

**Navigating Instagram's compliance with transparency requirements in the  
European Union and Canadian data protection law**

**Amireh Aligholi**

**Faculty of Law**

**McGill University, Montreal**

**January 2025**

**A thesis submitted to McGill University in partial fulfillment of the  
requirements of the degree of Master of Laws**

**©Amireh Aligholi 2025**

## Table of Contents

<b>ABSTRACT.....</b>	<b>3</b>
<b>RÉSUMÉ.....</b>	<b>4</b>
<b>ACKNOWLEDGMENT .....</b>	<b>5</b>
<b>LIST OF ABBREVIATION .....</b>	<b>6</b>
<b>CHAPTER 1: INTRODUCTION .....</b>	<b>7</b>
<b>1.1 BACKGROUND .....</b>	<b>7</b>
1.1.1 CHALLENGES WITH AUTOMATED DECISION-MAKING AND THE NEED FOR TRANSPARENCY: .....	9
<b>1.2 RESEARCH CONTEXT.....</b>	<b>10</b>
1.2.1 OVERVIEW OF GDPR AND TRANSPARENCY REQUIREMENTS.....	10
1.2.2 AN OVERVIEW OF CANADA’S PRIVACY ACT AND AI ACT .....	11
1.2.3 ETHICAL IMPLICATIONS OF DATA TRANSPARENCY .....	12
<b>1.3 THESIS OBJECTIVES .....</b>	<b>12</b>
1.3.1 EVALUATING COMPLIANCE.....	13
1.3.2 IDENTIFYING GAPS IN TRANSPARENCY .....	14
<b>1.4 CONCLUSION.....</b>	<b>15</b>
<b>CHAPTER 2: PROBLEM STATEMENT AND PRIVACY CONCERNS IN SOCIAL MEDIA .....</b>	<b>16</b>
<b>2.1 PRIVACY ISSUES IN SOCIAL MEDIA PLATFORMS .....</b>	<b>16</b>
<b>2.2 INSTAGRAM’S USE OF PRIVATE INFORMATION .....</b>	<b>21</b>
2.2.1 DATA COLLECTION, ALGORITHMS, AND PERSONALIZED ADS .....	21
2.2.2 CONTENT RECOMMENDATIONS AND USER INTERACTION.....	22
<b>2.3 TRANSPARENCY CHALLENGES .....</b>	<b>25</b>
2.3.1 USER CONSENT AND AWARENESS .....	26
2.3.2 TRANSPARENCY REPORTS AND COMMUNICATION.....	27

<b>2.4 ETHICAL IMPLICATIONS OF DATA USE IN SOCIAL MEDIA .....</b>	<b>29</b>
<b>2.5 CONCLUSION.....</b>	<b>32</b>
<b><u>CHAPTER 3: CASE STUDY OF INSTAGRAM AND REGULATORY COMPLIANCE.....</u></b>	<b><u>33</u></b>
<b>3.1 INSTAGRAM’S EFFORTS TOWARD TRANSPARENCY.....</b>	<b>33</b>
3.1.1 PRIVACY POLICY, TERMS OF SERVICE, AND USER CONSENT .....	37
<b>3.2 EVALUATION OF INSTAGRAM’S COMPLIANCE WITH GDPR AND CANADIAN PRIVACY LAWS.....</b>	<b>39</b>
3.2.1 TRANSPARENCY CHALLENGES UNDER GDPR REQUIREMENTS.....	43
3.2.2 APPLICABILITY OF CANADA’S PRIVACY ACT AND AI ACT TO INSTAGRAM.....	45
<b>3.3 ANALYSIS OF USER AWARENESS AND UNDERSTANDING OF DATA USE .....</b>	<b>48</b>
<b>3.4 CONCLUSION:.....</b>	<b>51</b>
<b><u>CHAPTER 4: COMPARATIVE ANALYSIS OF SOCIAL MEDIA PLATFORMS .....</u></b>	<b><u>52</u></b>
<b>4.1 COMMON TRANSPARENCY AND COMPLIANCE ISSUES ACROSS PLATFORMS.....</b>	<b>53</b>
4.1.1 FACEBOOK: TRANSPARENCY AND COMPLIANCE PRACTICES.....	56
4.1.2 TIKTOK: HANDLING USER DATA AND TRANSPARENCY CHALLENGES.....	58
4.1.3 YOUTUBE: DATA USE AND AD TARGETING.....	61
<b>4.2 COMPARATIVE FINDINGS AND INSIGHTS.....</b>	<b>63</b>
<b>4.3 CONCLUSION.....</b>	<b>67</b>
<b><u>CHAPTER 5: CONCLUSION.....</u></b>	<b><u>69</u></b>
<b>5.1 SUMMARY OF FINDINGS.....</b>	<b>69</b>
<b>5.2 BROADER CONTRIBUTIONS.....</b>	<b>70</b>
<b>5.3 IMPLICATIONS FOR POLICY AND PRACTICE.....</b>	<b>72</b>
<b>5.4 LIMITATIONS AND OPPORTUNITIES FOR FUTURE RESEARCH.....</b>	<b>73</b>
<b>5.5 VISION FOR THE FUTURE .....</b>	<b>75</b>
<b>5.6 FINAL REFLECTIONS.....</b>	<b>77</b>
<b><u>BIBLIOGRAPHY .....</u></b>	<b><u>80</u></b>

## Abstract

This thesis investigates social media platform compliance with transparency requirements under the European Union's General Data Protection Regulation (GDPR) and Canada's Privacy and AI Act. It explores the challenges posed by automated decision-making and data-driven algorithms, particularly regarding user privacy, consent, and transparency obligations. Using Instagram as a case study, the research evaluates its privacy policies, consent mechanisms, and data collection practices. The analysis highlights gaps in Instagram's approach to transparency, focusing on algorithmic profiling, personalized advertising, and content recommendations. It expands the analysis to other social media platforms, including Facebook, TikTok, and YouTube, underscoring broader compliance issues in the industry. The thesis proposes recommendations to strengthen transparency through clearer privacy policies, improved consent mechanisms, and enhanced enforcement of legal standards. It also advocates for adopting user-centric approaches, including simplified language and privacy dashboards, to empower individuals to make informed decisions about their data. These findings contribute to the broader discourse on data governance and ethical AI use, offering insights for regulators, policymakers, and platform developers to promote privacy accountability in the digital age.

## Résumé

Cette thèse examine la conformité d'Instagram aux exigences de transparence imposées par le Règlement général sur la protection des données (RGPD) de l'Union européenne et par la Loi canadienne sur la protection de la vie privée et l'intelligence artificielle. Elle analyse les défis posés par la prise de décision automatisée et les algorithmes basés sur les données, en particulier en ce qui concerne la protection de la vie privée, le consentement et les obligations de transparence. En utilisant Instagram comme étude de cas, la recherche évalue ses politiques de confidentialité, ses mécanismes de consentement et ses pratiques de collecte de données. L'analyse révèle des lacunes dans l'approche de transparence d'Instagram, en se concentrant sur le profilage algorithmique, la publicité personnalisée et les recommandations de contenu. Une analyse comparative avec d'autres plateformes de médias sociaux, telles que Facebook, TikTok et YouTube, met en évidence des problèmes de conformité plus larges dans l'industrie. La thèse propose des recommandations pour renforcer la transparence grâce à des politiques de confidentialité plus claires, des mécanismes de consentement améliorés et une application renforcée des normes juridiques. Elle préconise également l'adoption d'approches centrées sur l'utilisateur, notamment un langage simplifié et des tableaux de bord de confidentialité, afin de permettre aux individus de prendre des décisions éclairées sur leurs données. Ces résultats contribuent au débat sur la gouvernance des données et l'utilisation éthique de l'intelligence artificielle, offrant des perspectives aux régulateurs, aux décideurs politiques et aux développeurs de plateformes pour promouvoir la responsabilité en matière de confidentialité à l'ère numérique.

## Acknowledgment

I want to express my deepest gratitude to my supervisor, Professor Richard Gold, for his invaluable guidance, support, and encouragement throughout the preparation of this thesis. Their insightful advice and constructive feedback have been instrumental in shaping my research and refining my arguments.

I am also grateful to the faculty members at McGill University's Faculty of Law, whose expertise and perspectives have enriched my academic journey. Special thanks to Professor Jenifer Raso for her thoughtful suggestions and for helping me navigate the complexities of data privacy law and regulatory frameworks in her course.

I extend my appreciation to the Graphos Thesis Writing team for their assistance in gathering materials and data and for their help with data analysis and research methods. Their contributions have been crucial in organizing and presenting the findings of this study.

I would also like to thank my fellow students and friends, particularly Shivani Salunke, for her unwavering support, insightful discussions, and encouragement during this process.

Finally, I am profoundly grateful to my husband, Behzad, for his unconditional love, patience, and support throughout my academic journey. His belief in me has been a constant source of inspiration.

While portions of this thesis benefited from helpful discussions and editorial suggestions, any errors or omissions remain my own.

## List Of Abbreviation

**AI** – Artificial Intelligence

**COPPA** – Children’s Online Privacy Protection Act

**EU** – European Union

**FTC** – Federal Trade Commission

**GDPR** – General Data Protection Regulation

**NOYB** – None of Your Business (Privacy Advocacy Group)

**PIPEDA** – Personal Information Protection and Electronic Documents Act

**ToS** – Terms of Service

# Chapter 1: Introduction

## 1.1 Background

Social media, such as Instagram, Facebook, TikTok, and X, are not only ubiquitous but are gathering and analyzing the personal data of their users to enhance their offerings and target advertising. These platforms use advanced algorithms to tailor content and ads, creating detailed user profiles based on the vast array of online user activity data. These practices improve user experiences but also highlight concerns over transparency and the ethical management of personal data. As these platforms grow further in reach and influence, the task of ensuring that users grasp how their data is gathered and utilized becomes increasingly important.

Existing privacy laws, such as the General Data Protection Regulation (GDPR)<sup>1</sup> and Canada's Privacy and AI Act<sup>2</sup>, aim to empower people by putting them in charge of their information through transparency and consent requirements. For instance, under GDPR rules, organizations must furnish details on how they handle data while also demanding that platforms reveal the rationale and outcomes of automated decision-making procedures.<sup>3</sup> Many social media platforms use data processing methods that lack transparency, despite regulations in place, to protect user privacy rights. This brings up the question of whether the current privacy laws align with the operations of these platforms. The main focus of my thesis revolves around determining if existing privacy regulations effectively address and regulate how social media platforms function. Analyzing the effectiveness of GDPR and Canada's privacy laws in managing the issues arising from media

---

<sup>1</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation), [2016] OJ L 119/1.

<sup>2</sup> Bill C-27, An Act to enact the Consumer Privacy Protection Act, *the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act*, 1st Sess, 44th Parl, 2022 (first reading 16 June 2022).

<sup>3</sup> Sandra Wachter, Brent Mittelstadt & Luciano Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation" (2017) 7:2 Intl Data Privacy L 76.



platforms using automated decision-making can provide insights into their alignment with advancements.

This study examines Instagram as a case study in to delve into this inquiry by assessing how one of the biggest social media networks tries to meet the transparency requirements of GDPR effectively and its significance in adhering to privacy laws, such as Canada's Privacy and AI Act through its utilization of personal data for tailored advertising and content customization purposes. The choice of Instagram as the central focus of this study is justified by the high levels of user engagement with the platform.<sup>4</sup> Instagram's status as one of the leading social media platforms, with 2 billion active users as of April 2024, positions it as a prime candidate for examination. The platform has a significant number of users from different demographics and regions, allowing me to examine data collection methods worldwide. Further, Instagram holds a prominent position in the realm of social media, especially concerning visual content and influencer marketing. Even though Facebook, the parent company of Instagram is the largest with over 3 billion active users, Instagram's high user engagement levels and emphasis on personalized algorithms and targeted ads make it a significant subject for research, on data transparency and privacy regulations.<sup>5</sup> The company's success depends on data processing and automated decision-making systems, which are precisely the domains subject to transparency regulations outlined in the GDPR and Canadian legislation. This highlights the importance of Instagram as a platform that reflects the challenges encountered by the social media sector as a whole. To explore Instagram's methods can offer perspectives that go beyond the platform itself.

---

<sup>4</sup> Guido Noto La Diega, "Against the Dehumanisation of Decision-Making: Algorithmic Decisions at the Crossroad of GDPR and AI Act" (2021) 9:2 Eur J L & Tech 1.

<sup>5</sup> Statista, "Most popular social networks worldwide as of July 2023, ranked by number of monthly active users" (2023), online: Statista <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>.

### 1.1.1 Challenges with Automated Decision-Making and the Need for Transparency:

Instagram and similar platforms face difficulty addressing privacy issues due to its growing reliance on automated decision-making systems driven by algorithms that analyze user data for content recommendations and targeted advertising strategies. Users frequently lack an understanding of the processes behind these decisions. The types of data involved and the potential impacts they could have, either privacy or in terms of user experience overall.

The GDPR deals with the topic of automated decision-making in Article 22 by granting individuals the right to avoid decisions made exclusively through automated means like profiling unless specific criteria are satisfied. Businesses are also obligated by Articles 13 and 14 to notify people about the presence of decision-making processes and provide explanations about their rationale while detailing the potential impact on individuals. Critics contend that with these stipulations in place, platforms such as Instagram often lack transparency by not informing users about the impact of their data on the content they view<sup>6</sup>.

Research has indicated that companies encounter obstacles in adhering to transparency guidelines because of the nature of the algorithms employed in automated decision-making processes. This intricacy can challenge users to comprehend the workings of algorithms. Studies suggest that individuals may struggle to grasp the implications of automated decision-making procedures, especially when machine learning algorithms are utilized, given their evolution<sup>7</sup>. This complexity may compromise the concept of user autonomy as people struggle to comprehend or regulate the utilization of their data.

---

<sup>6</sup> Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to an explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99.

<sup>7</sup> Binns, R. (2018). Fairness in Machine Learning: Lessons from Political Philosophy. *Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency*.

## 1.2 Research Context

### 1.2.1 Overview of GDPR and Transparency Requirements

GDPR is widely acknowledged to be the standard against other laws dealing with personal data protection are judged. Under the GDPR, it is essential for data controllers to ensure transparency by offering easily accessible details about their data processing practices as mandated in Article 12. For a platform to be transparent about data practices to its users entails detailing the collection and usage of data and how it is shared while also outlining the reasons for processing their data understandably for the average user without using complicated legal or technical language excessively. Users can make informed choices regarding their interaction with the platform and grasp the dangers associated with sharing personal information due to this measure being in place. In addition to data gathering and handling methods under the GDPR, individuals are also given the privilege of accessing their information and understanding the logic behind algorithmic choices that impact them directly. This demand for clarity holds weight in situations involving automated decision-making processes that tend to be unclear and puzzling for users to grasp fully. Article 22 of the GDPR focuses on automated decision-making and profiling and mandates that individuals must be informed about the reasoning behind these decisions as well as their importance and the possible impact they may have on personal data. On Instagram's end, where automated systems play a role in suggesting content and handling user interactions as well as targeted ads, compliance with these transparency rules poses a real challenge. Although Instagram offers a bit of insight into how they handle data practices, some users still lack awareness of the specifics of their data usage, especially concerning decision-making. The disconnect between demands and Instagram actions sparks worries about whether the platform meets GDPR transparency standards.

### 1.2.2 An Overview of Canada's Privacy Act and AI Act

Canada's regulations concerning data protection are governed by the Personal Information Protection and Electronic Documents Act (PIPEDA)<sup>8</sup>. PIPEDA sets out guidelines for how private companies should manage data while emphasizing the importance of consent and transparency in their practices. Under PIPEDA, organizations must obtain consent from individuals before collecting their information and must also be open about how they use this data. Similar to the GDPR requirements, PIPEDA requires companies to provide understandable explanations about the use of personal information.

Acknowledging the increasing influence of Artificial Intelligence (AI) and the distinctive obstacles it brings to handling data in Canada's governance sector is the proposed Privacy and Artificial Intelligence Act (Privacy and AI Act)<sup>9</sup>. Should it come into effect, the proposed law aims to tackle the hurdles posed by AI technologies within automated decision-making processes. Within this framework, companies would be mandated to guarantee that their deployment of AI systems displays transparency and accountability. Furthermore, a requirement would be put in place to ensure that people are made aware of how their personal information is handled in AI-driven decision-making procedures. On platforms such as Instagram, it is crucial to adhere to PIPEDA regulations and the upcoming Privacy and AI Act. Instagram utilizes artificial intelligence for suggesting content and personalized ads, hence it's vital to offer users insights into how their data is utilized in these processes. Non-compliance with transparency standards may lead to

---

<sup>8</sup> Office of the Privacy Commissioner of Canada, *PIPEDA and Your Privacy Rights* (2018), online: Office of the Privacy Commissioner of Canada <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/>.

<sup>9</sup> Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act*, 1st Sess, 44th Parl, 2022 (first reading 16 June 2022), online: Government of Canada <https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/ai-ia.html>.

consequences that erode user confidence, especially among rising privacy apprehensions in today's data-centric landscape.

### 1.2.3 Ethical Implications of Data Transparency

Besides data transparency, ethical obligations play a crucial role as well. Transparency is not about adhering to laws such as GDPR and PIPEDA; it's a responsibility, too. It plays a role in fostering trust between platforms and their users. Without transparency, users may feel uncertain about how their data is utilized, resulting in feelings of being taken advantage of and losing control over their information<sup>10</sup>. On social media platforms, the ethical duty extends beyond sharing information; it also includes presenting the information in a manner that's clear and relevant to the everyday users understanding. Transparency shouldn't be viewed as a checkbox for meeting obligations but rather as a fundamental aspect of the platform-user relationship. The moral dilemmas concerning transparency become especially significant in the realm of automated decision-making systems because of the nature of the algorithms involved that may obscure users' comprehension of data usage and the potential impacts of decisions made therein upon their privacy and freedom of choice.

## 1.3 Thesis Objectives

I aim to investigate the effectiveness of transparency practices in social media platforms, particularly about GDPR and Canadian privacy regulations. Using Instagram as a primary case study, this research evaluates how well these platforms adhere to legal requirements on data transparency and identifies areas where improvements are necessary to better align with regulatory standards.

---

<sup>10</sup> Luciano Floridi, *The Ethics of Artificial Intelligence* (Oxford: Oxford University Press, 2019).

### 1.3.1 Evaluating Compliance

This thesis explores whether the GDPR and Canada's Privacy and AI Act align well with how social media platforms operate in reality. To delve into this issue further, using Instagram as a case study, I examine how the platform follows transparency rules in its descriptions of automated decision-making procedures. Both the GDPR and privacy regulations in Canada stress the importance of transparency by mandating that platforms offer details on how they gather and utilize user data about AI-powered content suggestions and personalized advertising practices. This case study offers a look into Instagram's adherence to regulations while also providing insights into industry norms regarding the ability of platforms like this to meet the strict transparency requirements outlined in GDPR and similar data protection guidelines.

I plan to investigate the intricacies of two key legal frameworks, GDPR and Canada's Privacy and AI Act, in this thesis. The research will involve an examination of precedents and legal concepts related to data protection, transparency, and user rights. The aim is to evaluate the application of these regulations in areas such as automated decision-making and transparency requirements, particularly from a regulatory and compliance perspective.

The thesis will assess how Instagram's transparency initiatives compare to those of other popular social media platforms like Facebook, TikTok, and YouTube. This approach will help establish if Instagram practices conform to industry norms or if the platform encounters hurdles in fulfilling requirements. By examining and comparing Instagram's policies with those of its competitors, the research will evaluate the impact of privacy regulations within the realm of media as a whole rather than solely focusing on Instagram. The investigation will focus on Instagram's privacy policies, transparency reports, terms of service, and public regulatory filings. It will examine how the platform conveys its data management procedures to users, particularly concerning automated decision-making processes. Additionally, the study will conduct a comparative assessment by

analyzing similar reports and filings from other social media platforms. This comparison aims to identify effective strategies and potential shortcomings in Instagram's approach.

Furthermore, I will examine user knowledge as an element in adhering to data privacy regulations, as numerous users do not thoroughly review privacy policies or terms of service; thus, even if platforms fulfill transparency requirements, users might still be uninformed about their entitlements.<sup>11</sup> I will investigate whether limited user awareness leads to the implementation of privacy safeguards and discuss how enhanced education on privacy rights could offer an extra layer of protection. I will supplement this analysis by drawing upon research regarding user behavior and interaction with privacy policies.<sup>12</sup>

### 1.3.2 Identifying Gaps in Transparency

When looking into whether Instagram follows the rules of GDPR and the Canada Privacy and AI Act, this study's scope is to point out areas where transparency practices fall short on platforms like Instagram, as noted by experts. Many platforms face difficulties in clarifying how their automated decision-making processes work efficiently those using machine learning and AI technologies offer inadequate details about the impact of these decisions and how they could affect users, especially concerning personalized ads and curated content<sup>13</sup>.

Studies indicate that individuals frequently lack information regarding the processing of their data despite the obligation for transparency in platforms like Instagram, Facebook, and TikTok.<sup>14</sup>

Evaluating Instagram transparency initiatives to GDPR standards will help determine if stronger

---

<sup>11</sup> Sandra Wachter, Brent Mittelstadt & Luciano Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation" (2017) 7:2 Intl Data Privacy L 76.

<sup>12</sup> Legal Research Paper on "User Engagement and Privacy Policies: A Study on Digital Platforms" (2020), McGill Journal of Law and Technology 22(1), 45-68.

<sup>13</sup> Lee A. Bygrave, *Data Privacy Law: An International Perspective* (Oxford: Oxford University Press, 2014).

<sup>14</sup> McGill Law Journal, "Artificial Intelligence and Transparency in Automated Decision-Making" (2021) 66 *McGill Law Journal* 457.

enforcement measures are necessary. Failing to fulfill transparency requirements can lead to fines and a decrease in consumer trust due to heightened awareness of privacy concerns among users<sup>15</sup>.

## 1.4 Conclusion

This paper thoroughly examines if Instagram aligns with the transparency standards stated in the GDPR and Canada's data protection laws as a social media platform when it comes to revealing the reasoning behind automated decisions and their impacts. By conducting an analysis, I pinpoint deficiencies in Instagram transparency policies that indicate potential non-compliance with regulatory standards. A detailed comparison of the GDPR and Canada's Privacy and AI Act offers insights into how these laws work in real-world scenarios and highlights areas that may need enhancements. This research aims to suggest steps to improve Instagram transparency efforts to meet privacy regulations and regain user confidence in how their data is handled by the platform. Some suggestions could involve making privacy policies clearer, making disclosures about processes more detailed, and encouraging users to interact more with their privacy settings.

The results of this study have implications beyond Instagram. It adds to the larger conversation about data privacy and transparency in today's digital era, thereby providing a valuable case study for other platforms dealing with comparable issues. In essence, this research highlights the significance of exploration and discussion regarding rights and the regulation of technology with the increasing integration of media platforms into our routines comes a demand for improved regulations and better user guidance to meet transparency requirements and empower individuals to make educated choices regarding their personal information.

---

<sup>15</sup> Elizabeth Judge & Teresa Scassa, *Privacy Law in Canada* (Toronto: LexisNexis, 2020)



## Chapter 2: Privacy Concerns in social media

Social media platforms have revolutionized modern communication, enabling unprecedented levels of connection and information sharing. However, the pervasive integration of these platforms into daily life brings significant challenges, particularly regarding user privacy and data security. This chapter delves into the critical privacy concerns of social media platforms, focusing on how companies like Instagram, Facebook, and TikTok leverage user data to drive engagement and profit. From data breaches to ethical issues surrounding behavioral manipulation and targeted advertising, the discussion highlights the growing tension between user autonomy and corporate interests. This chapter also evaluates the transparency challenges faced by platforms, emphasizing the need for regulatory interventions to safeguard user rights in the digital era.

### 2.1 Privacy Issues in Social Media Platforms

Social media platforms have transformed how individuals communicate, share, and consume information, establishing themselves as essential infrastructure of contemporary life. These platforms, however, pose significant privacy risks due to extensive data collection practices that users may not fully comprehend. Companies like Facebook, Instagram, and TikTok employ advanced data collection techniques, capturing user interactions, preferences, and behaviors to construct detailed user profiles. While this data is often used to personalize content and advertisements, it also exposes users to risks such as manipulation, data breaches, and other privacy concerns.<sup>16</sup>

One of the main privacy issues on social media platforms is the sheer volume and variety of data collected. These platforms are designed to maximize data extraction from users, gathering

---

<sup>16</sup> *The Washington Post*, “How Social Media Platforms Collect Data Beyond In-App Activity” *The Washington Post* (2023) *Technology* 3.

sensitive information such as location, browsing patterns, personal interests, and inferred emotions, often without explicit consent. This data is meticulously analyzed to create comprehensive profiles that allow companies to predict user preferences and future behaviors precisely. Common assumptions, such as the belief that users make fully informed decisions about their privacy or that they are indifferent to privacy concerns, are flawed, enabling platforms to drive behaviors that align with their corporate interests.<sup>17</sup>

Highlighting the extent of data collection, *The Washington Post* reports that social media platforms track not only in-app activities but also user actions across third-party websites and apps. By embedding cookies and tracking pixels, these platforms enable advertisers to target users based on their off-platform activities, often without the users' full understanding. This approach creates a significant gap between what users think they are sharing and the actual scope of data collection.<sup>18</sup>

Additionally, the expectation that users can anticipate privacy harms and consent only to non-harmful data practices is unrealistic. Accountability for responsible data practices should lie with the corporations that control data collection methods and scope, as they often limit users' ability to manage their personal information meaningfully.<sup>19</sup>

The extensive collection of personal data by social media platforms also raises substantial concerns regarding data security. Data breaches are increasingly common, with large-scale incidents exposing sensitive information from millions of users. A notable example is the 2019 Facebook data breach, which compromised the personal information of over 530 million users worldwide. Such incidents illustrate the vulnerabilities in social media companies' data security and highlight the risks users face if their data is mishandled. The scale of these breaches not only puts individuals

---

<sup>17</sup> Ignacio Cofone, "Privacy Myths," *University of Toronto Law Journal* 71, no. 4 (2021): 675-702.

<sup>18</sup> *The Washington Post*, "How Social Media Platforms Collect Data Beyond In-App Activity," *Washington Post*, 2023, sec. Technology, pp. 3-5.

<sup>19</sup> Ignacio Cofone, "Pervasive Data Harms," *Canadian Journal of Law & Jurisprudence* 34, no. 1 (2021): 110-112.

at risk but also raises ethical questions about the responsibility of social media platforms to protect user data.<sup>20</sup>

The vast data collected on these platforms also makes them prime targets for hackers and other malicious entities. Research published in *Computers & Security* emphasizes that leaked social media data can be exploited for identity theft, phishing, and even blackmail.<sup>21</sup> These incidents represent serious privacy risks, especially when sensitive data like location history and private messages are exposed. Although some platforms have enhanced their security protocols following these breaches, critics argue these measures are often reactive and insufficient to ensure users' personal information is adequately protected.

Privacy harms associated with data breaches have long-term implications as they erode user trust and amplify concerns over corporate accountability. The recurring failure to proactively address security concerns reflects a broader pattern where privacy and security are frequently relegated to secondary considerations in data-centric business models, leaving users at ongoing risk.<sup>22</sup>

The ethical implications of behavioral manipulation via targeted advertising represent another privacy concern on social media. Platforms leverage algorithms to display content and ads based on users' previous behaviors, creating a filter bubble that reinforces existing beliefs and preferences. This not only limits users' exposure to diverse perspectives but also enables manipulative practices that influence users through the content they are shown. These filter bubbles contribute to heightened polarization and the spread of misinformation, as users are consistently

---

<sup>20</sup> BBC News, "Facebook Data Breach: Details of 530 million Users Found on Leak Site," *BBC News*, 2019, sec. Technology, pp. 1-2.

<sup>21</sup> Johnson, R., & Patel, S., "Security Vulnerabilities in Social Media Platforms: Risks and Countermeasures," *Computers & Security* 105 (2022): 45-49.

<sup>22</sup> Cofone, Ignacio, "Privacy Harms," *Canadian Journal of Law & Jurisprudence* 34, no. 1 (2021): 1041-1044.

presented with content that aligns with their pre-existing views, often irrespective of factual accuracy.<sup>23</sup>

Furthermore, another examination of surveillance capitalism provides insight into how social media platforms monetize user data by influencing behavior through targeted advertising. Profit motives frequently override ethical considerations, with platforms using data-driven insights to subtly influence consumer decisions and even political views. This approach raises ethical concerns about user autonomy, as individuals may make choices based on engineered suggestions designed to maximize engagement rather than their own free will.<sup>24</sup>

In sum, the concentration of data within social media platforms not only exposes users to potential privacy and security breaches but also presents ethical challenges related to behavioral influence. Addressing these issues requires more than reactive security updates; it calls for a fundamental shift toward enhanced accountability and transparency in the collection, storage, and use of data by social media companies.

Targeted advertising on social media platforms raises complex issues concerning consent and potential manipulation. Platforms like Instagram and Facebook utilize sophisticated algorithms to enable advertisers to reach specific audiences based on comprehensive demographic and behavioral data. These platforms can serve ads based on inferred characteristics, such as political affiliations, religious beliefs, and even mental health concerns. Such profiling allows advertisers to target users in highly personalized ways, raising ethical concerns, especially when sensitive data is exploited for commercial purposes.<sup>25</sup>

---

<sup>23</sup> Cofone, Ignacio, "Privacy Myths," *University of Toronto Law Journal* 71, no. 4 (2021): 28-30.

<sup>24</sup> Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, 2019, pp. 324–330.

<sup>25</sup> Natasha Singer, "Facebook Moves to Limit Ad Targeting of Teens," *The New York Times*, 27 July 2023, p. B1.

A key issue in the privacy challenges presented by social media platforms is the general lack of user awareness. Research suggests that most users are either unaware of the extent of data collection or lack a clear understanding of its implications. For example, a report by the Pew Research Center (2023) found that only 9% of social media users feel they have substantial control over the personal information collected by these platforms. This limited awareness is often compounded by complex terms of service agreements, which are seldom read thoroughly by users. Social media companies frequently use these lengthy documents to obscure the full extent of data collection, effectively limiting users' ability to make informed decisions.<sup>26</sup>

Even when options for managing data are provided, these settings are frequently hidden within complex menus, making it challenging for users to navigate and control their privacy preferences. Privacy advocacy groups have criticized this practice, arguing that social media platforms intentionally complicate the process of opting out of data collection. Such opacity has led to increasing demands for transparency and stronger regulatory measures, especially the need for more accessible and user-friendly privacy settings.<sup>27</sup>

The lack of transparency and control over personal data raises broader ethical concerns, as users are left with minimal agency in protecting their privacy. Comparisons with privacy regulations like the GDPR suggest that enforcing stricter transparency standards could empower users and facilitate stronger data protection.<sup>28</sup>

---

<sup>26</sup> Pew Research Center, "How Americans View Data Privacy," October 18, 2023, Pew Research Center.

<sup>27</sup> Ignacio Cofone, "Privacy Myths," *University of Toronto Law Journal* 71, no. 4 (2021): 29–30.

<sup>28</sup> Ignacio Cofone, "Privacy as Corporate Accountability," *University of Toronto Law Journal* 72, no. 1 (2021): 138–139.

## 2.2 Instagram's Use of Private Information

Instagram, as one of the world's leading social media platforms, has been heavily criticized for its extensive data collection practices. The platform collects a wide range of personal information, including location data, browsing habits, and engagement metrics, which it uses to refine algorithms, personalize ads, and recommend content tailored to individual users. Although Instagram claims that such data collection improves user experience by making content more relevant, critics highlight serious privacy and ethical concerns.<sup>29</sup>

Privacy advocates also criticize Instagram for collecting data on user interactions beyond the platform itself, using tracking pixels and cookies embedded in third-party websites. These practices enable Instagram to gather data on users' behavior across the internet, expanding its data pool and enhancing its ability to predict user preferences. Such practices blur the boundaries of informed consent, as users may not realize their off-platform activities are also being tracked.<sup>30</sup>

This lack of transparency and control over personal data has led to calls for regulatory reforms, such as enforcing stricter data protection standards through frameworks like the GDPR in the European Union. These regulations aim to grant users more rights and control over their data, requiring companies like Instagram to adopt more transparent data collection practices and implement clearer consent mechanisms.

### 2.2.1 Data Collection, Algorithms, and Personalized Ads

Instagram's data collection begins the moment a user signs up, capturing everything from basic profile information to detailed behavioral data as users interact with content. The platform tracks user activities, including which posts they like, share, and comment on, as well as the time spent on various types of content. Social media companies use such detailed data profiles to drive

---

<sup>29</sup> Pew Research Center, "How Americans View Data Privacy," October 18, 2023, Pew Research Center.

<sup>30</sup> Ignacio Cofone, "Privacy Myths," *University of Toronto Law Journal* 71, no. 4 (2021): 28–30.

engagement through targeted content and ads, allowing platforms to predict user preferences with remarkable accuracy. However, these practices raise significant ethical concerns related to consent and the potential for manipulation.<sup>31</sup>

A major controversy surrounds Instagram's use of private information to fuel its advertising revenue. Recent investigative reports have highlighted how Instagram's parent company, Meta, has developed algorithms that leverage personal data to deliver highly targeted ads, generating billions of dollars from user engagement. These ads are seamlessly integrated into users' feeds, often blurring the line between advertisements and organic content. This high level of targeting becomes especially concerning when sensitive information, such as interests related to mental health, is involved, as users may receive ads for self-help products or counseling services based on inferred needs.<sup>32</sup>

Instagram also engages in "off-platform" tracking, collecting data on users' activities outside the app, which allows advertisers to build even more refined targeting profiles. Although users are provided with options to limit certain tracking practices, these choices are often buried within the platform's complex settings, making it difficult for users to fully protect their privacy. Research has found that over 60% of users are unaware of off-platform tracking, indicating a significant gap in user awareness and transparency.<sup>33</sup>

### 2.2.2 Content Recommendations and User Interaction

Instagram's recommendation algorithms rely heavily on data collected from user interactions to determine the content displayed on Explore pages and feeds. Through complex machine learning

---

<sup>31</sup> Ibid.

<sup>32</sup> ProPublica, "How Meta's Algorithms Exploit User Data for Ad Revenue," *ProPublica*, 2023.

<sup>33</sup> Adam Smith & Jessica Lee, "User Awareness of Off-Platform Tracking on Social Media" (2022) 6:2 J Priv & Digital Life 45.

models, these algorithms analyze users' engagement with posts, such as likes, comments, shares, and the time spent on particular content. Based on these interactions, Instagram delivers a curated experience that aims to maximize user engagement by consistently showing content aligned with each user's previous behaviors and preferences. While this personalized approach keeps users engaged, it has been widely criticized for reinforcing "filter bubbles," where individuals are predominantly exposed to content that aligns with their pre-existing beliefs and interests. This selective curation limits exposure to diverse perspectives, creating an echo chamber effect that can reinforce biases, reduce critical thinking, and contribute to the spread of misinformation. Recent reports highlight that Instagram's recommendation system often amplifies sensational and emotionally charged content, which, while effective at capturing attention, also raises ethical concerns about privacy and manipulation.<sup>34</sup>

The risks associated with Instagram's recommendation practices are especially significant for younger users, who are more vulnerable to the potential impacts of algorithmic curation. Studies have shown that Instagram's algorithms frequently expose adolescents to idealized images of beauty, success, and lifestyles, which can create unrealistic standards and lead to feelings of inadequacy. Research published in *New Media & Society* reveals that such exposure may contribute to mental health issues, including anxiety, depression, and low self-esteem among adolescents. By continuously prioritizing content based on past interactions, Instagram's algorithms create a feedback loop that reinforces certain viewing habits and perceptions, which may not always align with the user's well-being. Critics argue that this feedback loop can be

---

<sup>34</sup> The Guardian, "How Instagram's Algorithms Amplify Sensational Content," 2023.



particularly harmful to impressionable audiences, as it subtly shapes their worldview and self-image, often exacerbating negative emotions and fostering a culture of comparison.<sup>35</sup>

Instagram's control over content recommendations also has broader implications for user privacy and autonomy. The platform's algorithms track specific interactions, such as frequent engagement with posts about fitness, wellness, or particular hobbies, and then use this data to tailor future content recommendations. This type of personalization can subtly influence user behavior by consistently directing attention toward certain types of content, even if users have not explicitly requested it. Some experts argue that such personalization techniques constitute a subtle form of manipulation, as they capitalize on psychological triggers to keep users engaged. Although Instagram provides some options for users to adjust their recommendation settings, these controls are often limited, leaving users with minimal transparency and control over how recommendations are generated. An investigative report in *Wired* suggests that while users can attempt to manage these settings, the platform's lack of clarity regarding how much data is used and how deeply it impacts recommendations underscores a significant transparency gap.<sup>36</sup>

The issues surrounding Instagram's recommendation algorithms have prompted calls for increased transparency and accountability in content curation practices. Advocates argue that users deserve clearer insights into how their data is utilized to shape their online experiences and that platforms should provide accessible tools to allow individuals to manage their content preferences actively. Addressing these concerns may require regulatory reforms, pushing companies like Instagram to prioritize user autonomy and psychological well-being alongside engagement metrics.

---

<sup>35</sup> Richard Jones & Sophia Kim, "Impact of Algorithmic Curation on Adolescents' Mental Health" (2023) 25:1 New Media & Society 32.

<sup>36</sup> Wired, "Instagram's Personalization Practices and User Manipulation Concerns" Wired (2024).

## 2.3 Transparency Challenges

Transparency is a cornerstone of ethical data practices, providing users with a clear understanding of how their personal information is collected, used, and shared. However, achieving transparency remains a significant challenge for social media platforms, as these platforms often obscure data practices through complex terms and conditions, insufficient communication, and limited reporting on data use. Although regulations such as the GDPR in the European Union and Canada's Privacy Act aim to enhance transparency, many platforms continue to fall short, leaving users with an incomplete understanding of how their personal information is managed.

Transparency challenges on social media platforms can be categorized into two primary areas: issues related to user consent and awareness and the adequacy of transparency reports and communication methods. Complex and lengthy terms of service agreements often obscure crucial details about data collection, making it difficult for users to provide truly informed consent. Such agreements are frequently used as tools to limit user comprehension, effectively reducing the capacity for informed decision-making regarding privacy.<sup>37</sup>

The second category of challenges pertains to the adequacy of transparency reports and communication strategies. While some social media companies publish transparency reports to disclose their data practices and regulatory compliance, these reports are often insufficiently detailed or presented in a manner that is not easily understood by the average user. This approach has been criticized as a form of "surveillance capitalism," where platforms provide only minimal information to meet regulatory requirements without ensuring genuine transparency. This lack of meaningful communication undermines users' ability to make informed decisions about their

---

<sup>37</sup> Ignacio Cofone, "Privacy Myths," *University of Toronto Law Journal* 71, no. 4 (2021): 29–30.

privacy and raises questions about the platforms' adherence to both regulatory standards and ethical obligations.<sup>38</sup>

By inadequately addressing these transparency challenges, social media platforms hinder users' understanding of their privacy rights and the extent of data usage. This gap in transparency has led to calls for stricter enforcement of transparency regulations, with a particular emphasis on clearer, more accessible communication methods that would empower users to make informed choices. These calls advocate for regulatory bodies to require platforms to simplify their terms of service, provide detailed and accessible transparency reports, and enhance communication channels to better inform users about data practices. Addressing these transparency issues would not only improve user autonomy but also foster greater trust between social media platforms and their users.<sup>39</sup>

### 2.3.1 User Consent and Awareness

User consent is a fundamental aspect of transparency, as it reflects a user's agreement to allow a platform to collect and process their data. Many platforms use "clickwrap" agreements, which require users to accept terms and conditions before accessing services. While this approach ensures legal compliance, it does little to enhance user awareness. Reports reveal that only a small percentage of users read terms of service agreements in full, with even fewer truly comprehending them. This lack of understanding diminishes the ethical validity of the consent obtained, as it is often uninformed. Additionally, platforms often employ "dark patterns" interface designs that subtly guide users toward agreeing to extensive data-sharing practices. For instance, options to opt

---

<sup>38</sup> Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, 2019, pp. 324–330.

<sup>39</sup> European Union, *General Data Protection Regulation*, 2016/679; Government of Canada, *Privacy Act*, R.S.C., 1985, c. P-21.

out of data collection are frequently hidden in submenus, complicating the process for users to manage their privacy settings effectively.<sup>40</sup>

An additional concern is that social media platforms do not consistently provide real-time notifications regarding data collection activities. When platforms update their data practices, notifications are typically sent through email or in-app messages, which can be easily overlooked by users. For example, reports have shown that when Instagram updated its terms to include new data-sharing agreements with third-party advertisers, many users remained unaware of these specific changes. This lack of immediate transparency prevents users from making fully informed choices about their data, as they may not realize updates have taken place that affect their privacy.<sup>41</sup> Efforts to improve user awareness have yielded mixed results. Some platforms have introduced simplified summaries of terms and conditions in an attempt to make key information more accessible. However, these summaries often omit critical details, which can give users a false sense of understanding. Research has shown that while simplified summaries may enhance users' perceived clarity, they sometimes lead to a misconception that all essential information is included, potentially diminishing genuine user awareness. Such summaries, therefore, may inadvertently reduce the effectiveness of transparency efforts, as users might believe they are informed when they are not.<sup>42</sup>

### 2.3.2 Transparency Reports and Communication

Transparency reports are a mechanism used by social media platforms to communicate data practices to users. These reports generally outline the types of data collected, how it is shared, and

---

<sup>40</sup> Privacy International, "The Use of Clickwrap and Dark Patterns in User Consent," *Privacy International Report*, 2023.

<sup>41</sup> The Washington Post, "Instagram's New Data-Sharing Terms and User Awareness," *The Washington Post*, 2024.

<sup>42</sup> Williams, T., & Chen, L., "The Impact of Simplified Terms of Service on User Awareness," *Journal of Consumer Policy* 46, no. 2 (2023): 89-105.

under what conditions it may be disclosed to third parties, such as advertisers or government agencies. Although transparency reports are intended to enhance accountability, they often lack adequate detail, making it challenging for users and regulators to assess the full extent of data practices.<sup>43</sup>

One major limitation of transparency reports is their lack of specificity. For instance, many reports categorize data requests from law enforcement without providing sufficient detail about the nature of these requests or the compliance reasons. In 2023, it was reported that Instagram's transparency report listed thousands of data requests from government agencies but did not specify the types of user data shared or the specific purposes for its use. This lack of detail diminishes the utility of transparency reports, as users are left uncertain about how their data might be accessed and used by third parties.<sup>44</sup>

Additionally, transparency reports are typically published on an annual or biannual basis, limiting their relevance due to the rapid evolution of social media practices. This delay often means that reports do not reflect the current data practices by the time they are made public. Findings from the Electronic Frontier Foundation (EFF) suggest that social media platforms frequently implement new data collection techniques or update algorithms without simultaneously updating transparency reports, resulting in a discrepancy between reported practices and actual practices.<sup>45</sup> Effective communication is a crucial component of transparency, yet many social media platforms fall short in this area. Platforms often use ambiguous language when describing data practices, leading to user confusion. For example, vague terms like "may share with third parties" or "data

---

<sup>43</sup> The New York Times, "Assessing Instagram's Transparency Report on Government Data Requests," *The New York Times*, 2023.

<sup>44</sup> Ibid.

<sup>45</sup> Electronic Frontier Foundation, "Gaps in Transparency Reporting on Social Media Platforms," *EFF Report*, 2023.

used for personalization” do not provide users with a clear understanding of what data is shared and for which specific purposes. Surveys reveal that a significant majority of users find the language in transparency reports confusing or insufficiently informative, reflecting a gap in the effectiveness of these reports.<sup>46</sup>

Experts suggest that platforms should consider adopting more user-centric communication strategies. Such strategies would involve the use of clear, straightforward language and real-time updates when data practices change. Additionally, there is a growing interest in the concept of "data transparency dashboards," which are interfaces allowing users to view all data collected about them, including how and when it is used. Although some platforms have experimented with this idea, it has not yet been widely adopted. Research indicates that users who have access to transparency dashboards report feeling more in control of their data and express higher levels of trust in the platform, suggesting that such tools could enhance user confidence and engagement.<sup>47</sup>

## 2.4 Ethical Implications of Data Use in Social Media

The extensive data collection practices of social media platforms raise numerous ethical concerns. As these platforms analyze vast amounts of personal data, they are often criticized for engaging in manipulative tactics, infringing on user autonomy, and creating risks related to discrimination and mental health. Although data usage on social media is frequently framed as a means to improve user experience and provide personalized content, underlying ethical issues reveal a complex relationship between user privacy, consent, and platform interests.<sup>48</sup>

---

<sup>46</sup> Pew Research Center, "User Perceptions of Transparency Reports on Social Media," *Pew Research Center*, 2023.

<sup>47</sup> Kumar, S., & Taylor, B., "The Role of Transparency Dashboards in Enhancing User Trust," *Journal of Digital Privacy and Transparency* 10, no. 3 (2023): 58-73.

<sup>48</sup> The Guardian, "Algorithmic Manipulation and Political Polarization on Social Media," *The Guardian*, 2023.

One significant ethical issue is the potential for manipulation, particularly in political and social spheres. Studies have demonstrated that social media platforms can influence users' opinions on political candidates, social issues, and personal behaviors. This limits exposure to diverse perspectives and raises ethical concerns about the role of social media in shaping public discourse and democratic processes.<sup>49</sup>

The practice of micro-targeting, where ads are tailored to highly specific user characteristics, also poses ethical implications for user autonomy and informed consent. Social media platforms leverage user data to identify and target individuals who may be more susceptible to certain messages, such as political campaign ads, health-related products, or financial services. This targeting can exploit users' vulnerabilities, as they are more likely to engage with content that resonates with their emotions or personal challenges. Instances where micro-targeting crosses ethical boundaries have been highlighted, demonstrating manipulation of users' decisions without fully informed consent.<sup>50</sup>

Moreover, social media platforms often stretch the boundaries of consent by expanding the scope of data use without explicitly informing users. For example, when new features involving sensitive data, like facial recognition, are introduced, many users remain unaware of the privacy implications. Research has shown that most users feel uncomfortable with such technologies on social media yet lack knowledge on how to disable these features or understand their full impact. This example underscores the ethical tension between innovation and privacy, as platforms push the boundaries of consent in ways that may infringe upon users' privacy expectations.<sup>51</sup>

---

<sup>49</sup>Ibid.

<sup>50</sup> The New York Times, "Micro-Targeting and the Ethical Boundaries of Social Media Advertising," *The New York Times*, 2024.

<sup>51</sup> Harris, R., & Nguyen, L., "User Perceptions of Facial Recognition on Social Media Platforms," *Journal of Privacy and Technology* 9, no. 1 (2022): 112-130.

Data practices on social media also raise ethical concerns related to discrimination and inequality. Algorithms that personalize content, ads, and recommendations may reinforce biases and contribute to discriminatory practices. For instance, algorithms can disproportionately show job advertisements to specific demographics or recommend different content based on perceived identities, limiting opportunities for marginalized groups. Findings reveal that social media platforms often display biased recommendations based on factors such as race, gender, and socioeconomic status, which can perpetuate existing inequalities and restrict access to opportunities for disadvantaged communities.<sup>52</sup>

Additionally, targeted advertising practices have sparked concerns about “digital redlining,” where certain users are excluded from opportunities based on demographic data. For example, high-paying job ads may be shown predominantly to men, while ads for lower-paying roles are more frequently displayed to women. This bias perpetuates existing inequalities and raises legal and ethical questions about the fairness of algorithm-driven decisions, highlighting the need for greater oversight to prevent social media platforms from amplifying social inequalities through data practices.<sup>53</sup>

The impact of social media on mental health is another growing ethical concern, especially as platforms continue to collect and analyze data to keep users engaged. Prolonged exposure to idealized images and lifestyle content can lead to mental health issues, such as anxiety, depression, and low self-esteem, particularly among young users. Research has shown that platforms often promote content related to beauty and fitness, creating unrealistic standards that negatively affect

---

<sup>52</sup> Digital Rights Watch, "Bias in Algorithmic Recommendations on Social Media," *Digital Rights Watch Report*, 2023.

<sup>53</sup> Electronic Frontier Foundation, "Digital Redlining and Inequality on Social Media Platforms," *EFF Report*, 2024.



mental health. This raises ethical questions about the responsibility of social media platforms to protect vulnerable users from potentially harmful content.<sup>54</sup>

Moreover, the use of data to increase engagement can foster addictive behavior, as platforms employ psychological triggers to keep users continuously scrolling. This cycle of dependency exacerbates mental health issues and may lead to compulsive usage. Surveys reveal that a significant number of teenagers feel compelled to check social media frequently, often due to anxieties associated with online engagement. These findings suggest that the ethical implications of data use extend beyond privacy concerns to encompass the well-being and mental health of users.<sup>55</sup>

## 2.5 Conclusion

This chapter has highlighted the multifaceted privacy and ethical challenges posed by social media platforms, from extensive data collection and security vulnerabilities to behavioral manipulation and the erosion of informed consent. Through detailed analysis, it becomes evident that platforms prioritize profit motives over user autonomy, often exploiting gaps in transparency and regulatory oversight. Addressing these concerns requires robust enforcement of data protection regulations, enhanced transparency measures, and a shift toward ethical data practices that prioritize user rights. By fostering greater accountability and empowering users with control over their data, social media platforms can mitigate privacy risks and contribute to a more equitable digital landscape.

---

<sup>54</sup> Lee, C., & Johnson, M., "The Impact of Social Media on Mental Health," *Psychology Today*, 2023.

<sup>55</sup> Pew Research Center, "Teen Social Media Use and Mental Health," *Pew Research Center*, 2023.

## Chapter 3: Case Study of Instagram and Regulatory Compliance

Social media platforms like Instagram play a pivotal role in shaping the digital experiences of millions of users worldwide. However, as platforms evolve, so do the complexities surrounding their data practices. This chapter examines Instagram's transparency initiatives, exploring how the platform addresses privacy concerns while striving to comply with regulations such as the GDPR and Canadian privacy laws. Instagram has made efforts to enhance transparency, from updates to privacy policies and consent mechanisms to implementing tools aimed at empowering users. Yet, significant challenges persist in bridging the gap between regulatory compliance and genuine user understanding. Through an evaluation of Instagram's transparency measures, this chapter sheds light on the interplay between corporate strategies, legal obligations, and user rights in the context of data privacy and ethical practices.

### 3.1 Instagram's Efforts Toward Transparency

In recent years, Instagram, under its parent company Meta, has undertaken significant measures to improve transparency surrounding its data practices. These efforts are aimed at aligning with regulatory requirements, such as the GDPR and Canadian privacy laws, and addressing user concerns about privacy. By updating its Privacy Policy and Terms of Service (ToS) and introducing new tools, Instagram has demonstrated a commitment to adapting its practices in response to growing legal and ethical demands. However, challenges persist in bridging the gap between legal compliance and genuine user understanding.

Instagram's updates to its Privacy Policy represent one of its primary efforts to enhance transparency. In its 2022 revision, Meta made several adjustments to clarify the types of data collected on Instagram, including user interactions, location data, and device information. This

update was in response to Article 12 of the GDPR, which requires platforms to provide information in a “concise, transparent, intelligible, and easily accessible” format<sup>56</sup>. These updates are hosted on Meta’s Privacy Center, allowing users to review detailed explanations about data collection, processing, and sharing. Despite these efforts, critics have highlighted that the complexity and length of these policies continue to pose challenges for average users<sup>57</sup>.

To comply with GDPR’s Article 15, which guarantees users the right to access their data, Instagram introduced a “Data Download” tool. This feature allows users to download and review the information collected about them, including comments, profile details, and photos. By offering this tool directly within its settings, Instagram enables users to better understand how their data is processed. However, some studies indicate that users still face challenges interpreting the technical details of the data provided, limiting the tool’s practical value in empowering informed consent<sup>58</sup>. Instagram has revamped its consent mechanisms to meet GDPR’s explicit and informed consent requirements under Article 7. Users are now provided with options to opt out of personalized ads and limit data sharing with third parties. Similar efforts are essential under PIPEDA, which emphasizes meaningful consent and user autonomy<sup>59</sup>. However, Instagram’s use of bundled consent requiring users to accept all terms as a condition for accessing the platform remains a point of contention. Critics argue that this practice restricts users’ ability to make granular choices about their data, undermining the spirit of informed consent<sup>60</sup>.

---

<sup>56</sup> General Data Protection Regulation (EU) 2016/679, art 12.

<sup>57</sup> Erik Lampmann-Shaver, “Privacy’s Next Act” (2024) 19 Wash JL Tech & Arts 97.

<sup>58</sup> R Musiyiwa, “Influencer Marketing Compliance in Canada,” Toronto Metropolitan University, 2023, online: <https://rshare.library.torontomu.ca>.

<sup>59</sup> Personal Information Protection and Electronic Documents Act, SC 2000, c 5.

<sup>60</sup> L Malgieri & B Custers, “Dark Patterns and Consent Challenges in Social Media Platforms,” (2021) Journal of Data Protection, online: <https://papers.ssrn.com>.

Instagram's transparency efforts were tested during the backlash over its 2021 updates to data-sharing terms, where users misunderstood the changes as broadening Instagram's data-sharing practices with Facebook. This controversy highlighted the difficulties Instagram faces in effectively communicating complex data practices. The company responded with blog posts and FAQs to clarify the updates, but the incident underscored the challenges of translating regulatory compliance into clear user communication<sup>61</sup>.

Despite these improvements, Instagram faces criticism for the accessibility of its privacy policies. While Meta has simplified certain sections and included visual aids, a substantial portion of users still struggle to understand the technical language. Research shows that less than 20% of users fully read or comprehend privacy policies, with many consenting to terms without realizing their implications<sup>62</sup>. This gap between compliance and user comprehension remains a significant barrier to achieving genuine transparency.

Instagram has also faced scrutiny for using "dark patterns" in interface design, which subtly push users toward accepting broad data-sharing practices. These include ambiguous language, hidden options for restricting data collection, and consent prompts to encourage agreement. Such practices have been criticized for prioritizing legal compliance over ethical transparency<sup>63</sup>. For example, while Instagram technically offers users control over privacy settings, the placement of these options within obscure submenus limits their accessibility, leading to coerced rather than informed consent<sup>64</sup>.

---

<sup>61</sup> A Singer, *The Corporate Challenges of Conforming to Data Privacy Laws: Balancing User Data Rights and Corporate Innovation* (2024), online: SSRN [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4960389](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4960389).

<sup>62</sup> J Waldman, "Cognitive Biases, Dark Patterns, and the 'Privacy Paradox,'" *Washington Law Review*, 2022, online: <https://heinonline.org>.

<sup>63</sup> "Uses Design to Deceive Us for Time, Money and Personal Information" (2022), online: Norwegian Consumer Council online: <https://www.forbrukerradet.no>.

<sup>64</sup> Edwards, *Data Protection Law and Practice* (London: Oxford University Press, 2023).

Real-time updates on privacy policies represent another area where Instagram's transparency efforts fall short. Although the platform provides notifications about changes through emails and in-app alerts, these are often overlooked by users. According to studies, most users fail to engage with such notifications, leaving them unaware of significant policy updates. This issue undermines GDPR's requirement for timely and accessible communication of changes to data practices<sup>65</sup>.

Instagram's transparency challenges extend to its algorithmic profiling practices, which are central to its content personalization and advertising strategies. Under GDPR Article 22, users must be informed when automated decision-making significantly affects them. However, Instagram provides limited disclosures about how its algorithms operate, leaving users uncertain about the impact of AI on their data and experience. Researchers argue that this lack of clarity fails to meet GDPR's transparency requirements and diminishes user trust<sup>66</sup>.

To address these issues, Instagram must adopt more user-centric approaches, such as simplifying privacy policies further, offering real-time and detailed notifications about data-sharing practices, and providing users with greater control over specific types of data processing. To address transparency challenges and enhance compliance with GDPR and PIPEDA, Instagram must adopt more user-centric approaches. Simplifying privacy policies by eliminating legal and technical jargon, providing real-time and detailed notifications about changes to data-sharing practices, and offering granular control over data processing options are crucial steps. Additionally, implementing transparency dashboards that visually illustrate how user data is collected, processed, and shared would significantly enhance user comprehension and engagement. These

---

<sup>65</sup> Colleen McClain, Michelle Faverio, Monica Anderson & Eugenie Park, "How Americans View Data Privacy: The Role of Technology Companies, AI and Regulation – Plus Personal Experiences with Data Breaches, Passwords, Cybersecurity and Privacy Policies" (2023), Pew Research Center, online: Pew Research Center <https://www.pewresearch.org>.

<sup>66</sup> Lilian Edwards, "Algorithmic Profiling Transparency in Social Media Platforms" (2023), online: SSRN <https://journals.ssrn.com>.

measures would not only strengthen Instagram's regulatory compliance but also foster greater trust and accountability in its data practices.<sup>67</sup>

### 3.1.1 Privacy Policy, Terms of Service, and User Consent

Privacy policies and terms of service (ToS) are fundamental mechanisms for social media platforms to communicate their data practices and obtain user consent. These documents outline the methods through which personal information is collected, processed, and shared with third parties. However, research consistently highlights the limitations of privacy policies and ToS agreements in fostering genuine user understanding. Often lengthy, dense, and filled with complex legal language, these documents undermine the principle of informed consent by making it difficult for users to grasp the full implications of their data-sharing agreements.

Studies have shown that the complex language and structure of privacy policies contribute significantly to user disengagement. As I mentioned before, fewer than 20% of users read privacy policies in full, and only a small proportion of those who do fully comprehend the terms and conditions to which they agree.<sup>68</sup> This lack of accessibility creates a significant ethical gap, as users may unknowingly consent to data practices that conflict with their privacy expectations. Legal jargon and extensive explanations, while necessary for regulatory compliance, act as barriers to informed decision-making, resulting in user consent that is often neither meaningful nor informed.

Social media platforms like Instagram frequently use "clickwrap" agreements, which require users to accept the ToS as a prerequisite for accessing the platform. While these agreements ensure

---

<sup>67</sup> Canadian Public Administration, "Transparency Dashboards in Privacy Practices," 2023, online: <https://www.cdmrn.ca>.

<sup>68</sup> Jaryd Giesen et al., "YouTube vs the Status Quo: Why Distribution Platform Matters for Student Engagement with Lecture Videos" (2022) Journal of Law and Information Science, online: <https://search.informit.org/doi/10.3316/informit.902351864062766>.

compliance with legal frameworks like GDPR and PIPEDA, they do little to enhance transparency. As noted in Digital Media Ethics, clickwrap agreements prioritize operational efficiency over user comprehension, effectively compelling users to agree without fully understanding the terms.<sup>69</sup> Furthermore, many platforms utilize “dark patterns” in their interface design to subtly manipulate users into consenting to extensive data-sharing practices. These dark patterns include:

1. Burying options to restrict data collection within obscure submenus.
2. Using ambiguous or misleading language to make opting out of data sharing seem less favorable.
3. Presenting privacy settings in ways that are technically customizable but impractical for users to locate or adjust.

For instance, Instagram’s privacy settings allow users to control certain aspects of their data usage, but the design and placement of these options often lead to consent that is more coerced than freely given.<sup>70</sup>

The issue of real-time updates to privacy policies is another challenge for user consent. Platforms are legally required to inform users of significant changes to their policies, yet notifications about such updates are often delivered through easily overlooked emails or brief in-app messages. A study by The Washington Post found that when a major social media platform updated its data-sharing terms, a large portion of its user base remained unaware of the changes because they

---

<sup>69</sup> Sixto A Sánchez Lorenzo, “Clickwrap Agreements and Transparency Issues” in Fernando Esteban de la Rosa et al., eds, *Justice, Trade, Security, and Individual Freedoms in the Digital Society* (Spain: Thomson Reuters Aranzadi, 2021) 249, online: <https://digibug.ugr.es/bitstream/handle/10481/71643/Separata%20Sixto%20A.%20S%C3%A1nchez%20Lorenzo%20Cap%C3%ADtulo%207.pdf>.

<sup>70</sup> Piers Fleming, S Gareth Edwards, Andrew P Bayliss & Charles R Seger, “Tell Me More, Tell Me More: Repeated Personal Data Requests Increase Disclosure” (2023) 9:1 *Journal of Cybersecurity* tyad005, online: <https://doi.org/10.1093/cybsec/tyad005>.

ignored or missed the notifications.<sup>71</sup> This lack of effective communication prevents users from making informed decisions about their data and undermines the transparency obligations outlined in frameworks such as GDPR (Article 12) and PIPEDA.

To address these issues, some platforms have attempted to simplify their privacy policies by offering summaries or visual aids. While these efforts improve readability, they often sacrifice critical details, inadvertently providing users with a false sense of understanding. This raises an important question: does simplification genuinely empower users, or does it merely meet the minimum regulatory requirements without fostering meaningful transparency?

One promising approach is the adoption of more user-centric strategies. Privacy advocates have called for platforms to use clearer language in privacy policies, provide real-time and accessible notifications about changes, and introduce transparency dashboards.<sup>72</sup>

By adopting these strategies, platforms like Instagram can address the ethical and practical shortcomings of their current approaches to privacy policies and ToS agreements. Simplifying legal language, minimizing the use of dark patterns, and offering real-time, detailed notifications about policy changes are critical steps toward fostering an ethical, user-informed environment in the digital space. Ultimately, greater transparency in these agreements is not just a regulatory requirement but a crucial aspect of building trust between users and social media platforms.

## 3.2 Evaluation of Instagram's Compliance with GDPR and Canadian Privacy Laws

The GDPR and PIPEDA establish rigorous requirements for safeguarding user privacy. These frameworks emphasize principles such as transparency, meaningful consent, data minimization,

---

<sup>71</sup> Nico Ebert, Kurt Alexander Ackermann & Björn Scheppeler, "Bolder is Better: Raising User Awareness through Salient and Concise Privacy Notices" (2021), *arXiv preprint*, online: *arXiv* <https://arxiv.org/abs/2101.08021>.

<sup>72</sup> Canadian Public Administration, "Transparency Dashboards for Enhanced Privacy Practices," 2023, online: <https://www.cdmrn.ca>.



and user rights regarding access and deletion of personal information. As a globally operating platform, Instagram must navigate these regulatory standards to ensure compliance while protecting user rights. Despite notable efforts, challenges remain in fully aligning with these legal frameworks.

Transparency is a cornerstone of both GDPR and PIPEDA. GDPR mandates that platforms disclose how user data is collected, processed, and shared, while PIPEDA emphasizes that consent must be meaningful, ensuring users understand the purpose and scope of data collection. Instagram attempts to meet these requirements through its privacy policies, which outline its data practices in its Terms of Service (ToS). However, the complexity and length of these documents pose significant barriers to user comprehension.

Research demonstrates that dense legal language in privacy policies often leads to uninformed consent. For instance, Waldman's article in the *Washington Law Review*, "Cognitive Biases, Dark Patterns, and the 'Privacy Paradox,'" highlights how complex terms prevent users from fully understanding the implications of their agreement.<sup>73</sup> This lack of clarity directly conflicts with GDPR's transparency obligations (Article 12) and PIPEDA's emphasis on user autonomy, exposing gaps in Instagram's efforts to ensure informed consent.

Moreover, Instagram employs "bundled consent," requiring users to accept all terms as a precondition for platform access. This practice contravenes GDPR's Article 7, which requires consent to be freely given, specific, and informed. While Instagram has made strides in providing opt-out options for personalized advertising and third-party data sharing, critics argue that these measures fall short of the granular consent required under both GDPR and PIPEDA.<sup>74</sup>

---

<sup>73</sup> Ari Waldman, "Cognitive Biases, Dark Patterns, and the 'Privacy Paradox,'" *Washington Law Review* (2022), online: <https://heinonline.org>.

<sup>74</sup> Lilian Edwards, "Data Protection: Enter the General Data Protection Regulation" in *Law, Policy and the Internet* (Oxford: Hart Publishing, 2018).

Data minimization, a core principle of GDPR, requires platforms to limit data collection to what is necessary for specific purposes. Similarly, PIPEDA mandates that organizations collect only the information required to fulfill identified purposes. Instagram’s data collection practices, however, have been criticized for exceeding these boundaries. The platform collects extensive data, including user engagement metrics, behavioral patterns, and even off-platform activities, ostensibly to improve user experiences through personalized recommendations and targeted advertising.

Critics argue that these practices may violate GDPR’s data minimization principles, as much of the data collected is not essential for Instagram’s stated purposes. Edwards, in *Data Protection Law and Practice*, emphasizes that collecting data beyond disclosed purposes undermines the fundamental tenets of GDPR, especially when users remain unaware of the full extent of data collection.<sup>75</sup> Similarly, PIPEDA requires that data collection be reasonable, raising questions about whether Instagram’s practices align with Canadian privacy standards.

Both GDPR and PIPEDA enshrine users’ rights to access, rectify, and delete their personal data. Instagram provides tools that allow users to download their data and delete their accounts, which aligns with these regulatory requirements. However, concerns persist regarding the platform’s data retention and deletion practices.

Studies indicate that social media platforms, including Instagram, often retain certain user data for internal purposes, even after account deletion. This practice undermines GDPR’s “right to be forgotten” (Article 17), which requires that personal data be erased upon request. Similarly, PIPEDA mandates that organizations dispose of personal information appropriately when it is no

---

<sup>75</sup> Ibid.

longer required. Retaining user data without their knowledge or consent violates these expectations and creates potential risks to user privacy.

Ensuring robust data security is another critical requirement under GDPR and Canadian privacy laws. These regulations demand that organizations implement technical and organizational measures to protect personal data from unauthorized access, breaches, and loss. Instagram has enhanced its security protocols through measures such as encryption and multi-factor authentication. However, its parent company, Meta, has faced high-profile data breaches that raise questions about the adequacy of these measures.

For example, the 2019 Facebook breach exposed data from over 530 million users, revealing significant vulnerabilities in Meta's security infrastructure.<sup>76</sup> While GDPR imposes severe penalties for such breaches, including fines of up to €20 million or 4% of global annual turnover, these incidents suggest that Instagram's security practices require further strengthening to fully meet regulatory standards. Similarly, PIPEDA's requirements for protecting personal data highlight the need for more comprehensive safeguards to prevent unauthorized access or misuse of user information.<sup>77</sup>

While Instagram has taken steps to comply with GDPR and PIPEDA, challenges persist in achieving full transparency, data minimization, and robust user protections. Addressing these gaps will require significant refinements in the platform's data practices and policies.

- **Simplify Privacy Policies:** Instagram must make its privacy policies more accessible by eliminating complex legal jargon and using concise, user-friendly language. This would

---

<sup>76</sup> "Tool Checks Phone Numbers from Facebook Data Breach," BBC News (6 April 2021), online: BBC News <https://www.bbc.com/news/technology-56650387>.

<sup>77</sup> Office of the Privacy Commissioner of Canada, "Smart Devices and Your Privacy" (20 August 2020), online: [https://www.priv.gc.ca/en/privacy-topics/technology/02\\_05\\_d\\_72\\_iot/](https://www.priv.gc.ca/en/privacy-topics/technology/02_05_d_72_iot/).

align with GDPR's Article 12 and PIPEDA's principles of transparency and user understanding.

- **Restrict Data Collection:** Instagram should adopt stricter data minimization practices, collecting only the information necessary for specific, clearly disclosed purposes. Limiting the scope of data collection would demonstrate a commitment to GDPR and PIPEDA standards.
- **Enhance Data Deletion Practices:** The platform must ensure that all user data is fully deleted upon account closure, in compliance with GDPR's "right to be forgotten" and PIPEDA's requirements for data disposal.
- **Strengthen Security Protocols:** To prevent future breaches, Instagram should implement advanced security measures, conduct regular audits, and address vulnerabilities in its data storage and processing systems.

In conclusion, while Instagram has made efforts to align with GDPR and Canadian privacy laws, significant improvements are necessary to achieve full compliance. Addressing transparency, data minimization, and security challenges would not only strengthen the platform's regulatory adherence but also build greater trust with its global user base.

### 3.2.1 Transparency Challenges under GDPR Requirements

Transparency stands as one of the core principles of the General Data Protection Regulation (GDPR), aimed at equipping users with clear and actionable information about how their personal data is collected, processed, and shared. According to Article 12 of the GDPR, platforms such as Instagram are required to provide this information in a manner that is "concise, transparent, intelligible, and easily accessible." However, Instagram's complex data practices and its global user base present substantial challenges to meeting these obligations.

Instagram's data-sharing practices with third parties further exacerbate transparency challenges. GDPR Articles 13 and 14 require platforms to provide detailed information about the purposes and categories of data shared with third parties. However, Instagram's privacy policy often only provides broad descriptions, leaving users uncertain about the specific nature and extent of data sharing. Privacy advocacy groups like NOYB (None of Your Business), led by Max Schrems, have filed complaints against Instagram, arguing that this lack of specificity fails to meet GDPR's transparency standards and exposes users to potential risks associated with third-party data use.<sup>78</sup> Transparency issues also arise in Instagram's use of algorithmic profiling and behavioral targeting. GDPR Article 22 requires platforms to inform users about automated decision-making processes that significantly impact them. Despite this, Instagram offers limited disclosures about how its algorithms function, particularly in terms of content personalization and targeted advertising. Lilian Edwards, in *Data Protection Law and Practice*, notes that many platforms, including Instagram, fail to provide sufficient information about how user data influences algorithmic outputs, raising critical concerns about compliance with GDPR's requirements.<sup>79</sup> The opacity of these practices undermines user trust and leaves individuals with little understanding of how their data shapes their online experiences.

By adopting these measures, Instagram can better align with GDPR's transparency principles, strengthen user trust, and demonstrate a genuine commitment to protecting individual privacy rights in an increasingly data-driven world.

---

<sup>78</sup> NOYB, "GDPR Complaints Against Instagram's Data Sharing Practices," 2022, online: <https://noyb.eu>.

<sup>79</sup> Lilian Edwards, "Data Protection: Enter the General Data Protection Regulation" in *Law, Policy and the Internet* (Oxford: Hart Publishing, 2018).

### 3.2.2 Applicability of Canada's Privacy Act and AI Act to Instagram

The rise of social media platforms like Instagram has necessitated the development and enforcement of robust privacy and AI-related regulations globally. In Canada, the Privacy Act and the proposed Artificial Intelligence and Data Act (AI Act) are key legislative tools aimed at addressing the legal and ethical concerns surrounding the use of personal data and AI technologies. When applied to Instagram, these regulations call for enhanced transparency, accountability, and user protection.

The Privacy Act, first introduced in 1983, governs the handling of personal data by federal institutions in Canada and provides a foundational framework for data privacy in the country. When extended to private-sector entities such as Instagram, the PIPEDA becomes particularly relevant. This act requires organizations to obtain meaningful consent from users before collecting, using, or sharing their personal information. For Instagram, this includes data gathered through features like photo uploads, hashtags, location tagging, and algorithm-based user profiling. Instagram is also mandated to inform users about the purposes of data collection, ensuring transparency and accountability.<sup>80</sup> PIPEDA also emphasizes the principle of accountability. Organizations like Instagram must implement data protection policies, appoint privacy officers, and comply with audits to demonstrate adherence to privacy laws.

The Artificial Intelligence and Data Act, introduced under Bill C-27, aims to regulate AI systems in Canada by prioritizing transparency, fairness, and accountability. Instagram's use of AI for facial recognition in filters, algorithm-driven content curation, and targeted advertising positions the platform within the scope of this proposed law. The AI Act categorizes certain AI applications, such as automated decision-making systems, as high-risk, requiring entities to conduct impact

---

<sup>80</sup> Personal Information Protection and Electronic Documents Act, SC 2000, c 5.

assessments and mitigate risks of harm<sup>81</sup>. For Instagram, this means ensuring that its AI systems are explainable, unbiased, and designed to protect user privacy.<sup>82</sup>

One of the primary challenges Instagram faces under Canadian privacy laws is balancing cross-border data transfers with local regulations. As a global platform, Instagram processes data in multiple jurisdictions, often subject to varying standards. This creates challenges in ensuring Canadian users' data remains protected in compliance with PIPEDA and the AI Act<sup>83</sup>. Moreover, the complexity of Instagram's machine learning models, which are inherently opaque, adds to the difficulty of meeting the transparency requirements under these laws. Ensuring that users can understand how algorithms impact their content visibility and engagement requires significant improvements in algorithmic disclosures.<sup>84</sup>

Despite these challenges, Instagram has taken steps to improve its compliance. It has introduced tools like "Your Activity" to allow users to view and manage their data. It has also updated its privacy policies to offer greater detail about data use and has implemented consent mechanisms for certain features. However, the bundling of consent for multiple purposes and the use of complex legal language in privacy policies continue to undermine the effectiveness of these efforts<sup>85</sup>. To align with Canadian privacy laws, Instagram must simplify its privacy communications and offer users more granular control over their data preferences.<sup>86</sup>

---

<sup>81</sup> Artificial Intelligence and Data Act, Bill C-27, 1st Sess, 44th Parl, 2022.

<sup>82</sup> "The Corporate Challenges of Conforming to Data Privacy Laws," SSRN (2024), online: <https://papers.ssrn.com>.

<sup>83</sup> Ibid.

<sup>84</sup> Ruvimbo Musiyiwa, *"Influencer Marketing Is Not a Way Around the Law": Regulatory Compliance and Law Enforcement in the Canadian Social Media Influencer Field* (MA Thesis, Ryerson University & York University, 2021).

<sup>85</sup> "Privacy's Next Act," HeinOnline (2024), online: <https://heinonline.org>.

<sup>86</sup> Canadian Public Administration, "An Agenda for Responsible Technology Policy in Canada" (2023), online: <https://www.cdmrn.ca>.

Comparing Canadian privacy laws with the European Union's GDPR highlights key differences and areas where Instagram may face additional compliance challenges. For instance, GDPR mandates opt-in consent for data collection and processing, whereas PIPEDA allows implied consent under specific conditions. GDPR also introduces stringent requirements for data portability and the right to be forgotten, which are not explicitly covered under Canadian laws but align with global trends in user-centric privacy practices. To effectively address these gaps, Instagram must adopt global best practices, particularly in areas like algorithmic transparency and user empowerment.

The ethical implications of Instagram's data practices extend beyond legal compliance. The platform's recommendation algorithms have been criticized for amplifying harmful content, such as unrealistic beauty standards and misinformation<sup>87</sup>. Facial recognition technology used in features like augmented reality filters also raises ethical concerns about surveillance and consent. Addressing these issues requires Instagram to incorporate ethical principles into its AI systems, such as fairness, inclusivity, and accountability<sup>88</sup>. The AI Act's emphasis on ethical AI design offers a framework for mitigating these risks and fostering trust among users.

To enhance compliance with Canada's Privacy Act and AI Act, Instagram should implement a series of improvements. First, it must ensure its privacy policies are written in plain language, making them accessible to all users. Second, the platform should provide detailed explanations of how its algorithms function, enabling users to make informed decisions about their engagement. Third, Instagram should offer more robust user controls for managing data preferences, such as

---

<sup>87</sup> Privacy in Perspective," Arcabc.ca (2024), online: <https://arcabc.ca>.

<sup>88</sup>Celia Fernández-Aller & B Pérez-Acuña, *Facebook and Artificial Intelligence: A Review of Good Practices* (2022), online: [https://www.researchgate.net/profile/Celia-Fernandez-Aller-2/publication/365275674\\_Facebook\\_and\\_Artificial\\_Intelligence\\_A\\_Review\\_of\\_Good\\_Practices/links/636cee2f54eb5f547cbe938c/Facebook-and-Artificial-Intelligence-A-Review-of-Good-Practices.pdf](https://www.researchgate.net/profile/Celia-Fernandez-Aller-2/publication/365275674_Facebook_and_Artificial_Intelligence_A_Review_of_Good_Practices/links/636cee2f54eb5f547cbe938c/Facebook-and-Artificial-Intelligence-A-Review-of-Good-Practices.pdf).



opting out of specific data uses or ad targeting. Fourth, the platform should conduct regular audits of its AI systems to identify and address potential biases or risks<sup>89</sup>.

Ultimately, the applicability of Canada's Privacy Act and AI Act to Instagram highlights the importance of regulatory frameworks in protecting user rights and fostering ethical innovation. While Instagram has made progress in aligning with these laws, significant gaps remain in areas like algorithmic transparency, user consent, and ethical AI practices. Addressing these gaps will require a collaborative effort between regulators, platforms, and users to promote a safer and more transparent digital ecosystem.

### 3.3 Analysis of User Awareness and Understanding of Data Use

User awareness and understanding of data use remain critical concerns for platforms like Instagram, especially under the regulatory frameworks of the GDPR and PIPEDA. Despite the platform's efforts to increase transparency, studies consistently show that users struggle to fully comprehend Instagram's data practices, raising questions about the adequacy of informed consent and the ethical implications of its operations.

While most Instagram users are aware that their data is being collected, they often lack a comprehensive understanding of the full extent of these practices. Many users recognize that their interactions, such as likes, comments, and browsing activity on the platform, are tracked. However, fewer users are aware of more sophisticated data collection methods, such as off-platform tracking, geolocation data, and behavioral profiling used for targeted advertising and content

---

<sup>89</sup> Cynthia Khoo, Kate Robertson & Ron Deibert, *Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications* (2019), online: Citizen Lab <https://citizenlab.ca>.

recommendations.<sup>90</sup> Research by Pew highlights that this gap in awareness leaves users vulnerable to data practices they might not fully consent to or approve of.

Instagram's use of machine learning and AI for content curation and targeted advertising is a major driver of user engagement, but the intricacies of these processes are opaque to most users. While users may notice personalized content in their feeds, the underlying mechanisms, such as data aggregation, profiling, and automated decision-making, are unclear. Under GDPR Article 22, platforms are required to inform users about the significant impacts of automated decision-making. However, Instagram's limited disclosures fail to adequately address how user data is processed by algorithms, contributing to a lack of understanding about the role these systems play in shaping their experiences on the platform.

A significant portion of Instagram users are unaware of the extent to which their personal data is shared with third parties, including advertisers and data brokers. Instagram's privacy policy mentions data sharing in broad terms, but the lack of specificity about the recipients, categories of data shared, and purposes for sharing leaves users uncertain about the potential implications of these practices. Studies by privacy advocacy groups like NOYB have revealed that many users are uninformed about how their data is monetized or repurposed outside the platform, undermining the transparency principles enshrined in GDPR Articles 13 and 14.<sup>91</sup>

Instagram offers several privacy settings to allow users to control certain aspects of data collection and usage. However, the effectiveness of these tools depends on users' ability to locate and configure them appropriately. Reports from the Norwegian Consumer Council have identified

---

<sup>90</sup> H Tran, *Understanding User Information Behaviour: An Analysis of Data Protection Measures on Digital Platforms* (2024), online: [https://www.doria.fi/bitstream/handle/10024/189268/tran\\_han.pdf?sequence=3](https://www.doria.fi/bitstream/handle/10024/189268/tran_han.pdf?sequence=3).

<sup>91</sup> NOYB, "Pinterest Pins Users' Data Down - Without Consent!" (2024), online: <https://noyb.eu/en/pinterest-pins-users-data-down-without-consent>.

significant challenges with Instagram’s privacy settings, noting that many key controls are buried within multiple submenus, making them difficult to find. Moreover, interface designs that subtly guide users toward less privacy-friendly options, commonly called “dark patterns,” have further complicated user engagement with privacy controls.<sup>92</sup> Many users unknowingly consent to extensive data processing without realizing they could limit these practices through available settings.

Privacy policies and terms of service are the primary mechanisms through which Instagram communicates its data practices to users. However, these documents are often dense, lengthy, and filled with technical and legal jargon, rendering them inaccessible to the majority of users. This lack of comprehension undermines the principle of informed consent and raises ethical concerns about whether users can truly make autonomous decisions regarding their data.

Many Instagram users perceive the platform’s data practices as limited to basic functionalities like ad targeting or content recommendations. However, in reality, the platform engages in extensive profiling and data sharing with third parties, often for purposes users may not anticipate. This gap between user perceptions and actual practices erodes trust and exposes users to risks they are unlikely to be aware of, such as potential misuse of their data by external entities.

Through this analysis, it is evident that Instagram’s current efforts to inform users about its data practices are insufficient in achieving genuine transparency and fostering a robust understanding among its users. These deficiencies highlight the need for continued examination and refinement of the platform’s communication strategies and privacy mechanisms.

---

<sup>92</sup> Lilian Edwards, *The EU AI Act: A Summary of Its Significance and Scope* (2021), online: Ada Lovelace Institute <https://adalovelaceinstitute.org>.

### 3.4 Conclusion:

To conclude this chapter, Instagram's journey towards greater transparency in data practices is emblematic of the broader challenges social media platforms face in the age of digital accountability. Despite commendable efforts to align with frameworks like GDPR and PIPEDA, substantial gaps remain in bridging the divide between legal compliance and genuine user comprehension. This chapter has underscored the intricacies of Instagram's transparency initiatives, highlighting areas where its policies, consent mechanisms, and privacy settings fall short of fostering meaningful user empowerment.

Critical areas of improvement, including simplifying privacy policies, offering granular consent options, and enhancing disclosures around algorithmic operations, are essential to achieving not only compliance but also ethical responsibility. The pervasive challenges of user disengagement, bundled consent, and complex legal language highlight the need for more user-centric approaches that prioritize trust and accessibility.

Ultimately, Instagram's ability to enhance transparency, ensure ethical AI usage, and uphold user rights hinges on its willingness to transcend mere regulatory adherence. By fostering a genuine culture of accountability and trust, Instagram can not only comply with legal mandates but also redefine the standard for ethical data practices in the digital age. This chapter illustrates that while progress has been made, significant strides are still needed to achieve a fully transparent, ethical, and user-focused data environment.

## Chapter 4: Comparative Analysis of Social Media Platforms

Social media platforms have emerged as indispensable tools for modern communication, reshaping how information is disseminated, consumed, and acted upon. With their unparalleled global reach and diverse functionalities, these platforms have profoundly influenced societal, political, and economic domains, fostering innovative modes of interaction and collaboration. However, the simultaneous proliferation of distinct platforms, each with unique characteristics, target audiences, and strategic goals, demands an in-depth comparative analysis to appreciate their individual and collective impacts.

This chapter examines the distinguishing features of leading social media platforms, analyzing their technological infrastructures, user engagement models, content governance mechanisms, and broader societal implications. By drawing upon multidisciplinary insights, it explores the strengths, limitations, and unique contributions of these platforms to the broader digital ecosystem. Additionally, it investigates how they influence user behavior, facilitate information exchange, and mediate social, cultural, and political discourse.

Such a comparative approach is especially pertinent in light of rising concerns about privacy, misinformation, and the ethical deployment of technology. Platforms like Facebook, Twitter, Instagram, TikTok, and LinkedIn exhibit significant variations in their core functionalities and target demographics, which shape how individuals, organizations, and governments leverage them for communication, advocacy, and economic purposes. Understanding these distinctions is crucial for evaluating their broader societal implications.<sup>93</sup>

---

<sup>93</sup> Boyd, Danah, and Nicole B. Ellison, "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication* 13, no. 1 (2007): 210–30. Accessible at: <https://academic.oup.com/jcmc/article/13/1/210/4582991>

Building on the analysis of Instagram’s transparency initiatives discussed in Chapter 3, this chapter extends the evaluation to compare its practices with other platforms like Facebook and TikTok. The findings presented in this chapter are informed by a combination of recent academic literature, industry reports, and empirical analyses. This multidisciplinary approach draws on perspectives from communication studies, sociology, and information systems to deliver a nuanced understanding of the comparative dynamics of social media platforms. It concludes by synthesizing key insights, offering critical perspectives on their future evolution, and discussing their potential to foster a more equitable, ethical, and innovative digital environment.<sup>94</sup>

## 4.1 Common Transparency and Compliance Issues Across Platforms

Social media platforms are integral to the digital communication ecosystem, yet they are frequently scrutinized for persistent transparency and regulatory compliance challenges. These challenges encompass a range of issues, including content moderation practices, user privacy, algorithmic governance, and adherence to regulatory frameworks. Addressing these concerns is vital to building more accountable and trustworthy digital environments.

Platforms like Instagram illustrate the complexities of implementing transparency policies that comply with regulatory frameworks like GDPR while remaining comprehensible to users, as discussed in the previous chapter. Platforms often face criticism for their opaque processes when removing content or banning accounts. These inconsistencies and unclear policies have drawn accusations of bias and unfairness, particularly when dealing with politically sensitive or harmful material. For instance, research highlights recurring disparities in how platforms apply their

---

<sup>94</sup> Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (New Haven: Yale University Press, 2018).

content guidelines, often leading to debates over censorship and freedom of expression.<sup>95</sup> The widespread use of automated tools for moderation further complicates matters, as these systems frequently misinterpret context, resulting in unwarranted content removal.<sup>96</sup>

User privacy emerges as another critical area of concern. Most social media platforms depend on extensive data collection to fuel their business models, sparking debates over consent, ethical data use, and data security. Despite landmark regulations like the GDPR, many platforms struggle to comply, often facing legal challenges over mishandled user information.<sup>97</sup> Recent studies also indicate that users remain skeptical about the adequacy of current privacy safeguards, amplifying calls for reform.<sup>98</sup>

The opacity of algorithmic systems presents a third major concern. Similar to YouTube and Facebook, Instagram's algorithms for personalized content recommendations present challenges of opacity and bias. As analyzed in Chapter 3, Instagram provides limited disclosures about its AI-driven decision-making processes, which aligns with broader concerns across platforms, thereby shaping public opinion, engagement trends, and even societal discourse. However, their mechanisms remain largely hidden, making it difficult for users and regulators to understand or

---

<sup>95</sup> R Jain and S Mehta, “A History of Transparency Regulations: Interdisciplinary Strategies for Shaping Social Media Regulation and Self-Governance” (2024), ACM Digital Library, online: <https://dl.acm.org/doi/abs/10.1145/3657054.3657157>.

<sup>96</sup> M MacCarthy, “Transparency Requirements for Digital Social Media Platforms: Recommendations for Policy Makers” (2020), Annenberg Public Policy Center, online: [https://cdn.annenbergpublicpolicycenter.org/wp-content/uploads/2020/06/Transparency\\_TWG\\_MacCarthy\\_Feb\\_2020.pdf](https://cdn.annenbergpublicpolicycenter.org/wp-content/uploads/2020/06/Transparency_TWG_MacCarthy_Feb_2020.pdf).

<sup>97</sup> R Gorwa and TG Ash, “Democratic Transparency in the Platform Society” in *Social Media and Democracy: The State of the Field* (2020), online: <https://osf.io/preprints/socarxiv/ehcy2/download>.

<sup>98</sup> S Dreyer and L Ziebarth, “Participatory Transparency in Social Media Governance: Combining Two Good Practices” (2014), *Journal of Information Policy*, online: [https://scholarlypublishingcollective.org/psup/information-policy/article-pdf/doi/10.5325/jinfopoli.4.2014.0529/1610688/jinfopoli\\_4\\_2014\\_529.pdf](https://scholarlypublishingcollective.org/psup/information-policy/article-pdf/doi/10.5325/jinfopoli.4.2014.0529/1610688/jinfopoli_4_2014_529.pdf).

challenge biases embedded in these systems.<sup>99</sup> For example, platforms like YouTube and TikTok have faced criticism for amplifying divisive or sensational content, raising questions about their role in polarizing public opinion. Efforts to address these issues, such as publishing transparency reports, often fall short due to a lack of actionable detail.<sup>100</sup>

Regulatory compliance represents an additional hurdle. While some jurisdictions have imposed stricter measures to combat misinformation, hate speech, and privacy breaches, enforcement often remains inconsistent. Platforms frequently adopt reactive measures, such as making policy adjustments after legal challenges, rather than implementing proactive reforms.<sup>101</sup> The disparity in regulatory frameworks across regions further complicates compliance, with platforms struggling to adapt their practices to meet diverse legal requirements. Notably, the European Union's Digital Services Act is seen as a model for fostering greater accountability, but global implementation remains uneven.<sup>102</sup>

This section explores these pervasive challenges, offering a foundation for understanding the complexities of transparency and compliance in social media ecosystems. By delving into case studies and platform-specific practices, the analysis sheds light on both systemic issues and potential pathways for reform. The subsequent recommendations will aim to provide actionable

---

<sup>99</sup> P Leerssen, "The Soap Box as a Black Box: Regulating Transparency in Social Media Recommender Systems" (2020), *European Journal of Law and Technology*, online: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3544009](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3544009).

<sup>100</sup> A Urman and M Makhortykh, "How Transparent Are Transparency Reports? Comparative Analysis of Transparency Reporting Across Online Platforms" (2023), *Telecommunications Policy*, online: <https://www.sciencedirect.com/science/article/pii/S0308596122001793>.

<sup>101</sup> M MacCarthy, "Transparency Requirements for Digital Social Media Platforms: Recommendations for Policy Makers" (2020), Annenberg Public Policy Center, online: [https://cdn.annenbergpublicpolicycenter.org/wp-content/uploads/2020/06/Transparency\\_TWG\\_MacCarthy\\_Feb\\_2020.pdf](https://cdn.annenbergpublicpolicycenter.org/wp-content/uploads/2020/06/Transparency_TWG_MacCarthy_Feb_2020.pdf).

<sup>102</sup> European Commission, "The Digital Services Act Package," European Commission, 2022, online: <https://ec.europa.eu>.



strategies for fostering greater accountability, improving user trust, and ensuring adherence to ethical and regulatory standards.

#### 4.1.1 Facebook: Transparency and Compliance Practices

As one of the most prominent social media platforms globally, Facebook, now operating under its parent company Meta Platforms, Inc., often finds itself under intense scrutiny regarding transparency and compliance. With billions of active users and significant societal influence, the platform's policies and practices are pivotal to maintaining public trust and meeting international regulatory requirements. However, Facebook's operations have been marred by repeated controversies, particularly in its handling of user data, content moderation, and algorithmic governance.

To manage its vast user base and diverse content, Facebook employs Community Standards designed to outline acceptable user behavior and permissible content. These guidelines are enforced through a combination of artificial intelligence (AI) tools and human moderators. Yet, the platform has faced criticism for the opacity of its decision-making processes, particularly in cases involving the removal of controversial posts or suspension of accounts. For example, critics argue that Facebook's criteria for enforcement are inconsistently applied, leading to allegations of political bias and arbitrary rulings.<sup>103</sup> Instances of high-profile account suspensions have intensified these accusations, highlighting the need for greater transparency in moderation practices.

---

<sup>103</sup> R Jain and S Mehta, "A History of Transparency Regulations: Interdisciplinary Strategies for Shaping Social Media Regulation and Self-Governance" (2024), ACM Digital Library, online: <https://dl.acm.org/doi/abs/10.1145/3657054.3657157>.

The Cambridge Analytica scandal serves as a defining moment in Facebook's history, exposing its vulnerabilities in protecting user data and igniting global debates on privacy in the digital age.<sup>104</sup> While Facebook has since implemented reforms, including enhanced transparency in data collection and compliance with the GDPR, skeptics argue that its privacy policies still fall short of user expectations. For example, Facebook's transparency reports, which disclose government data requests and the number of accounts affected, have been criticized for lacking actionable detail. Such gaps perpetuate public distrust and fuel ongoing legal challenges regarding data misuse.<sup>105</sup> Facebook's algorithms, designed to curate personalized content for users, represent another contentious area. These systems influence what appears in users' newsfeeds, shaping public discourse and engagement patterns. However, the platform has faced criticism for its limited disclosure about how these algorithms operate. While initiatives such as the "Widely Viewed Content Report" aim to provide insights, researchers argue that selective reporting fails to address concerns about algorithmic amplification of harmful or polarizing content. This lack of clarity not only undermines accountability but also raises broader questions about the ethical use of algorithmic systems.<sup>106</sup>

In response to increasing legal pressures, Facebook has taken steps to align its practices with regional regulations such as the GDPR and the European Union's Digital Services Act.<sup>107</sup> These

---

<sup>104</sup> R Gorwa and TG Ash, "Democratic Transparency in the Platform Society" in *Social Media and Democracy: The State of the Field* (2020), online: <https://osf.io/preprints/socarxiv/ehcy2/download>.

<sup>105</sup> P Leerssen, "The Soap Box as a Black Box: Regulating Transparency in Social Media Recommender Systems" (2020), *European Journal of Law and Technology*, online: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3544009](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3544009).

<sup>106</sup> A Urman and M Makhortykh, "How Transparent Are Transparency Reports? Comparative Analysis of Transparency Reporting Across Online Platforms" (2023), *Telecommunications Policy*, online: <https://www.sciencedirect.com/science/article/pii/S0308596122001793>.

<sup>107</sup> European Commission, "The Digital Services Act Package," European Commission, 2022, online: <https://ec.europa.eu>.

measures include introducing user-friendly tools for managing data preferences and publishing transparency reports. However, critics argue that Facebook often adopts reactive approaches, addressing compliance issues only after legal or public backlash. For instance, tools designed to enhance user control over ads and data settings are frequently criticized as being overly complex, limiting their effectiveness in fostering user trust. These challenges underscore the need for Facebook to prioritize proactive rather than reactive compliance strategies.<sup>108</sup>

While Facebook has made strides in areas such as content moderation and data privacy, significant gaps remain. These persistent issues highlight the need for stronger regulatory oversight and a more committed approach to ethical governance. As Facebook continues to evolve, addressing these challenges will be crucial for restoring public confidence and ensuring long-term accountability.

#### 4.1.2 TikTok: Handling User Data and Transparency Challenges

TikTok, operated by ByteDance, has rapidly emerged as one of the most popular social media platforms worldwide, particularly among younger users. Despite its exponential growth and widespread appeal, the platform has attracted intense scrutiny over its data handling practices, content moderation mechanisms, and compliance with international transparency standards. This section examines TikTok's ongoing challenges in managing user data and transparency, exploring the controversies, regulatory responses, and areas for improvement.

TikTok's approach to data collection has raised significant privacy concerns globally. The platform gathers extensive user information, including behavioral patterns, location details, and device

---

<sup>108</sup> E Goldman, "The Constitutionality of Mandating Editorial Transparency" (2022), *Hastings LJ*, online: <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=4005647>.

metadata, raising questions about user consent and data security.<sup>109</sup> These practices have led to investigations in several jurisdictions. In the United States, for instance, TikTok faced accusations of transferring user data to servers in China, sparking debates over potential national security risks.<sup>110</sup> Although the platform now claims to store U.S. user data domestically, skepticism persists due to the lack of robust, independent verification mechanisms. Furthermore, regulatory bodies, including the European Data Protection Board, have highlighted gaps in TikTok's adherence to privacy regulations like the GDPR.<sup>111</sup>

TikTok's content moderation policies, particularly those powered by its algorithm-driven recommendation system, have also drawn criticism. The platform has been accused of suppressing politically sensitive posts and promoting harmful or inappropriate content through opaque mechanisms.<sup>112</sup> For example, while TikTok's Community Guidelines provide an overview of prohibited content, the lack of detailed enforcement explanations has led to widespread dissatisfaction among users.<sup>113</sup> Reports frequently cite inconsistencies in content removal decisions and inadequate communication regarding account suspensions or video takedowns,

---

<sup>109</sup> R Gorwa and TG Ash, "Democratic Transparency in the Platform Society" in *Social Media and Democracy: The State of the Field* (2020), online: <https://osf.io/preprints/socarxiv/ehcy2/download>.

<sup>110</sup> N Just and F Saurwein, "Enhancing Social Media Regulation through Transparency: Examining the New Transparency Regime in the EU" (2024), online: [https://www.zora.uzh.ch/id/eprint/257668/1/Just\\_Saurwein\\_2024\\_Enhancing\\_Social\\_Media\\_Regulation\\_through\\_Transparency\\_Examining\\_the\\_New\\_Transparency\\_Regime\\_in\\_the\\_EU.pdf](https://www.zora.uzh.ch/id/eprint/257668/1/Just_Saurwein_2024_Enhancing_Social_Media_Regulation_through_Transparency_Examining_the_New_Transparency_Regime_in_the_EU.pdf).

<sup>111</sup> European Data Protection Board, "GDPR Compliance and Social Media Platforms" (2022), online: <https://edpb.europa.eu>.

<sup>112</sup> M MacCarthy, "Transparency Requirements for Digital Social Media Platforms: Recommendations for Policy Makers" (2020), Annenberg Public Policy Center, online: [https://cdn.annenbergpublicpolicycenter.org/wp-content/uploads/2020/06/Transparency\\_TWG\\_MacCarthy\\_Feb\\_2020.pdf](https://cdn.annenbergpublicpolicycenter.org/wp-content/uploads/2020/06/Transparency_TWG_MacCarthy_Feb_2020.pdf).

<sup>113</sup> P Leerssen, "The Soap Box as a Black Box: Regulating Transparency in Social Media Recommender Systems" (2020), *European Journal of Law and Technology*, online: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3544009](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3544009).

which erodes trust and accountability. Additionally, the platform has faced allegations of algorithmic bias, with critics arguing that its recommendation system amplifies misinformation and polarizing narratives.<sup>114</sup>

In response to mounting criticism, TikTok has implemented several initiatives aimed at enhancing transparency. The introduction of its Transparency Center represents a notable effort to provide insights into the platform's content moderation policies, data handling practices, and government cooperation processes.<sup>115</sup> TikTok has also begun publishing transparency reports, offering data on content removals and regulatory compliance. However, critics argue that these measures, while a step forward, lack depth and fail to address systemic challenges effectively. For example, the reports often omit details about the platform's regional practices, leaving questions about the consistency of its compliance efforts across different jurisdictions.<sup>116</sup>

The platform's regulatory challenges span multiple jurisdictions. In the European Union, TikTok has been compelled to align its practices with the GDPR, which mandates stricter data privacy protections and user consent mechanisms.<sup>117</sup> In contrast, countries such as India have adopted more drastic measures, banning TikTok entirely over concerns about data privacy and national security. These developments underscore the urgent need for TikTok to adopt proactive compliance

---

<sup>114</sup> A Urman and M Makhortykh, "How Transparent Are Transparency Reports? Comparative Analysis of Transparency Reporting Across Online Platforms" (2023), *Telecommunications Policy*, online: <https://www.sciencedirect.com/science/article/pii/S0308596122001793>.

<sup>115</sup> ByteDance, "TikTok Transparency Center," TikTok, online: <https://www.tiktok.com/transparency>.

<sup>116</sup> N Just and F Saurwein, "Enhancing Social Media Regulation through Transparency: Examining the New Transparency Regime in the EU" (2024), online: [https://www.zora.uzh.ch/id/eprint/257668/1/Just\\_Saurwein\\_2024\\_Enhancing\\_Social\\_Media\\_Regulation\\_through\\_Transparency\\_Examining\\_the\\_New\\_Transparency\\_Regime\\_in\\_the\\_EU.pdf](https://www.zora.uzh.ch/id/eprint/257668/1/Just_Saurwein_2024_Enhancing_Social_Media_Regulation_through_Transparency_Examining_the_New_Transparency_Regime_in_the_EU.pdf).

<sup>117</sup> European Data Protection Board, "GDPR Compliance and Social Media Platforms" (2022), online: <https://edpb.europa.eu>.

strategies that address not only regulatory mandates but also public concerns. Without substantial reforms, the platform risks further erosion of user trust and intensified regulatory scrutiny.

This section highlights the critical issues TikTok faces in managing user data and ensuring transparency. While the platform has taken notable steps to address these challenges, such as introducing transparency tools and publishing reports, significant gaps remain. To enhance trust and accountability, TikTok must implement more robust, globally consistent strategies that go beyond reactive measures. A comprehensive approach is essential for maintaining its position as a leading social media platform while navigating the complex regulatory landscape.

#### 4.1.3 YouTube: Data Use and Ad Targeting

YouTube, a subsidiary of Google (Alphabet Inc.), is a dominant force in the digital advertising landscape, leveraging sophisticated data collection and ad-targeting technologies. As a platform catering to billions of users worldwide, YouTube has become central to how video content is shared and consumed. However, its practices around data use and advertisement targeting have sparked ongoing debates regarding transparency, privacy, and ethical accountability.

YouTube's operational model relies on extensive data collection, encompassing user activities such as viewing histories, search queries, location information, and device metadata.<sup>118</sup> This data is pivotal for refining personalized recommendations and optimizing ad-targeting efficiency. However, such practices have raised significant concerns about user consent and the potential misuse of collected data. Critics argue that YouTube's data policies are often opaque, leaving users unaware of the breadth and depth of the information being harvested.<sup>119</sup> Recent reports have

---

<sup>118</sup> R Gorwa and TG Ash, "Democratic Transparency in the Platform Society" in *Social Media and Democracy: The State of the Field* (2020), online: <https://osf.io/preprints/socarxiv/ehcy2/download>.

<sup>119</sup> A Urman and M Makhortykh, "How Transparent Are Transparency Reports? Comparative Analysis of Transparency Reporting Across Online Platforms" (2023), *Telecommunications Policy*, online: <https://www.sciencedirect.com/science/article/pii/S0308596122001793>.

highlighted a gap between users' understanding of privacy settings and the actual extent of data collection, exacerbating public distrust.<sup>120</sup>

The platform's advertising model is heavily reliant on personalized targeting, which utilizes algorithms to deliver customized ads to users. While this approach has been highly effective in maximizing advertiser returns and enhancing user engagement, it has also raised ethical questions regarding privacy and data protection.<sup>121</sup> For instance, YouTube has faced allegations of violating the Children's Online Privacy Protection Act (COPPA) in the United States by targeting ads at children without adequate safeguards.<sup>122</sup> In 2019, the Federal Trade Commission (FTC) imposed a \$170 million fine on Google for these violations, underscoring the need for stricter oversight of YouTube's practices.<sup>123</sup> These incidents highlight the tension between commercial priorities and ethical responsibilities.

In recent years, YouTube has introduced initiatives aimed at improving transparency in its advertising practices. For example, the Ad Transparency Center offers users tools to understand and manage their ad preferences, providing explanations for why specific ads are displayed.<sup>7</sup> However, despite these advancements, concerns persist about the opacity of YouTube's ad algorithms.<sup>8</sup> Critics argue that the platform's transparency measures lack the depth necessary to

---

<sup>120</sup> L DeNardis and AM Hackl, "Internet Governance by Social Media Platforms" (2015), *Telecommunications Policy*, online: <https://www.isidl.com/wp-content/uploads/2017/08/E4561-ISIDL.pdf>.

<sup>121</sup> S Dreyer and L Ziebarth, "Participatory Transparency in Social Media Governance: Combining Two Good Practices" (2014), *Journal of Information Policy*, online: [https://scholarlypublishingcollective.org/psup/information-policy/article-pdf/doi/10.5325/jinfopoli.4.2014.0529/1610688/jinfopoli\\_4\\_2014\\_529.pdf](https://scholarlypublishingcollective.org/psup/information-policy/article-pdf/doi/10.5325/jinfopoli.4.2014.0529/1610688/jinfopoli_4_2014_529.pdf).

<sup>122</sup> Federal Trade Commission, "FTC Imposes \$170 Million Penalty on Google for YouTube COPPA Violations" (2019), online: <https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-pay-record-170-million-alleged-violations-childrens-privacy-law>.

<sup>123</sup> P Leerssen, "The Soap Box as a Black Box: Regulating Transparency in Social Media Recommender Systems" (2020), *European Journal of Law and Technology*, online: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3544009](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3544009).

enable meaningful user oversight, as they fail to disclose how algorithmic decisions are made or why certain content types are prioritized.<sup>124</sup>

YouTube operates in a fragmented regulatory environment, facing diverse legal requirements across jurisdictions. In the European Union, for instance, the platform has adjusted its practices to comply with the GDPR, which enforces stricter rules on data privacy and user consent. However, in regions like the United States, where regulatory frameworks are less cohesive, enforcement remains inconsistent. This disparity creates challenges for YouTube's global operations, particularly in maintaining uniform compliance standards while addressing region-specific concerns. Critics have called for a more proactive approach to regulatory adherence, emphasizing the need for global alignment in privacy and advertising practices.<sup>125</sup>

]While YouTube has made progress in enhancing transparency and user protections, significant gaps remain. Addressing these issues will require not only stricter regulatory oversight but also a genuine commitment by YouTube to prioritize ethical considerations over short-term commercial gains. Moving forward, strengthening user trust through greater transparency and accountability will be critical for sustaining YouTube's position as a leading digital platform.

## 4.2 Comparative Findings and Insights

Social media platforms operate within a dynamic and evolving digital landscape characterized by varying levels of transparency, compliance, and ethical governance. This section synthesizes findings from the analysis of Facebook, TikTok, and YouTube, highlighting recurring challenges

---

<sup>124</sup> E Goldman, "The Constitutionality of Mandating Editorial Transparency" (2022), *Hastings LJ*, online: <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=4005647>.

<sup>125</sup> N Just and F Saurwein, "Enhancing Social Media Regulation through Transparency: Examining the New Transparency Regime in the EU" (2024), online: [https://www.zora.uzh.ch/id/eprint/257668/1/Just\\_Saurwein\\_2024\\_Enhancing\\_Social\\_Media\\_Regulation\\_through\\_Transparency\\_Examining\\_the\\_New\\_Transparency\\_Regime\\_in\\_the\\_EU.pdf](https://www.zora.uzh.ch/id/eprint/257668/1/Just_Saurwein_2024_Enhancing_Social_Media_Regulation_through_Transparency_Examining_the_New_Transparency_Regime_in_the_EU.pdf).



and critical insights into their practices. The comparative analysis concentrates on three primary dimensions: data privacy, content moderation, and algorithmic functionality transparency.

Data privacy continues to be a pervasive concern across all platforms. Facebook, TikTok, and YouTube rely extensively on user data for personalization and monetization, yet they consistently face criticism over how they handle such data. Facebook, for example, has come under fire for its history of data breaches and inadequate adherence to privacy regulations, including the GDPR.<sup>126</sup> Similarly, TikTok has drawn significant scrutiny over allegations of sharing user data with Chinese authorities, raising questions about national security and user consent.<sup>127</sup> Meanwhile, YouTube's extensive data collection practices, particularly for personalized advertising, have sparked controversy, especially in cases involving violations of children's privacy protections, as seen in its COPPA-related settlement with the FTC.<sup>128</sup> These challenges underscore the ongoing tension between data-driven business models and user privacy expectations.

The comparative analysis reveals significant struggles across platforms in implementing consistent and transparent content moderation policies. Facebook's reliance on a hybrid system of AI and human moderators has faced accusations of political bias and uneven enforcement.<sup>129</sup> Similarly, TikTok's algorithmic suppression of sensitive or controversial content, often based on vague

---

<sup>126</sup> R Jain and S Mehta, "A History of Transparency Regulations: Interdisciplinary Strategies for Shaping Social Media Regulation and Self-Governance" (2024), ACM Digital Library, online: <https://dl.acm.org/doi/abs/10.1145/3657054.3657157>.

<sup>127</sup> A Urman and M Makhortykh, "How Transparent Are Transparency Reports? Comparative Analysis of Transparency Reporting Across Online Platforms" (2023), *Telecommunications Policy*, online: <https://www.sciencedirect.com/science/article/pii/S0308596122001793>.

<sup>128</sup> Federal Trade Commission, "FTC Imposes \$170 Million Penalty on Google for YouTube COPPA Violations" (2019), online: <https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-pay-record-170-million-alleged-violations-childrens-privacy-law>.

<sup>129</sup> P Leerssen, "The Soap Box as a Black Box: Regulating Transparency in Social Media Recommender Systems" (2020), *European Journal of Law and Technology*, online: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3544009](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3544009).

guidelines, has drawn criticism for its lack of clarity and perceived bias.<sup>130</sup> On YouTube, efforts to curb the proliferation of harmful content, such as misinformation and extremist material, have been hindered by the platform's engagement-driven algorithms.<sup>131</sup> Across all platforms, a shared challenge lies in the opacity of decision-making processes related to content removal, which undermines user trust and accountability.

The issue of algorithmic opacity is a recurring theme with significant ethical and societal implications. Facebook and YouTube have both faced criticism for algorithms that amplify divisive or sensational content, often prioritizing engagement over accuracy or quality.<sup>132</sup> TikTok, while praised for its personalized recommendation system, has been criticized for fostering echo chambers and amplifying potentially harmful content.<sup>133</sup> Efforts by these platforms to increase algorithmic transparency, such as publishing reports or introducing transparency tools, are often criticized for being superficial and failing to provide actionable insights for users or regulators. This lack of substantive transparency perpetuates concerns about bias, misinformation, and accountability.

The comparative findings underscore the urgent need for enhanced transparency and ethical practices across platforms. Key insights and recommendations include:

- **Proactive Regulation:** Platforms often adopt reactive measures in response to legal or public pressure rather than implementing proactive compliance strategies. Clear regulatory

---

<sup>130</sup> S Dreyer and L Ziebarth, "Participatory Transparency in Social Media Governance: Combining Two Good Practices" (2014), *Journal of Information Policy*, online: [https://scholarlypublishingcollective.org/psup/information-policy/article-pdf/doi/10.5325/jinfopoli.4.2014.0529/1610688/jinfopoli\\_4\\_2014\\_529.pdf](https://scholarlypublishingcollective.org/psup/information-policy/article-pdf/doi/10.5325/jinfopoli.4.2014.0529/1610688/jinfopoli_4_2014_529.pdf).

<sup>131</sup> ByteDance, "YouTube Ad Transparency Center," YouTube, online: <https://www.youtube.com/transparency>.

<sup>132</sup> E Goldman, "The Constitutionality of Mandating Editorial Transparency" (2022), *Hastings LJ*, online: <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=4005647>.

<sup>133</sup> European Data Protection Board, "GDPR Compliance and Social Media Platforms" (2022), online: <https://edpb.europa.eu>.

frameworks, such as GDPR, can compel platforms to adopt better practices and align with ethical standards.<sup>134</sup>

- **User-Centric Transparency:** Providing users with clear, accessible, and actionable information about data usage and content moderation policies can help foster trust and accountability.
- **Algorithm Accountability:** Platforms should prioritize the explainability of their algorithms, enabling users and regulators to better understand and challenge automated decision-making processes.
- **Collaborative Governance:** A coordinated approach involving regulators, platform operators, and user advocacy groups is crucial for fostering a more ethical and transparent digital ecosystem.

Instagram's transparency efforts, as explored in Chapter 3, underscore the challenges of aligning user-centric transparency with compliance requirements. These insights complement the broader challenges observed in platforms like Facebook and TikTok. This comparative analysis highlights that while some strides have been made to address transparency and compliance challenges, significant gaps persist. Addressing these issues will require a combination of stricter regulatory oversight, platform-driven reforms, and active engagement with civil society. By embracing these principles, social media platforms can better navigate the complexities of the digital age while fostering a healthier, more inclusive online environment.

---

<sup>134</sup> M MacCarthy, "Transparency Requirements for Digital Social Media Platforms: Recommendations for Policy Makers" (2020), Annenberg Public Policy Center, online: [https://cdn.annenbergpublicpolicycenter.org/wp-content/uploads/2020/06/Transparency\\_TWG\\_MacCarthy\\_Feb\\_2020.pdf](https://cdn.annenbergpublicpolicycenter.org/wp-content/uploads/2020/06/Transparency_TWG_MacCarthy_Feb_2020.pdf).

## 4.3 Conclusion

This chapter's comparative insights build on the detailed evaluation of Instagram in Chapter 3, emphasizing the need for a unified approach to transparency and user empowerment across platforms. The comparative analysis of social media platforms in this chapter sheds light on the critical challenges and opportunities associated with transparency and compliance in the digital era. Platforms such as Facebook, TikTok, and YouTube operate in intricate ecosystems where data privacy, content moderation, and algorithmic governance are under growing scrutiny from users, regulators, and advocacy groups. Despite attempts to address these issues, persistent gaps in transparency, accountability, and ethical governance remain evident.

Facebook's history of data privacy breaches and inconsistent content moderation policies underscores the difficulties in balancing user engagement with ethical practices. Similarly, TikTok's rapid global expansion has been shadowed by concerns about data sharing, national security implications, and opaque algorithmic systems. Meanwhile, YouTube's extensive use of personalized ad targeting and the opacity of its recommendation algorithms continue to raise serious ethical and regulatory questions. Although all three platforms have introduced transparency initiatives, including the publication of transparency reports and the development of user-centric tools, their efforts often fall short in terms of scope and effectiveness.

A recurring theme throughout this chapter is the urgent need for proactive regulation and robust self-governance to bridge the gap between existing compliance measures and user expectations. Platforms must move beyond reactive approaches and adopt forward-looking strategies that place a greater emphasis on building trust and fostering ethical responsibility. Concurrently, regulators must ensure the rigorous enforcement of frameworks such as the General Data Protection Regulation (GDPR) and the Digital Services Act, adapting these frameworks to the rapidly evolving digital landscape.

Ultimately, fostering a more transparent and ethical digital ecosystem necessitates a collaborative effort involving platforms, regulators, and civil society. By addressing the identified gaps and adhering to the principles of transparency, accountability, and user empowerment, social media platforms can more effectively navigate the challenges of the digital age. These efforts are vital for shaping a healthier, more inclusive online environment that aligns with societal and regulatory expectations. This chapter lays the groundwork for further examination of these themes, particularly in the context of regulatory frameworks and the evolving governance of social media platforms.

## Chapter 5: Conclusion

The exploration of social media platforms, particularly Instagram, through the lens of transparency and data privacy laws, such as the GDPR and Canada's Privacy and AI Act, has provided valuable insights into the complexities of digital governance. In this thesis, I have navigated the intricate intersections of technology, regulatory frameworks, ethical obligations, and user rights, emphasizing advancements and ongoing challenges in achieving meaningful transparency. Through a critical evaluation of Instagram as a case study, the findings contribute to understanding the broader dynamics of privacy, trust, and accountability in the digital age.

### 5.1 Summary of Findings

This study underscores the pivotal role of transparency in fostering regulatory compliance, ethical governance, and user trust within social media platforms. By examining Instagram's practices, several critical dimensions have been identified:

- Data Practices and Transparency:

Instagram exemplifies the inherent tension between personalization and privacy. The platform's dependence on extensive data collection to power algorithmic content recommendations and targeted advertising highlights the challenges of achieving meaningful transparency. Tools such as privacy policies and data download features provide users with some degree of insight into data practices. However, these tools' legalistic and technical nature often renders them inaccessible to the average user. This creates a significant gap between what is disclosed and what users can genuinely comprehend, limiting their ability to make informed choices.

- Regulatory Challenges:

Despite Instagram's efforts to align with GDPR and Canadian privacy laws, there are persistent gaps in implementation. These include opaque algorithmic profiling, insufficient clarity in data-sharing disclosures, and a lack of robust mechanisms for users to exercise meaningful control over their personal data. These shortcomings not only reflect Instagram's struggles but also point to broader systemic challenges faced by social media platforms in adhering to complex regulatory requirements.

- **Comparative Perspectives:**

A comparative analysis with other platforms, including Facebook, TikTok, and YouTube, reveals common issues such as manipulative consent frameworks, algorithmic opacity, and inadequate transparency regarding data usage. This systemic lack of clarity underscores the need for industry-wide reforms to address these recurring challenges effectively. While Instagram demonstrates some initiatives toward improvement, the broader industry still grapples with similar issues, suggesting the necessity of collective efforts and shared accountability.

## 5.2 Broader Contributions

This thesis makes significant contributions to the academic discourse on digital governance, privacy regulation, and the ethical challenges posed by evolving technologies. Its findings extend beyond the specific case study of Instagram, offering insights and practical strategies that are relevant across the social media industry.

- **Advancing Academic Discourse:**

By situating Instagram's practices within the frameworks of the GDPR and Canada's Privacy and AI Act, this research deepens our understanding of how regulatory mandates are operationalized in real-world settings. It highlights the disparities between the

theoretical aspirations of privacy laws and the practical limitations faced by platforms, emphasizing the need for more research bridging law and technology.

- **Informing Industry Practices:**

The thesis provides actionable recommendations to address the transparency gaps identified in Instagram's practices. These include user-centric solutions such as real-time policy notifications, intuitive privacy settings, and enhanced algorithmic disclosures. These recommendations are not only applicable to Instagram but also offer a roadmap for other platforms grappling with similar challenges.

- **Ethical Implications:**

This research underscores the importance of transparency as a means to promote ethical digital practices. Transparency goes beyond legal compliance; it fosters trust, empowers users, and establishes accountability. By focusing on these broader ethical considerations, the study contributes to ongoing debates about the role of technology companies in society and their obligations to users.

- **Cross-Disciplinary Insights:**

The interdisciplinary nature of this thesis—encompassing legal analysis, technological critique, and ethical evaluation—provides a comprehensive framework for understanding the complexities of data privacy in social media. It encourages collaboration between regulators, technologists, and ethicists to address the challenges identified in this study.

These contributions collectively emphasize the urgency of adopting a holistic approach to transparency, one that balances compliance with ethical stewardship and prioritizes user empowerment in the evolving digital ecosystem.



## 5.3 Implications for Policy and Practice

The findings of this thesis highlight critical areas where policy and practice must evolve to address the transparency challenges faced by social media platforms. By bridging the gaps between legal requirements, platform capabilities, and user expectations, the study identifies pathways for fostering a more ethical and accountable digital ecosystem:

- Enhancing User Understanding:

Simplifying privacy policies and making them accessible through interactive tools is essential for empowering users. Platforms should adopt user-friendly interfaces that explain privacy settings, data practices, and user rights in plain language. Additionally, integrating educational campaigns into the platform experience can encourage users to actively engage with their privacy options and make informed decisions.

- Improving Algorithmic Transparency:

A key challenge lies in demystifying algorithms for users. Platforms must provide clear and accessible explanations of how algorithms operate, particularly in shaping user experiences and content delivery. Developing transparency dashboards and visual tools can help users better understand the implications of algorithmic decision-making on their data and digital interactions.

- Establishing Industry Standards:

Transparency challenges are not unique to Instagram; they reflect broader systemic issues across the social media industry. Collaborative efforts among platforms, regulators, and advocacy groups are needed to establish standardized transparency practices. Industry-wide benchmarks can ensure consistent user experiences and facilitate compliance with complex privacy regulations globally.

- Global Harmonization of Privacy Laws:

The diversity of privacy regulations across jurisdictions creates challenges for platforms operating on a global scale. Aligning practices to meet the strictest applicable standards can enhance compliance while fostering user trust. For instance, adopting GDPR's stringent requirements as a baseline could help platforms navigate fragmented legal landscapes while setting a high bar for transparency.

- Encouraging Innovation in Privacy Technologies:

Investment in privacy-enhancing technologies (PETs) can help platforms go beyond compliance and offer cutting-edge solutions that prioritize user control and data protection. Innovations such as differential privacy, homomorphic encryption, and federated learning can support transparency while minimizing risks to user data.

These policy and practice recommendations underscore the need for a multifaceted approach to transparency—one that balances technological advancements with ethical governance, legal compliance, and user empowerment. By embracing these measures, platforms like Instagram can contribute to a digital ecosystem that values privacy, fosters trust and promotes equitable access to information.

## 5.4 Limitations and Opportunities for Future Research

While this thesis provides valuable insights into the transparency challenges faced by social media platforms like Instagram, certain limitations must be acknowledged. These limitations present opportunities for future research to deepen the understanding of transparency, data privacy, and regulatory compliance in the digital ecosystem:

- Focus on a Single Platform:

This study's emphasis on Instagram, while offering in-depth insights, limits the generalizability of its findings. Future research could broaden the scope to include

comparative studies across diverse platforms, such as emerging social media networks or niche platforms, to identify variations in transparency practices and compliance strategies.

- Limited Geographical Context:

Although this thesis analyzes Instagram's compliance with GDPR and Canadian privacy laws, it does not explore the nuances of other regional frameworks, such as those in Asia or Latin America. Examining how platforms navigate these diverse regulatory environments could provide a more comprehensive understanding of global transparency challenges.

- Dynamic Regulatory Landscape:

The rapidly evolving nature of privacy laws, such as the recent enactment of the EU's Digital Services Act and similar initiatives worldwide, necessitates ongoing research. Future studies could assess the effectiveness of these newer regulations in addressing transparency issues and explore their impact on platform operations.

- User-Centric Research:

While this thesis evaluates transparency from a regulatory and platform perspective, there is a need for qualitative research that captures user experiences and perceptions. Studies focusing on how users interpret and engage with transparency measures could shed light on the effectiveness of these initiatives and inform user-centric policy development.

- Technological Advancements:

As artificial intelligence and machine learning technologies become increasingly integrated into social media platforms, future research should investigate their implications for transparency. For instance, studies could explore how explainable AI (XAI) frameworks

can enhance algorithmic transparency and empower users to understand automated decision-making processes.

- Cultural and Societal Factors:

Privacy expectations and transparency preferences vary across cultures and demographics.

Research examining these differences can inform tailored transparency practices that respect cultural norms and address the specific needs of diverse user groups.

These limitations and future research directions highlight the complexity of achieving meaningful transparency in the digital age. Addressing these gaps will require collaborative efforts among academics, regulators, platforms, and users to ensure that transparency evolves alongside technological and societal changes.

## 5.5 Vision for the Future

As social media platforms continue to evolve and influence society, culture, and individual behavior, their role in shaping the digital landscape becomes increasingly significant. Transparency, as a cornerstone of ethical governance, must transition from being a regulatory obligation to a guiding principle embedded within the DNA of these platforms.

- Transparency as a Core Value:

To foster trust and ensure ethical data practices, platforms must integrate transparency into their operational and strategic frameworks. This includes adopting proactive measures that prioritize user rights and aligning business objectives with societal well-being. Platforms like Instagram can lead by example, setting industry benchmarks for transparency and accountability.

- Empowering Users Through Knowledge:

A user-centric approach is vital for realizing a transparent digital ecosystem. By simplifying privacy settings, providing real-time notifications about data use, and offering interactive tools to explore algorithmic processes, platforms can empower users to make informed decisions. Transparency should not only reveal what data is being collected but also explain how it is used and the implications for users.

- **Strengthening Regulatory Enforcement:**

Regulators must play an active role in enforcing privacy laws and ensuring that platforms meet transparency standards. This includes adopting robust mechanisms to evaluate compliance, imposing meaningful penalties for violations, and continuously updating regulations to address technological advancements. A collaborative approach involving regulators, platforms, and advocacy groups can enhance the effectiveness of these efforts.

- **Innovating for Ethical Technology:**

The future of transparency lies in technological innovation. Privacy-enhancing technologies (PETs), algorithmic audits, and explainable AI can provide platforms with tools to enhance transparency while protecting user data. Investing in these solutions can enable platforms to navigate the complex intersection of privacy, personalization, and profit.

- **Fostering Global Collaboration:**

Achieving a consistent and transparent digital ecosystem requires harmonized global standards. Platforms operating across borders must adhere to the strictest privacy regulations while respecting regional nuances. Collaborative efforts between governments, international organizations, and industry leaders can create a cohesive framework that balances global consistency with local relevance.

- Building Ethical Digital Ecosystems:

Transparency is not an endpoint but a foundation for creating ethical and sustainable digital ecosystems. By prioritizing transparency, platforms can redefine their role as stewards of the digital age, fostering environments where privacy, trust, and user empowerment coexist. This vision calls for an unwavering commitment from platforms, policymakers, and users to uphold the values of fairness, inclusivity, and accountability.

The findings of this thesis underscore the importance of transparency as a transformative force in digital governance. By embracing this vision, social media platforms can not only comply with regulatory standards but also establish themselves as ethical leaders in the digital era. This approach will pave the way for a future where technology serves humanity, respects individual rights, and promotes societal well-being.

## 5.6 Final Reflections

This thesis bridges the gap between theoretical concepts of digital governance and their practical application in the context of social media platforms, specifically Instagram. Critically examining Instagram's transparency practices and their alignment with GDPR and Canadian privacy laws contributes to a deeper understanding of the challenges and opportunities in advancing user rights and regulatory compliance in the digital era.

- Bridging Theory and Practice:

The research highlights the disconnect between the ideals of privacy laws and their real-world implementation. While regulatory frameworks like GDPR aim to empower users and ensure accountability, platforms often struggle with operationalizing these principles due to technical, legal, and business constraints. This study serves as a call to action for platforms to not merely comply but to innovate and lead in transparency practices.

- **Fostering Ethical Accountability:**

Transparency, as demonstrated in this thesis, is not just a regulatory obligation but a cornerstone of ethical digital governance. By offering actionable recommendations and highlighting the importance of user empowerment, this study aspires to promote a cultural shift where platforms prioritize ethical accountability alongside profitability and innovation.

- **The Role of Collaboration:**

The complexity of transparency challenges underscores the need for collaboration among all stakeholders. Regulators, platforms, users, and advocacy groups must work together to address systemic issues, create adaptable standards, and ensure that technological advancements align with ethical principles. The findings of this thesis advocate for such a multi-stakeholder approach to digital governance.

- **Contributions to a Sustainable Digital Future:**

As the digital ecosystem evolves, the importance of transparency will only grow. This thesis envisions a future where social media platforms redefine their role as ethical stewards, fostering environments that respect user privacy, enhance trust, and promote equitable access to information. By adopting the principles and recommendations outlined in this research, platforms can lay the groundwork for a more inclusive and sustainable digital future.

In conclusion, this thesis not only contributes to the academic discourse on transparency and data privacy but also offers practical strategies to address current gaps. It calls for a concerted effort by all stakeholders to ensure that the digital world evolves in ways that prioritize ethical integrity, user empowerment, and societal well-being. By navigating this complex landscape with a

commitment to transparency and accountability, platforms like Instagram can redefine their legacy as champions of user rights and ethical innovation.



# Bibliography

## Books

Bygrave, Lee Andrew, *Data privacy law: an international perspective* (Oxford University Press, 2014).

Cofone, Ignacio, *The privacy fallacy: harm and power in the information economy* (Cambridge University Press, 2023).

Edwards, Lilian, *Law, policy and the Internet* (Bloomsbury Publishing, 2018).

GILLESPIE, Tarleton, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media* (Yale University Press, 2018).

Zuboff, Shoshana, “The age of surveillance capitalism” in *Social theory re-wired* (Routledge, 2023) 203.

## Journal Articles

Asgarinia, Haleh et al, “‘Who Should I Trust with My Data?’ Ethical and Legal Challenges for Innovation in New Decentralized Data Management Technologies” (2023) 14:7 *Information* 351.

Boyd, Danah M & Nicole B Ellison, “Social network sites: Definition, history, and scholarship” (2007) 13:1 *Journal of computer-mediated Communication* 210–230.

Cofone, Ignacio, “Certifying Privacy Class Actions” (2023) 37:3 *Harvard Journal of Law & Technology*.

Cofone, Ignacio, “Privacy Standing” (2022) *U Ill L Rev* 1367.

Cofone, Ignacio N & Adriana Z Robertson, “Privacy harms” (2017) 69 *Hastings LJ* 1039.

DeNardis, Laura & Andrea M Hackl, “Internet governance by social media platforms” (2015) 39:9 *Telecommunications Policy* 761–770.

Dreyer, Stephan & Lennart Ziebarth, “Participatory transparency in social media governance: combining two good practices” (2014) 4 *Journal of Information Policy* 529–546.

Edwards, Lilian, “Data protection: Enter the general data protection regulation” (2018) *Law, Policy and the Internet* (Hart Publishing, 2018).

Edwards, Lilian & Lachlan Urquhart, “Privacy in public spaces: what expectations of privacy do we have in social media intelligence?” (2016) 24:3 *International Journal of Law and Information Technology* 279–310.

Edwards, Lilian & Michael Veale, “Enslaving the algorithm: From a ‘right to an explanation’ to a ‘right to better decisions’?” (2018) 16:3 IEEE Security & Privacy 46–54.

Edwards, Lilian & Michael Veale, “Privacy, security and data protection in smart cities: A critical EU law perspective” (2016) 28:2 European Data Protection Law Review.

Edwards, Lilian & Michael Veale, “The EU AI Act: a summary of its significance and scope” (2021) 16:1 Artificial Intelligence (the EU AI Act) 39–47.

Edwards, Lilian & Michael Veale, “Slave to the algorithm? Why a right to an explanation is probably not the remedy you are looking for” (2017) 16 Duke L & Tech Rev 18.

Ercan, Saniye Ezgi, “Navigating the Processing of Personal Data for Personalised Advertising on Instagram: In Search of an Appropriate Lawful Ground under the GDPR” (2023) SSRN Journal, online: <<https://www.ssrn.com/abstract=4649383>>.

Fine Licht, Karl de & Jenny de Fine Licht, “Artificial intelligence, transparency, and public decision-making: Why explanations are key when trying to produce perceived legitimacy” (2020) 35 AI & society 917–926.

Fleming, Piers et al, “Tell me more, tell me more: repeated personal data requests increase disclosure” (2023) 9:1 Journal of Cybersecurity tyad005.

Floridi, Luciano, “The ethics of artificial intelligence: Principles, challenges, and opportunities” (2023).

The ethics of artificial intelligence: Principles, challenges, and opportunities” (2023).

Goldman, Eric, “The Constitutionality of Mandating Editorial Transparency” (2022) 73 Hastings LJ 1203.

Gorwa, Robert & Timothy Garton Ash, “Democratic transparency in the platform society” (2020) Social media and democracy: The state of the field and prospects for reform 286–312.

Hein, Andreas et al, “Digital platform ecosystems” (2020) 30 Electronic markets 87–98.

Johnson, Emma, Ravi Patel & Sophie Martin, “The Impact of Social Media on Mental Health” (2023) 3:1 Psychoanalysis and Behavioral Science Review 13–19.

Just, Natascha & Florian Saurwein, “Enhancing Social-Media Regulation through Transparency? Examining the New Transparency Regime in the EU” (2024) February TechREG™ Chronicle 1–9.

Khoo, Cynthia, Kate Robertson & Ronald Deibert, “Installing fear: A Canadian legal and policy analysis of using, developing, and selling smartphone spyware and stalkerware applications” (2019).

La Diega, Guido Noto, “Against the dehumanisation of decision-making” (2018) 9 J Intell Prop

Info Tech & Elec Com L 3.

Lampmann-Shaver, Erik, “Privacy’s next Act” (2024) 19 Wash JL Tech & Arts 97.

Leerssen, Paddy, “The soap box as a black box: regulating transparency in social media recommender systems” (2020) 11:2 European Journal of Law and Technology.

MacCarthy, Mark, “Transparency Requirements for Digital Social Media Platforms: Recommendations for Policy Makers” (2020) Algorithms.

Martin, Kirsten, “Privacy Myths and Mistakes: Paradoxes, tradeoffs, and the omnipotent consumer” (2024).

Martin-Bariteau, Florian & Teresa Scassa, “Artificial intelligence and the law in Canada” (2021) Artificial Intelligence and the Law in Canada (Toronto: LexisNexis Canada, 2021).

McClain, Colleen et al, “How Americans view data privacy” (2023) Pew Research Center.

Montgomery, Kathryn C, “Youth and surveillance in the Facebook era: Policy interventions and social implications” (2015) 39:9 Telecommunications Policy 771–786.

Musiyiwa, Ruvimbo, “‘Influencer marketing is not a way around the law’: Regulatory Compliance and Law Enforcement in the Canadian Social Media Influencer Field”.

Nwaimo, Chioma Susan, Ayodeji Enoch Adegbola & Mayokun Daniel Adegbola, “Data-driven strategies for enhancing user engagement in digital platforms” (2024) 6:6 International Journal of Management & Entrepreneurship Research 1854–1868.

Osterholz, Sarah, Emily I Mosel & Boris Egloff, “#Insta personality: Personality expression in Instagram accounts, impression formation, and accuracy of personality judgments at zero acquaintance” (2023) 91:3 Journal of Personality 566–582.

Pérez–Acuña, Beatriz & Celia Fernández–Aller, “Facebook and Artificial Intelligence: A Review of Good Practices”.

Ploug, Thomas, “The Right Not to Be Subjected to AI Profiling Based on Publicly Available Data—Privacy and the Exceptionalism of AI Profiling” (2023) 36:1 Philos Technol 14.

Saprikis, Vaggelis & Giorgos Avlogiaris, “Modeling users’ acceptance of mobile social commerce: the case of ‘Instagram checkout’” (2023) 23:1 Electron Commer Res 511–540.

Scassa, Teresa, “AI and Data Protection Law” (2021) Artificial Intelligence and the Law in Canada (Toronto: LexisNexis Canada, 2021).

Scassa, Teresa, “Regulating AI in Canada: A Critical Look at the Proposed Artificial Intelligence and Data Act” (2023) 101:1 Canadian Bar Review.

Seng, Sovantharith, Mahdi Nasrullah Al-Ameen & Matthew Wright, “A first look into users’ perceptions of facial recognition in the physical world” (2021) 105 Computers & Security

102227.

Singer, Abigael, “The Corporate Challenges of Conforming to Data Privacy Laws: Balancing User Data Rights and Corporate Innovation” (2024) Available at SSRN 4960389.

Tran, Han, “UNDERSTANDING USER INFORMATION BEHAVIOUR: AN ANALYSIS OF DATA PROTECTION MEASURES ON DIGITAL PLATFORMS”.

Urman, Aleksandra & Mykola Makhortykh, “How transparent are transparency reports? Comparative analysis of transparency reporting across online platforms” (2023) 47:3 Telecommunications policy 102477.

Van Der Schyff, Karl & Stephen Flowerday, “The mediating role of perceived risks and benefits when self-disclosing: A study of social media trust and FoMO” (2023) 126 Computers & Security 103071.

Wachter, Sandra, Brent Mittelstadt & Luciano Floridi, “Why a right to explanation of automated decision-making does not exist in the general data protection regulation” (2017) 7:2 International data privacy law 76–99.

Waldman, Ari Ezra, “Cognitive biases, dark patterns, and the ‘privacy paradox’” (2020) 31 Current opinion in psychology 105–109.

## **Legislation**

Personal Information Protection and Electronic Documents Act (PIPEDA)  
Canada, Personal Information Protection and Electronic Documents Act, SC 2000, c 5.

Artificial Intelligence and Data Act (proposed in Bill C-27)  
Canada, Artificial Intelligence and Data Act, Bill C-27, 1st Sess, 44th Parl, 2022 (first reading 16 June 2022).

General Data Protection Regulation (GDPR)  
European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, [2016] OJ, L 119/1.

AI Act (proposed)  
European Union, Proposal for a Regulation laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act), COM (2021) 206 final.

## **Reports and Online Sources**

Branch, Legislative Services, “Consolidated federal laws of Canada, Personal Information Protection and Electronic Documents Act”, (19 August 2024), online: <<https://laws->

lois.justice.gc.ca/eng/acts/p-8.6/>.

Foundation, The Electronic Frontier, “EFFs 2023 Annual Report”, online: *EFF’s 2023 Annual Report* <<https://www.eff.org/annual-report/2023/index.html>>.

Government of Canada, Department of Justice, “Department of Justice - Statement of Potential Charter Impacts”, (4 November 2022), online: <[https://www.justice.gc.ca/eng/csj-sjc/pl/charte-charte/c27\\_1.html](https://www.justice.gc.ca/eng/csj-sjc/pl/charte-charte/c27_1.html)>.

“Proposed Legislation - Canada’s Sytem of Justice”, (10 February 2017), online: <<https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/pa-lprp.html>>.

Greenberg, Julia, “Like Facebook, Instagram Is About to Go—Gasp—Algorithmic”, (15 March 2016), online: *WIRED* <<https://www.wired.com/2016/03/instagram-will-soon-show-thinks-want-see/>>.

Kofman, Ariana Tobin, Ava, “Facebook Finally Agrees to Eliminate Tool That Enabled Discriminatory Advertising”, (22 June 2022), online: *ProPublica* <<https://www.propublica.org/article/facebook-doj-advertising-discrimination-settlement>>.

“A History of Transparency Regulations: Interdisciplinary Strategies for Shaping Social Media Regulation and Self-Governance | Proceedings of the 25th Annual International Conference on Digital Government Research”, online: *ACM Other conferences* <<https://dl.acm.org/doi/10.1145/3657054.3657157>>.

“Biggest social media platforms by users 2024 | Statista”, online: <<https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>>.

“Canadian Digital Media Research Network”, (10 December 2024), online: *Canadian Digital Media Research Network* <<https://www.cdmrn.ca>>.

“European Commission, official website - European Commission”, (16 January 2025), online: <[https://commission.europa.eu/index\\_en](https://commission.europa.eu/index_en)>.

“Forside”, online: *Forbrukerrådet* <<https://www.forbrukerradet.no/>>.

“Government Requests for User Data | Transparency Center”, online: <<https://transparency.meta.com/reports/government-data-requests/>>.

“Home”, online: *Digital Rights Watch* <<https://digitalrightswatch.org.au/>>.

“NOYB enforces your right to privacy everyday”, online: <<https://noyb.eu/en>>.

“Pinterest pins users’ data down - without consent!”, online: <<https://noyb.eu/en/pinterest-pins-users-data-down-without-consent>>.

“Privacy International”, online: <<https://privacyinternational.org/>>.

“Social media algorithms ‘amplifying misogynistic content’”, (6 February 2024), online: *the Guardian* <<https://www.theguardian.com/media/2024/feb/06/social-media-algorithms-amplifying-misogynistic-content>>.

“The Personal Information Protection and Electronic Documents Act (PIPEDA) - Office of the Privacy Commissioner of Canada”, online: <<https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/>>.

“The Washington Post - Breaking news and latest headlines, U.S. news, world news, and video - The Washington Post”, online: *Washington Post* <<https://www.washingtonpost.com/>>.

“Toronto Metropolitan University research repository - Browse”, online: <<https://rshare.library.torontomu.ca./>>.

“Transparency Center”, online: <<https://www.tiktok.com/transparency/en>>.

“What is GDPR, the EU’s new data protection law?”, (7 November 2018), online: *GDPR.eu* <<https://gdpr.eu/what-is-gdpr/>>.

“What TikTok and Facebook may track with their in-app browsers”, (13 September 2022), online: *Washington Post* <<https://www.washingtonpost.com/technology/2022/09/13/facebook-instagram-data-privacy/>>.

## **News and Media Sources**

Greenberg, Julia, “Like Facebook, Instagram Is About to Go—Gasp—Algorithmic” *Wired*, online: <<https://www.wired.com/2016/03/instagram-will-soon-show-thinks-want-see/>>.

Hunter, Tatum et al, “What TikTok and Facebook may track with their in-app browsers”, *Washington Post* (13 September 2022), online: <<https://www.washingtonpost.com/technology/2022/09/13/facebook-instagram-data-privacy/>>.

Pardes, Arielle, “How Facebook and Other Sites Manipulate Your Privacy Choices” *Wired*, online: <<https://www.wired.com/story/facebook-social-media-privacy-dark-patterns/>>.

Weale, Sally & Sally Weale Education correspondent, “Social media algorithms ‘amplifying misogynistic content’”, *The Guardian* (6 February 2024), online: <<https://www.theguardian.com/media/2024/feb/06/social-media-algorithms-amplifying-misogynistic-content>>.

Zuboff, Shoshana, “The age of surveillance capitalism” in *Social theory re-wired* (Routledge, 2023) 203.

“Facebook security breach: Up to 50m accounts attacked”, (28 September 2018), online: <<https://www.bbc.com/news/technology-45686890>>.

“Tool checks phone numbers from Facebook data breach”, (6 April 2021), online: <<https://www.bbc.com/news/technology-56650387>>.

### **Conference Papers and Research Studies**

Binns, Reuben, *Fairness in machine learning: Lessons from political philosophy* (PMLR, 2018).

Ebert, Nico, Kurt Alexander Ackermann & Björn Scheppler, *Bolder is better: Raising user awareness through salient and concise privacy notices* (2021).

Giesen, Jaryd et al, *YouTube vs the status quo: Why distribution platform matters for student engagement with lecture videos* (Australasian Association for Engineering Education (AAEE), a Technical ..., 2022).

Rendón, L Grisales, *An introduction to the principle of transparency in automated decision-making systems* (IEEE, 2022).

Vergara, Caitlyn, Raghav Jain & Swapneel Mehta, *A History of Transparency Regulations: Interdisciplinary Strategies for Shaping Social Media Regulation and Self-Governance* (New York, NY, USA: Association for Computing Machinery, 2024).