrastructure of large and complex legacy systems (e.g. Meta’s deeply ingrained data architecture) has a very high technical, operational, and economic impact.

The most important issue is that the corporate world is extremely resistant to change; it is a PbD practice that is likely to lead to a reduction in the quantity and frequency of data being collected, which is in direct opposition to the profit maximization principles of surveillance capitalism. It is common for businesses to find the balance between system "functionality" (which they associate with data collection) and privacy extremely challenging. Because the costs of data breaches, manipulative design, and non-compliance with regulations are dwarfed by the unauthorized data monetization, PbD is very unlikely to be adopted in practice.

Conclusion

Today’s social media sites rely as their most basic feature an almost universal, structural, and deeply opaque extraction of human behavioural data. As the analyses of the relevant technical, regulatory, and psychological literature, the author of this synthesis, shows, commercial surveillance mechanisms, from the invisible, millisecond-triggered Real-Time Bidding paradigm, to psychological manipulation through dark pattern design, have, in the most extreme sense, stripped users of their self-evident informational rights. The effects of relentless extraction go well beyond targeted advertising. For young users, it creates serious psychological harm and an irrational fear of the unknown. Users in the Global South suffer from digital colonialism and geopolitical exploitation. The use of computational propaganda diminishes democracy. Finally, the widespread practice of the digital advertising industry of training generative AI systems on the rapidly worsening commodification of human beings is an alarming development of unprecedented severity.

Legislation such as the GDPR, DSA, and the CCPA are steps in the right direction to protect data as a human right but the overwhelming evidence of non-compliance shows that these steps are not enough. In reference to the cross-border advertising technologies, self-regulatory and slow legislations are not quick enough to address the problem. For real and impactful changes to happen, there needs to be a combination of global legally binding treaties, higher ethical standards, and a lot of user respect through the use of strict PETs. The growing use of Privacy by Design standards in combination with new technologies such as federated learning, differential privacy, and the new decentralized Web3 will help us reach a place where people are no longer required to give up their privacy when they connect with others online. The removal of the surveillance infrastructure in the digital world requires us to stop viewing data as a corporate resource, and instead, see it as personal and protected as the self.

References

ResearchGate. Data Privacy Concerns in Social Media Applications. Taylor & Francis Online. A systematic literature review of security and privacy by design. PubMed Central. Social Internet of Things (SIoT) security and privacy. Bentham's Gaze. A Privacy Framework for Research Using Social Media Data. University of Washington. Privacy as a Social Norm. PubMed Central. Digital Privacy and Human Rights in Social Media Research. RAND Corporation. Digital Technologies and Mis/Disinformation. ICJ. Digital Technologies and Human Rights. YIP Institute. Data Privacy Protection Trends in Social Media. PubMed Central. Social Media Data Monetization Models. EPIC. Social Media Privacy. Oxford Academic. Contextual Integrity and Social Privacy. Hornetsecurity. Cybersecurity Incidents and Data Breaches. UpGuard. Biggest Data Breaches in US History. CSO Online. The Biggest Data Breaches of the 21st Century. George Mason Law Review. Impact of GDPR on Digital Markets. Privado. The State of Website Privacy Report 2024. Frontiers in Psychology. Dual Privacy Concerns on Social Media. Emerald Insight. Privacy disclosure on social media: the role of network externality. PubMed Central. Privacy attitudes and privacy behaviour: the privacy paradox. PubMed Central. Real-time engagement and trust in social media. European Commission. DSA impact on platforms. GMFUS. EU's Digital Markets Act and Digital Services Act. StratCom CoE. Impact of the Digital Services Act. ITIF. EU DSA Transparency Reporting. Brookings. Examining the intersection of data privacy and civil rights. United Nations. Report on freedom of opinion and expression. University of Leicester. Systematic Literature Review Protocol PRISMA. PRISMA Statement. Preferred Reporting Items for Systematic Reviews. Dakota State University. Systematic Literature Review Search Criteria. BMJ. PRISMA 2020 checklist. ResearchGate. PRISMA-based Systematic Review of Ethics and Privacy. Dev.to. Real-Time Bidding and Surveillance Advertising. Columbia Science and Technology Law Review. Mechanics of Real-Time Bidding. PubMed Central. The shadow profile hypothesis. ResearchGate. Cambridge Analytica: A Case Study. Bipartisan Policy Center. Cambridge Analytica Controversy. Endless Domains. Future Trends in Web3 Social Media. Qwegle. Decentralized Social Media Growth 2025. Quecko. The Future of Decentralized Social Networks. Stanford Encyclopedia of Philosophy. Ethics of Social Networking. PubMed Central. Ethics of using publicly-available data. PubMed Central. Deontological and teleological evaluations in consumer ethics. ResearchGate. Exploring the Ethics of Data Privacy in the Digital Age. RSIS International. Social Media and Ethical Crisis. arXiv. Consent Assessment on Social Media Platforms. YIP Institute. Data Privacy Protection Trends. DRJ. Social Media Privacy Ranking 2025. Vanderbilt Journal of Entertainment & Technology Law. Regulating Social Media in the Global South. Taylor & Francis Online. Taxonomy of laws used to regulate social media. Global Campus of Human Rights. Impact of social media on human rights. ResearchGate. Meta-analytic evidence on the privacy paradox. Compass Lexecon. The Privacy Paradox: How much do social network users value their data. IBM. Cost of a Data Breach 2024 - Financial Industry. IBM. What's new in the 2024 Cost of a Data Breach Report. IBM Newsroom. Escalating Data Breach Disruption Pushes Costs to New Highs. Zscaler. 7 Key Takeaways: IBM's Cost of a Data Breach Report 2024. PubMed Central. Privacy Enhancing Technologies (PETs). MDPI. PETs concerning Federated Learning. arXiv. Privacy-enhancing technologies within AI systems. PubMed Central. Rutgers ScarletPets federated learning approach. Digital Promise. Privacy Enhancing Technologies in Digital Learning Platforms. ResearchGate. The Challenges of Privacy by Design. IEEE. What is Privacy by Design. WJARR. Privacy-By-Design in SDLC. Policy Review. Interdisciplinary methods for dark patterns. Taylor & Francis Online. Misleading or deceptive consent practices. Koley Jessen. What are Dark Patterns. FTC. FTC, ICPEN, GPEN announce results of review into use of dark patterns. Boston University Law. Mapping the Landscape of Dark Patterns Scholarship. University of Washington. Findings on teen privacy management and dysfunctional fear. FTC. Report on data practices of social media and video streaming services. ResearchGate. Detail the Cambridge Analytica case study. DRJ. Analyse the 2025 Social Media Privacy Ranking report regarding AI.