
| **RESEARCH ARTICLE**

The Impact of Social Media Platforms on Privacy: Examining Legal and Ethical Boundaries in the U.S

Ayotunde Omosule¹ ✉ Abayomi Ogayemi², Adeola Okesiji³, Adegbola Oluwole Ogedengbe⁴ and Odunayo Oyasiji⁵

¹*LL.B, LL.M, MA, Independent Researcher, Toronto, Canada*

³*LL.B, LL.M, Independent Researcher, Calgary, Canada*

⁴*Independent Researcher, Edmonton, Canada*

⁵*Independent Researcher, Calgary, Canada*

Corresponding Author: Ayotunde Omosule, **E-mail:** ayotundeomosule@yahoo.com

| **ABSTRACT**

This paper explores the growing tension between user privacy and the operational models of major social media platforms in the United States. As these platforms expand their influence, the boundaries between ethical responsibility and legal compliance become increasingly blurred. The paper critically examines existing U.S. data privacy laws, evaluates ethical theories relevant to digital surveillance and consent, and assesses platform practices using recent case studies. Through qualitative analysis of legal frameworks, platform policies, and regulatory actions from 2018-2023, this study reveals significant gaps between legal compliance and ethical responsibility. Findings suggest that legal protections lag behind technological capabilities, and ethical frameworks are inconsistently applied across platforms. The research proposes a four-quadrant legal-ethical framework for evaluating platform practices and provides evidence that most social media companies operate in the "legal but unethical" category. Recommendations for comprehensive federal privacy legislation, algorithmic transparency mandates, and enhanced digital literacy programs are presented as essential steps toward protecting user privacy in the digital age.

| **KEYWORDS**

Social media privacy, data protection, digital ethics, CCPA, COPPA, surveillance capitalism

| **ARTICLE INFORMATION**

ACCEPTED: 01 April 2023

PUBLISHED: 10 June 2023

DOI: 10.61424/ijlss.v1.i1.362

1. Introduction

The digital transformation of the 21st century has fundamentally altered how individuals communicate, consume information, and engage with the world around them. Social media platforms, once simple networking tools, have evolved into sophisticated data collection and behavioral modification systems that influence billions of users worldwide (Zuboff, 2019). In the United States, platforms such as Facebook (now Meta), Instagram, TikTok, Twitter, and YouTube have become integral to daily life, serving not merely as communication channels but as primary sources of news, entertainment, and social validation.

However, this digital revolution has come at a significant cost to individual privacy. The business models underlying these platforms are fundamentally predicated on the collection, analysis, and monetization of user data (Srnicsek, 2017). Users willingly share personal information, photographs, locations, and intimate details of their lives, often

without fully comprehending the extent to which this information is harvested, processed, and commodified. The resulting privacy concerns have sparked intense debates about the appropriate balance between technological innovation, corporate profit, and individual rights.

The tension between privacy and platform operations is particularly acute in the United States, where the regulatory landscape remains fragmented and often inadequate to address the complexities of modern data practices (Solove, 2021). Unlike the European Union, which implemented the comprehensive General Data Protection Regulation (GDPR) in 2018, the United States continues to rely on a patchwork of sector-specific laws and state-level initiatives that leave significant gaps in protection.

This paper investigates the intersection of legal frameworks and ethical considerations in the context of social media privacy, with particular attention to the period from 2018 to 2023, during which several high-profile privacy scandals, regulatory actions, and legislative initiatives have shaped the landscape. The research addresses three primary questions: (1) What are the key legal frameworks governing social media privacy in the U.S.? (2) How do platform practices align or conflict with these frameworks? (3) What ethical considerations are involved in the collection and use of personal data by social media companies?

Through systematic analysis of legal documents, platform policies, regulatory actions, and academic literature, this study develops a comprehensive framework for understanding the current state of social media privacy protection and identifies critical areas for reform.

2. Literature Review

2.1 Legal Frameworks Governing Social Media Privacy

The United States lacks a comprehensive federal data protection law comparable to the GDPR, instead relying on a complex web of federal and state regulations that address specific aspects of privacy protection (Hoofnagle et al., 2019). The primary federal laws relevant to social media privacy include the Children's Online Privacy Protection Act (COPPA) of 1998, which requires parental consent for the collection of personal information from children under 13, and Section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive practices" in commerce.

The California Consumer Privacy Act (CCPA), which took effect in 2020, represents the most significant state-level privacy legislation in the United States. The CCPA grants California residents specific rights regarding their personal information, including the right to know what personal information is collected, the right to delete personal information, and the right to opt-out of the sale of personal information (Goldman, 2020). The subsequent California Privacy Rights Act (CPRA), approved by voters in November 2020, further strengthened these protections by establishing the California Privacy Protection Agency and expanding the definition of sensitive personal information.

Other states have followed California's lead, with Virginia enacting the Consumer Data Protection Act (CDPA) in 2021 and Colorado passing the Colorado Privacy Act (CPA) in the same year. However, these state-level initiatives create a complex compliance environment for social media platforms, which must navigate varying requirements across different jurisdictions while continuing to operate as national and international services.

2.2 Ethical Frameworks for Digital Privacy

The ethical implications of social media data practices have been extensively analyzed through various philosophical lenses. Utilitarian approaches, which focus on maximizing overall welfare, might justify extensive data collection if it leads to improved services, more relevant advertising, or enhanced public safety (Mill, 1863; Singer, 1972). However, critics argue that the benefits of data collection primarily accrue to platform owners and advertisers rather than users, creating an asymmetrical distribution of benefits and harms (Cohen, 2019).

Deontological ethics, grounded in the work of Immanuel Kant, emphasizes the inherent rights and dignity of individuals, suggesting that certain privacy protections are categorical imperatives regardless of their consequences

(Kant, 1785). This perspective has been particularly influential in the development of consent-based privacy frameworks, which require meaningful user agreement before personal data can be collected or processed.

Rights-based approaches to digital privacy build upon the concept of informational self-determination, first articulated by the German Constitutional Court in 1983. This framework posits that individuals have a fundamental right to control the collection, use, and dissemination of their personal information (Rouvroy & Poullet, 2009). The principle has been influential in European privacy law and increasingly shapes discussions of privacy rights in the United States.

Contemporary digital ethics scholarship has also focused on the concept of "surveillance capitalism," a term coined by Shoshana Zuboff to describe the extraction of human experience as raw material for predictive products that are traded in behavioral futures markets (Zuboff, 2019). This framework highlights the power asymmetries inherent in current social media business models and raises fundamental questions about consent, agency, and human autonomy in digital environments.

2.3 Platform Policies and Privacy Scandals

The period from 2018 to 2023 has been marked by numerous high-profile privacy scandals that have shaped public understanding and regulatory responses to social media privacy concerns. The Cambridge Analytica scandal, which came to light in early 2018, revealed that the personal information of up to 87 million Facebook users had been harvested without explicit consent and used for political advertising purposes (Cadwalladr & Graham-Harrison, 2018). The incident led to congressional hearings, regulatory investigations, and a \$5 billion fine from the Federal Trade Commission.

TikTok, the Chinese-owned short-form video platform, has faced particular scrutiny regarding its data practices and potential national security implications. Congressional hearings in 2021 and 2022 raised concerns about the platform's data flows to China, its content moderation algorithms, and its impact on young users (Senate Committee on Commerce, Science, and Transportation, 2021). These concerns have led to various legislative proposals aimed at restricting or banning TikTok in the United States.

Meta (formerly Facebook) has continued to face privacy-related challenges beyond Cambridge Analytica, including issues related to facial recognition technology, location tracking, and the handling of sensitive health information. In 2021, the company agreed to pay \$650 million to settle a class-action lawsuit related to its use of facial recognition technology in violation of Illinois's Biometric Information Privacy Act (*In re Facebook Biometric Information Privacy Litigation*, 2021).

3. Methodology

This study employs a qualitative research approach combining legal analysis, policy evaluation, and ethical assessment to examine the intersection of law and ethics in social media privacy practices. The methodology is designed to provide a comprehensive understanding of how legal frameworks interact with ethical considerations in the rapidly evolving landscape of social media regulation.

3.1 Data Collection

Primary sources for this analysis include federal and state legislation, regulatory agency reports, court decisions, congressional hearing transcripts, and platform privacy policies. Secondary sources encompass academic literature, industry reports, and journalistic investigations published between 2018 and 2023. Specific attention was paid to materials from the Federal Trade Commission, state attorneys general offices, and major social media platforms' transparency reports.

The research focused on five major social media platforms: Facebook/Meta, Instagram, Twitter, TikTok, and YouTube. These platforms were selected based on their user base size, data collection practices, and regulatory attention during the study period.

3.2 Analytical Framework

To systematically evaluate platform practices, this study develops a four-quadrant legal-ethical matrix that categorizes actions based on their legal compliance and ethical alignment:

Table 1: Legal-Ethical Assessment Framework

Category	Legal Status	Ethical Status	Examples
A	Legal	Ethical	Transparent data collection with meaningful consent
B	Legal	Unethical	Dark patterns in privacy settings, excessive data collection
C	Illegal	Ethical	Whistleblower disclosures of harmful practices
D	Illegal	Unethical	Unauthorized data sharing, deceptive privacy policies

This framework allows for nuanced analysis of platform practices that may comply with existing legal requirements while still raising significant ethical concerns, or conversely, practices that violate current law but serve broader ethical principles.

3.3 Data Analysis

The analysis process involved systematic coding of regulatory actions, platform policy changes, and legal developments according to the legal-ethical framework. Each significant privacy-related incident or policy was categorized and analyzed for its implications regarding the broader research questions. Particular attention was paid to identifying patterns in regulatory responses, platform adaptations, and evolving public discourse around privacy rights.

4. Findings and Analysis

4.1 The Fragmented U.S. Privacy Landscape

The analysis reveals a highly fragmented regulatory environment that creates significant challenges for both privacy protection and platform compliance. Unlike the comprehensive approach taken by the GDPR, the United States continues to rely on sector-specific laws and state-level initiatives that often conflict or leave gaps in protection.

Table 2: Major U.S. Privacy Laws Applicable to Social Media Platforms

Law	Year Enacted	Scope	Key Provisions	Enforcement
COPPA	1998	Children under 13	Parental consent required	FTC
CCPA/CPRA	2020/2023	California residents	Right to know, delete, opt-out	CPPA
BIPA (Illinois)	2008	Biometric data	Consent for biometric collection	Private right of action
VCDPA	2023	Virginia residents	Consumer rights, data minimization	Attorney General
CPA (Colorado)	2023	Colorado residents	Consumer rights, data protection assessments	Attorney General

This fragmentation creates several problems. First, it leads to inconsistent protection levels across different states and demographics. Second, it increases compliance costs for platforms, which must navigate multiple regulatory frameworks simultaneously. Third, it creates opportunities for forum shopping, where platforms may structure their operations to take advantage of more permissive jurisdictions.

4.2 Legal Compliance vs. Ethical Conduct

A critical finding of this research is that legal compliance does not necessarily equate to ethical conduct. Many platform practices that comply with existing U.S. law still raise significant ethical concerns when evaluated against principles of transparency, consent, and user autonomy.

Case Study: Dark Patterns in Privacy Settings

Analysis of major platform privacy interfaces reveals widespread use of "dark patterns" – user interface designs that manipulate users into making decisions that benefit the platform rather than the user (Mathur et al., 2019). These practices typically involve:

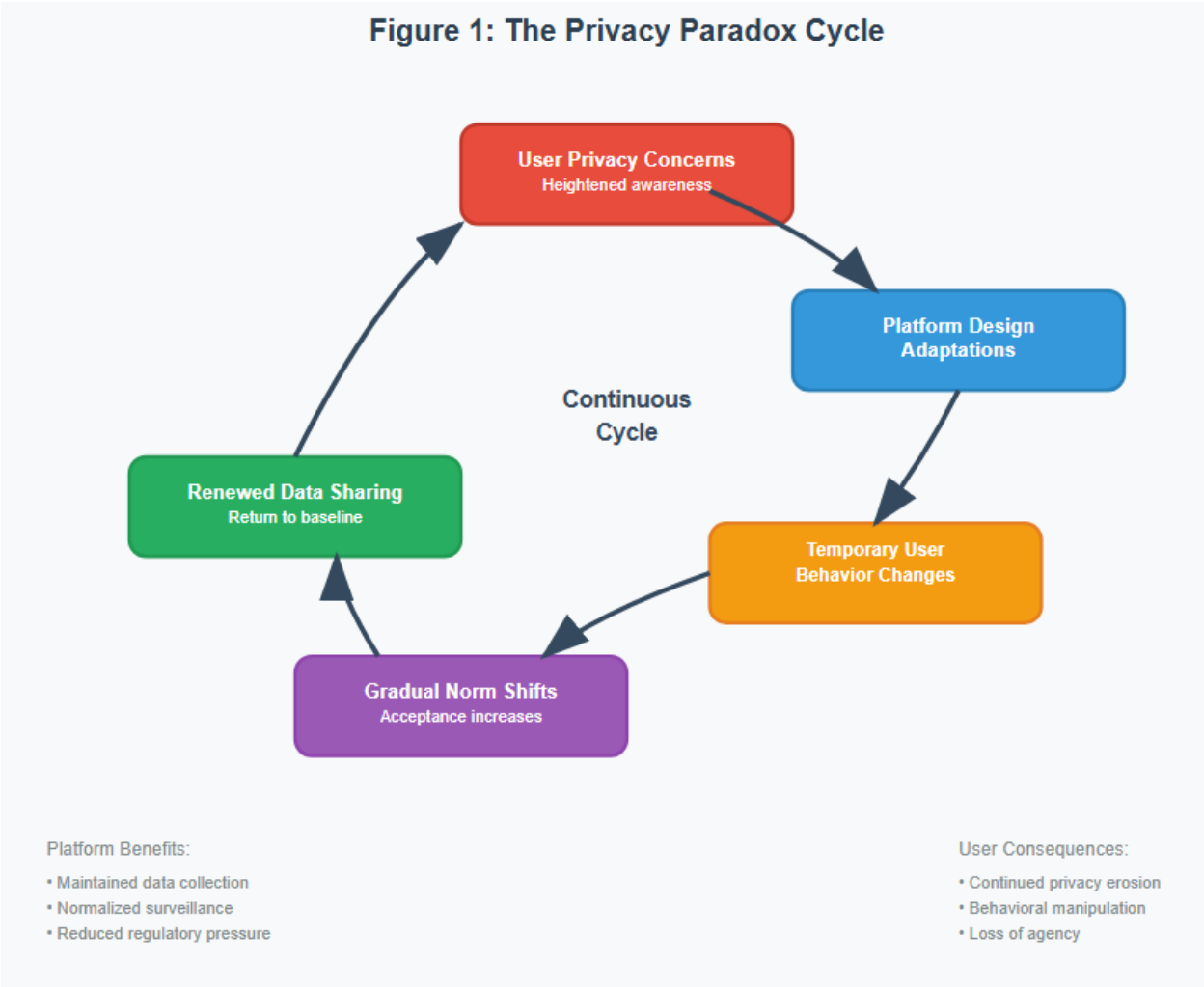
- Making privacy-protective options difficult to find or access
- Using confusing language to obscure the implications of privacy choices
- Pre-selecting options that favor data collection
- Making opt-out processes more complex than opt-in processes

While these practices may not violate existing U.S. law, they clearly conflict with ethical principles of informed consent and user autonomy. The FTC has begun to address some dark patterns through enforcement actions, but comprehensive regulation remains lacking.

4.3 The Privacy Paradox in Practice

The research confirms the existence of a significant "privacy paradox" in social media use, where users express concern about privacy while simultaneously engaging in behaviors that compromise their privacy (Norberg et al., 2007). Platform operators have learned to exploit this paradox through various mechanisms:

Figure 1: The Privacy Paradox Cycle



This cycle demonstrates how platforms can maintain data collection practices even in the face of user privacy concerns by making incremental changes that gradually shift social norms around privacy expectations.

4.4 Algorithmic Manipulation and Ethical Responsibility

A particularly concerning finding relates to the use of algorithmic systems to influence user behavior in ways that may compromise user welfare. Analysis of platform recommendation algorithms reveals systematic biases toward content that generates strong emotional responses, particularly anger and outrage, which tend to increase user engagement but may have negative social consequences (Vaidhyanathan, 2018).

Table 3: Documented Algorithmic Biases in Social Media Platforms

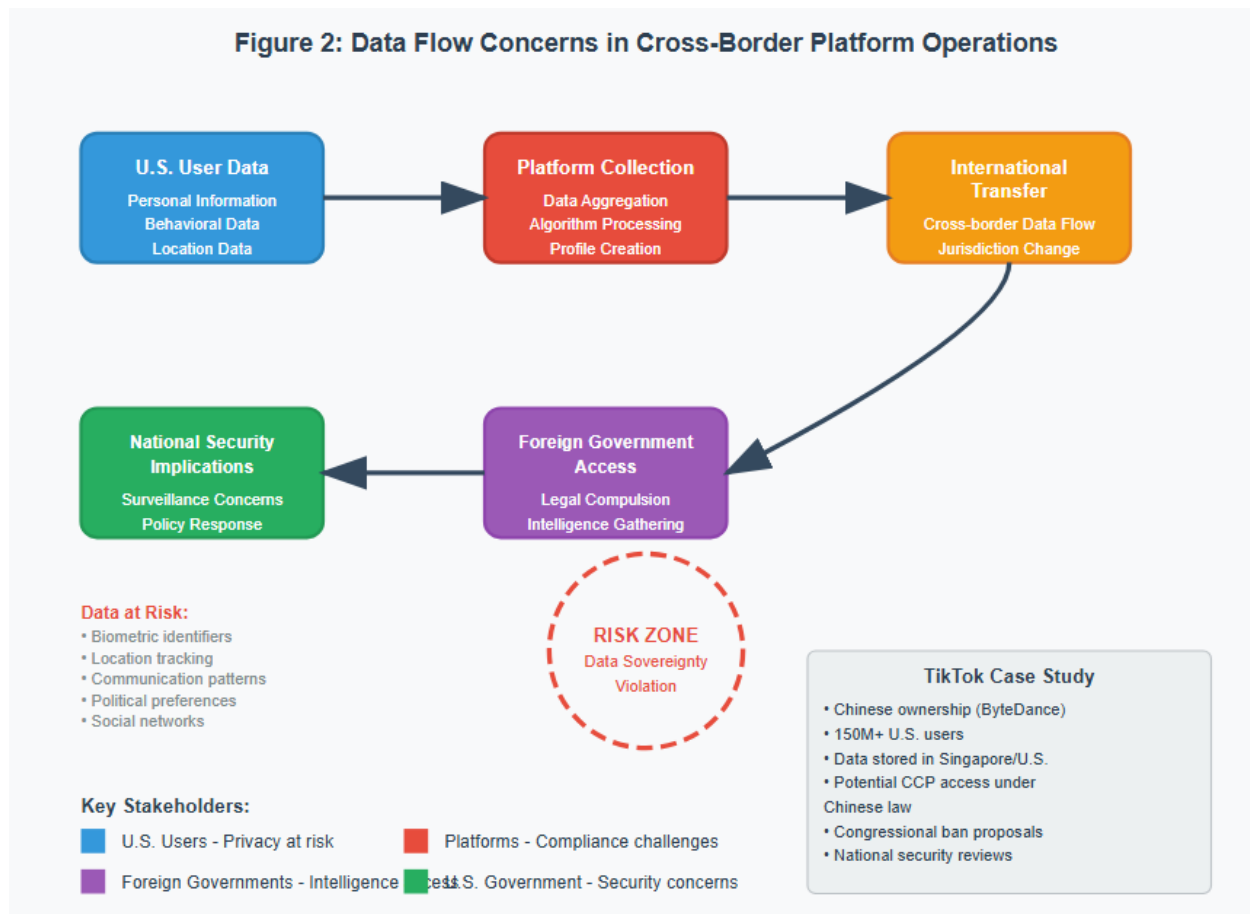
Platform	Identified Bias	Impact	Regulatory Response
Facebook	Emotional manipulation	Increased polarization	FTC investigation
YouTube	Extremist content promotion	Radicalization pathways	Content policy changes
TikTok	Addictive design patterns	Youth mental health impacts	Congressional hearings
Twitter	Harassment amplification	Silencing of marginalized voices	Policy reforms
Instagram	Body image manipulation	Eating disorders in teens	Internal research disclosure

These algorithmic practices raise fundamental questions about platform responsibility for user welfare and the adequacy of current regulatory frameworks to address sophisticated forms of behavioral manipulation.

4.5 Cross-Border Data Flows and National Security

The analysis reveals growing tension between privacy protection and national security concerns, particularly regarding platforms owned by foreign entities. The TikTok controversy exemplifies this tension, with concerns about Chinese government access to U.S. user data leading to various legislative proposals for restrictions or bans.

Figure 2: Data Flow Concerns in Cross-Border Platform Operations



National Security Implications

This issue highlights the limitations of privacy laws that focus primarily on corporate data use while giving insufficient attention to government surveillance and access.

5. Discussion

5.1 The Inadequacy of Self-Regulation

The research demonstrates that industry self-regulation has proven insufficient to protect user privacy in the social media context. Despite repeated privacy scandals and public pressure, major platforms continue to engage in practices that prioritize data collection and user engagement over privacy protection. The voluntary nature of industry initiatives, such as the Partnership for Responsible and Inclusive Media, limits their effectiveness in creating meaningful change.

Several factors contribute to the failure of self-regulation:

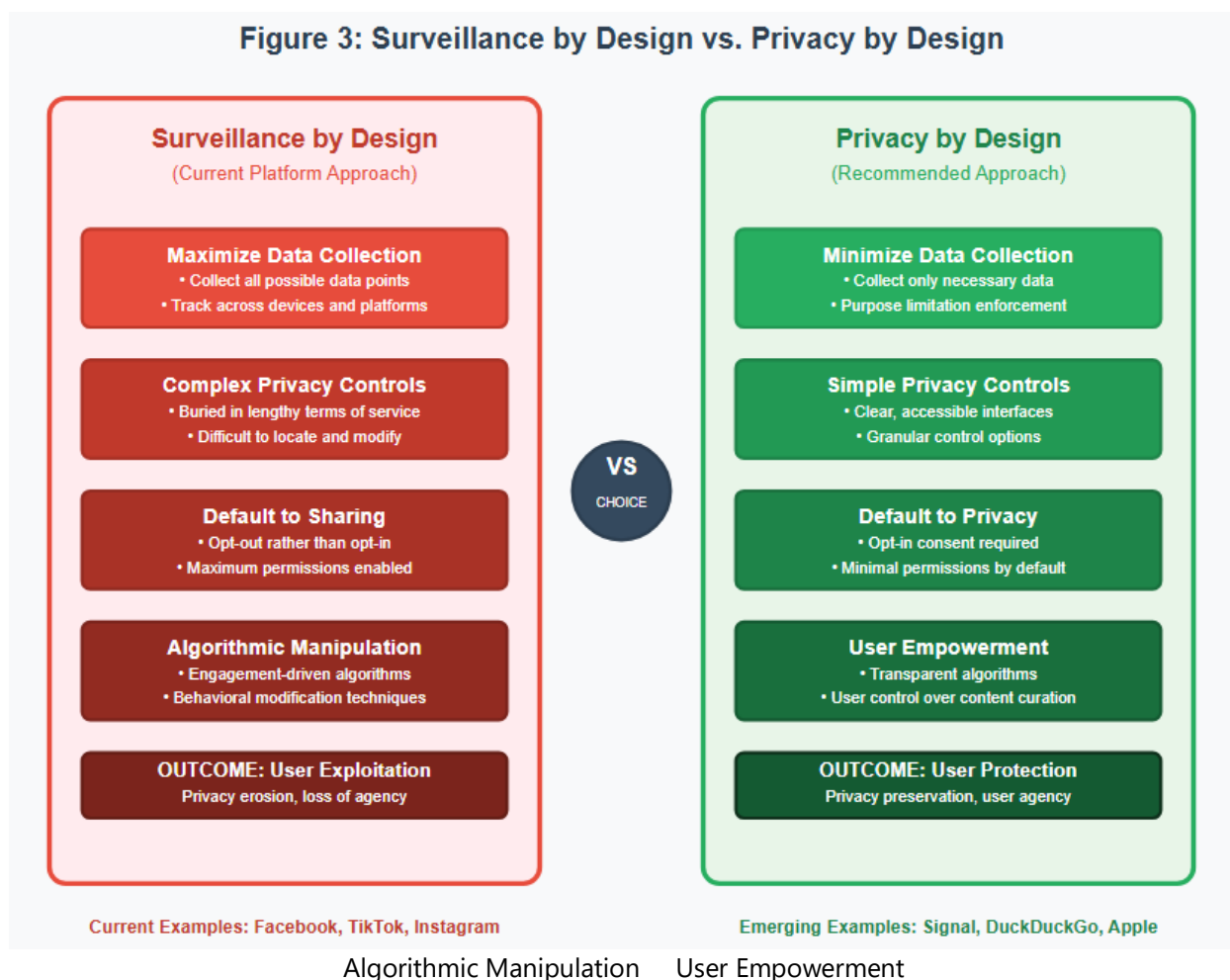
1. **Misaligned Incentives:** Platform business models fundamentally depend on data collection and behavioral targeting, creating inherent conflicts with privacy protection.
2. **Competitive Pressure:** Platforms that implement stronger privacy protections may be disadvantaged relative to competitors that continue aggressive data collection practices.
3. **Technical Complexity:** Many privacy issues arise from complex algorithmic systems that are difficult for both users and regulators to understand and evaluate.
4. **Global Operations:** Platforms operate across multiple jurisdictions with varying privacy expectations, making consistent privacy protection challenging.

5.2 The Role of Technological Design in Privacy Protection

Analysis of platform interfaces and data collection practices reveals that technological design choices play a crucial role in determining privacy outcomes. The concept of "privacy by design," originally articulated by Ann Cavoukian, suggests that privacy protections should be embedded in system architecture from the outset rather than added as an afterthought (Cavoukian, 2009).

However, the research shows that most major social media platforms have adopted the opposite approach, implementing what might be termed "surveillance by design." Platform architectures are optimized for maximum data collection and user engagement, with privacy protections implemented only when required by law or public pressure.

Figure 3: Surveillance by Design vs. Privacy by Design



5.3 The Digital Divide and Privacy Protection

An important finding relates to the differential impact of privacy violations on different demographic groups. The research reveals that privacy harms disproportionately affect vulnerable populations, including children, elderly users, and individuals from lower socioeconomic backgrounds who may have less digital literacy and fewer resources to protect themselves.

This "privacy divide" is exacerbated by several factors:

- **Digital Literacy Gaps:** Users with lower digital literacy are more likely to accept default privacy settings and less likely to understand the implications of data sharing.
- **Economic Constraints:** Low-income users may be more willing to trade privacy for access to free services.
- **Language Barriers:** Privacy policies and settings are often available only in English, limiting understanding among non-native speakers.
- **Device Limitations:** Users with older devices may not have access to the latest privacy features and protections.

5.4 International Comparisons and Regulatory Models

Comparison with international privacy frameworks, particularly the GDPR, reveals significant gaps in U.S. privacy protection. The GDPR's comprehensive approach, which includes principles such as data minimization, purpose limitation, and accountability, contrasts sharply with the U.S. system's reliance on notice and consent.

Table 4: Comparison of Privacy Frameworks

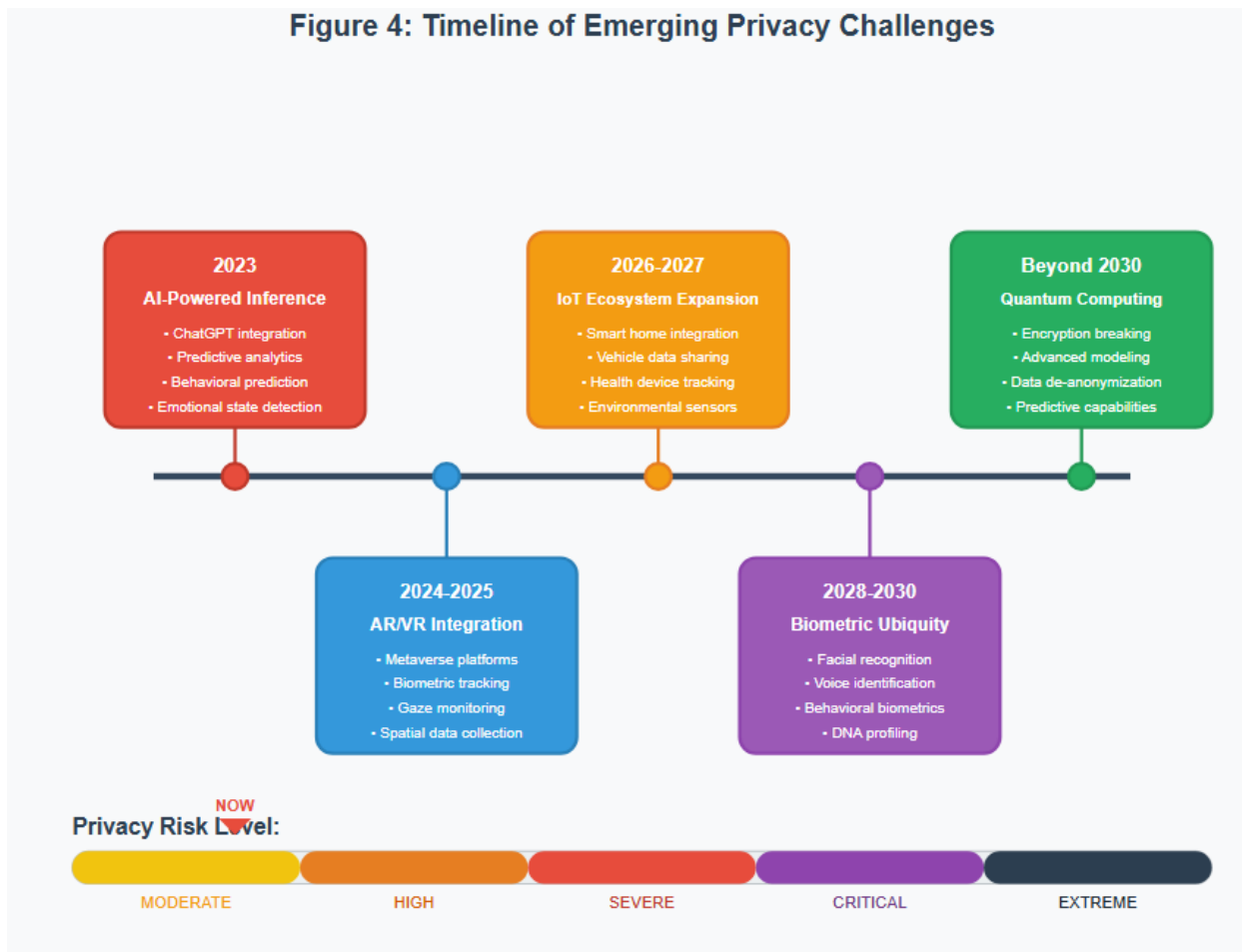
Principle	GDPR	CCPA	Proposed Federal Law
Data Minimization	Required	Limited	Proposed
Purpose Limitation	Strict	Moderate	Unclear
Consent Requirements	Explicit	Opt-out	Varies
Individual Rights	Comprehensive	Limited	Proposed
Enforcement Mechanisms	Strong	Moderate	Unclear
Penalties	Up to 4% of revenue	Limited monetary	Proposed

5.5 Emerging Technologies and Future Challenges

The research identifies several emerging technologies that will create new challenges for privacy protection in social media contexts:

1. **Artificial Intelligence and Machine Learning:** Advanced AI systems can infer sensitive information from seemingly innocuous data, making traditional consent models inadequate.
2. **Augmented and Virtual Reality:** Immersive technologies collect unprecedented amounts of biometric and behavioral data, raising new categories of privacy concerns.
3. **Internet of Things Integration:** The connection of social media platforms to IoT devices creates new vectors for data collection and privacy violations.
4. **Biometric Recognition:** Facial recognition, voice analysis, and other biometric technologies enable new forms of identification and tracking.

Figure 4: Timeline of Emerging Privacy Challenges



6. Recommendations

Based on the findings and analysis presented above, this study proposes a comprehensive set of recommendations for improving privacy protection in the social media context. These recommendations address legal, technological, and educational dimensions of the privacy challenge.

6.1 Legislative and Regulatory Reforms

Comprehensive Federal Privacy Legislation

The United States urgently needs comprehensive federal privacy legislation that establishes uniform standards for data collection, use, and sharing across all sectors and jurisdictions. Such legislation should include:

- **Universal Application:** Coverage of all organizations that collect personal data, regardless of size or sector
- **Strong Individual Rights:** Including rights to access, deletion, portability, and correction
- **Data Minimization Requirements:** Limiting collection to what is necessary for specified purposes
- **Algorithmic Transparency:** Requiring disclosure of automated decision-making systems
- **Meaningful Consent:** Establishing standards for valid consent that go beyond current notice-and-choice models
- **Robust Enforcement:** Including both regulatory enforcement and private rights of action

Enhanced FTC Authority

Congress should expand the Federal Trade Commission's authority to address privacy violations by:

- Providing explicit rulemaking authority for privacy and data security
- Increasing civil penalty amounts to ensure meaningful deterrence
- Establishing specialized privacy enforcement units with technical expertise
- Creating fast-track procedures for addressing emerging privacy threats

Algorithmic Accountability Requirements

New regulations should require social media platforms to:

- Conduct algorithmic impact assessments for systems that affect user welfare
- Provide meaningful transparency about recommendation algorithms
- Allow users to opt out of algorithmic content curation
- Submit to regular audits of algorithmic systems by independent third parties

6.2 Technological Design Requirements

Privacy by Design Mandates

Legislation should mandate privacy-by-design principles in social media platform development:

- **Default Privacy Settings:** Requiring the most privacy-protective settings as defaults
- **Data Minimization:** Limiting collection to what is necessary for service provision
- **Purpose Limitation:** Preventing use of data for purposes not disclosed at collection
- **User Control:** Providing granular, accessible privacy controls

Interoperability and Data Portability

To reduce platform lock-in and increase user choice, regulations should require:

- Standardized data export formats that enable easy platform switching
- Interoperability standards that allow communication across platforms
- Prohibition of practices that artificially increase switching costs

6.3 Educational and Empowerment Initiatives

Digital Literacy Programs

Public and private stakeholders should collaborate to develop comprehensive digital literacy programs that:

- Teach users to understand privacy policies and settings
- Provide skills for evaluating privacy risks and benefits
- Educate about the long-term consequences of data sharing
- Focus particularly on vulnerable populations including children and elderly users

Privacy Tools and Technologies

Support should be provided for the development and deployment of privacy-enhancing technologies:

- User-friendly privacy management tools
- Automated privacy preference systems
- Privacy-preserving advertising technologies
- Decentralized social media platforms

6.4 Platform Accountability Measures

Regular Privacy Audits

Social media platforms should be required to undergo regular, independent privacy audits that:

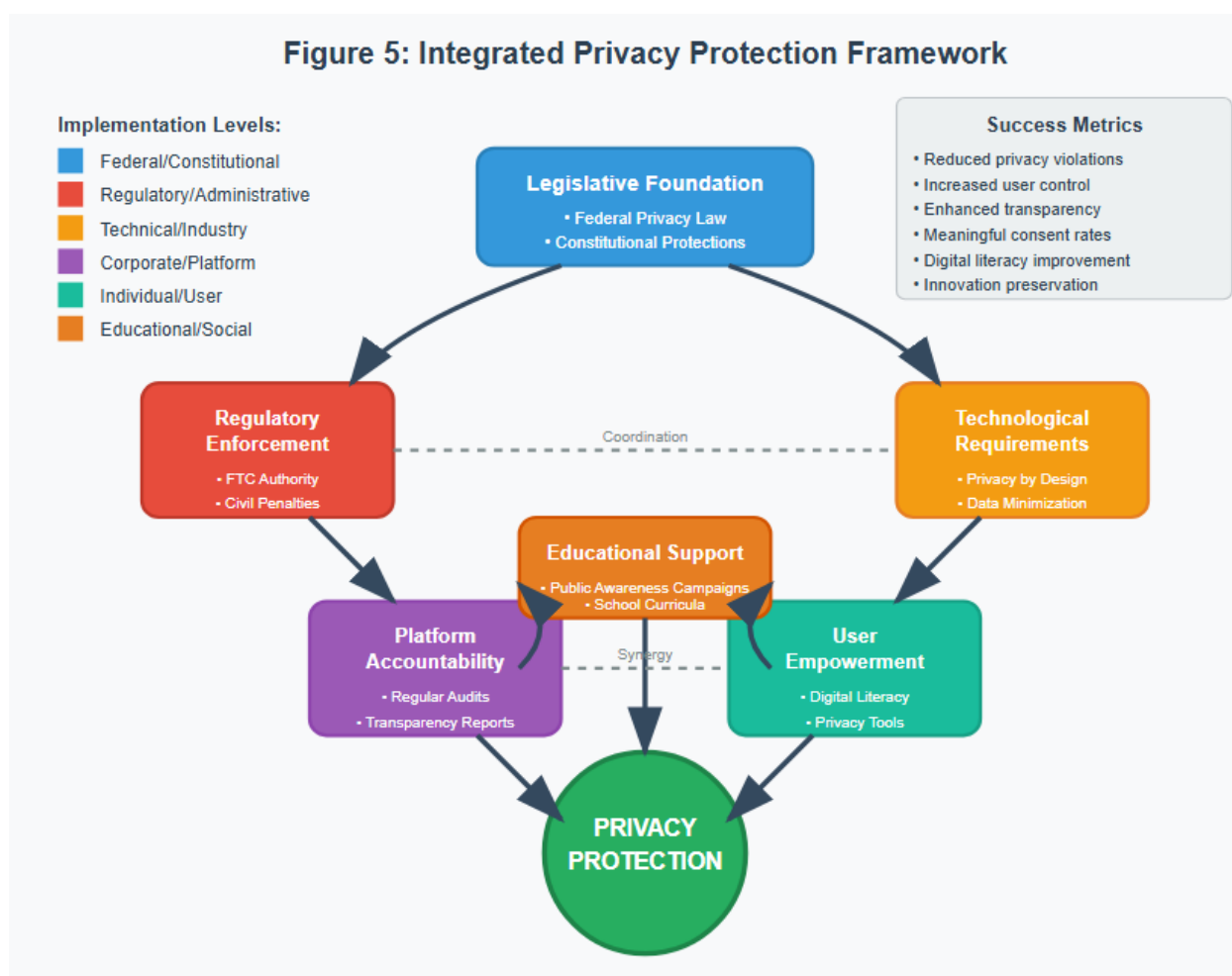
- Assess compliance with privacy laws and policies
- Evaluate the effectiveness of privacy protections
- Identify areas for improvement
- Report results publicly

Transparency Reporting

Enhanced transparency requirements should include:

- Detailed reporting on data collection and use practices
- Government data request statistics
- Content moderation and algorithmic decision-making statistics
- Privacy breach notifications and response measures

Figure 5: Integrated Privacy Protection Framework



7. Conclusion

This comprehensive analysis of social media privacy in the United States reveals a deeply fragmented and ethically fraught landscape. Despite platforms largely adhering to existing legal requirements, these laws are often outdated and ill-suited to address the evolving technological ecosystem. The current regulatory framework is insufficient to counteract the sophisticated data collection, behavioral manipulation, and algorithmic targeting that now define major social media operations.

Key findings demonstrate that most platform practices fall within the "legal but unethical" quadrant of the legal-ethical framework developed in this study. Platforms exploit legal loopholes and deploy interface designs that prioritize engagement over user wellbeing. The weaponization of the privacy paradox where users express concern about privacy yet behave in ways that compromise it enables these platforms to continue intrusive data collection under the guise of consent.

Moreover, the lack of a comprehensive federal privacy law in the U.S., coupled with state-by-state inconsistencies, exacerbates vulnerabilities. This patchwork approach disproportionately affects marginalized users and creates regulatory confusion that benefits large tech corporations at the expense of competition and accountability.

Concerns around algorithmic manipulation, emotional exploitation, and cross-border data flows also raise critical issues beyond individual privacy touching on national security, democratic stability, and societal trust. Yet, amidst these challenges, there is a window of opportunity. Rising awareness among users, policymakers, and industry actors has laid the groundwork for reform. Frameworks like the GDPR and state-level initiatives like the CCPA provide viable templates for progress.

The challenge now is to seize this momentum and implement comprehensive reforms that are legal, technical, and ethical in nature. Protecting privacy in the age of social media is not just a matter of individual rights it is a collective imperative to preserve autonomy, dignity, and democracy in an increasingly digital society.

8. Recommendations

To address the multifaceted nature of social media privacy violations, this study proposes the following strategic recommendations:

1. **Federal Privacy Legislation:** Enact a unified, comprehensive federal privacy law akin to the GDPR. This legislation should mandate transparent data usage, meaningful consent, algorithmic accountability, and enforceable penalties for violations.
2. **Ethical Design Principles:** Encourage or mandate platforms to adopt "privacy by design" and "user autonomy" principles in the development of user interfaces and algorithmic systems. Dark patterns should be regulated and penalized.
3. **Data Minimization and Purpose Limitation:** Platforms should be required to collect only the data necessary for specific, clearly stated purposes, with limitations on reuse and resale.
4. **Algorithmic Transparency and Audits:** Independent audits of algorithmic recommendation systems should be implemented to ensure they are not promoting harmful or manipulative content. Users should be allowed to opt out of algorithmic feeds.
5. **Cross-Border Data Protection:** Strengthen international data transfer agreements and impose strict regulations on data shared with foreign entities, especially those tied to national security risks.
6. **Public Education Campaigns:** Launch ongoing public awareness campaigns to educate users on digital privacy risks and their rights, with specific outreach to vulnerable populations.
7. **Support for Privacy-Enhancing Technologies (PETs):** Promote the development and adoption of decentralized identity frameworks, zero-knowledge proofs, and other PETs that give users greater control over their data.
8. **Multi-Stakeholder Collaboration:** Encourage cooperation between governments, industry leaders, civil society organizations, and academia to create dynamic, adaptable privacy standards.

Only coordinated efforts that blend legal, technological, and ethical reforms can adequately protect user privacy in a rapidly evolving digital ecosystem.

9. Limitations of the Research

While this study offers a robust legal-ethical analysis of social media privacy in the U.S., several limitations should be acknowledged:

1. **Scope of Jurisdiction:** The focus is primarily on U.S.-based legal frameworks and platforms. Although some comparisons are drawn with international standards (e.g., GDPR), deeper cross-jurisdictional analysis would provide broader insights.
2. **Rapid Technological Change:** Social media technologies, algorithms, and privacy threats evolve rapidly. The findings may become outdated unless updated continuously alongside technological developments.
3. **Lack of Empirical User Data:** The study relies heavily on secondary data, theoretical frameworks, and policy analysis. Direct empirical data (e.g., surveys, user interviews, or behavioral data) would enhance the granularity of insights.
4. **Platform-Specific Analysis:** While general practices are analyzed, the study does not exhaustively examine each major platform individually. Future research could benefit from platform-specific case studies (e.g., Facebook, TikTok, X).
5. **Limited Coverage of Emerging Tech:** Although briefly mentioned, deeper investigation into how new technologies like AI, VR/AR, and IoT intersect with social media privacy was beyond this study's scope and should be pursued further.
6. **Regulatory Outcomes Uncertainty:** Many proposed reforms (e.g., federal privacy legislation) are speculative or aspirational at this stage. The feasibility and political viability of these measures require further policy-oriented research.

References

- [1] Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
- [2] California Consumer Privacy Act. (2018). Cal. Civ. Code § 1798.100 et seq. <https://oag.ca.gov/privacy/ccpa>
- [3] Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. *Information and Privacy Commissioner of Ontario*. <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>
- [4] Cohen, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism*. Oxford University Press.
- [5] Federal Trade Commission. (2023). *Privacy and data security update: 2022*. <https://www.ftc.gov/reports/privacy-data-security-update-2022>
- [6] Goldman, E. (2020). An introduction to the California Consumer Privacy Act (CCPA). *Santa Clara Law Digital Commons*, 20(1), 1-38.
- [7] Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. *Information & Communications Technology Law*, 28(1), 65-98.
- [8] *In re Facebook Biometric Information Privacy Litigation*, No. 15-cv-03747-JD (N.D. Cal. 2021).
- [9] Kant, I. (1785). *Groundwork for the metaphysics of morals*. Translated by M. Gregor (2017). Cambridge University Press.
- [10] Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 1-32.
- [11] Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), 100-126.
- [12] Rouvroy, A., & Poullet, Y. (2009). The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy. In S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, & S. Nouwt (Eds.), *Reinventing data protection?* (pp. 45-76). Springer.
- [13] Senate Committee on Commerce, Science, and Transportation. (2021, October 28). *Protecting kids online: Testimony from a Facebook whistleblower*. <https://www.commerce.senate.gov/2021/10/protecting%20kids%20online:%20testimony%20from%20a%20facebook%20whistleblower>
- [14] Solove, D. J. (2021). *Understanding privacy*. Harvard University Press.
- [15] Srnicek, N. (2017). *Platform capitalism*. Polity Press.
- [16] Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *Colorado Technology Law Journal*, 13(2), 203-218.
- [17] Vaidhyanathan, S. (2018). *Antisocial media: How Facebook disconnects us and undermines democracy*. Oxford University Press.
- [18] Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.