**Ethical Concerns and Privacy Issues in Social Media: A Focus on Instagram**

**Balaram Saripalli, Avinash Gorrepati, and Karthik Chekuri**

**Regis University  
MDSD640 - Ethics/ Privacy/ Social Justice  
Ksenia Polson**

**April 9, 2024**

**Ethical Concerns and Privacy Issues in Social Media: A Focus on Instagram**

**Introduction**

Instagram, created by Kevin Systrom and Mike Krieger in 2010, has grown into a giant in the social media landscape, now part of Meta Platforms, Inc., which also owns Facebook. As of 2022, Instagram boasts over two billion monthly users (Britannica, 2024). The platform is straightforward: users share photos or short videos that, depending on their privacy settings, can be viewed by anyone on Instagram or just their followers. Its vast user base makes it highly attractive to advertisers, and this popularity has also given rise to influential users who can significantly impact others' opinions and purchasing decisions.

However, the platform's extensive data collection practices can negatively affect users' personal information, as it involves tracking user activity and preferences, often for targeted advertising, which raises concerns about privacy and data security.

**Abstract**

This case explores the ethical and privacy concerns associated with Instagram and its unauthorized third-party viewer tools. Instagram is a globally popular social media platform owned by Meta Platforms. Its popularity has generated various third-party applications that enable users to view private profiles, photos, and stories without consent. This intrusion of privacy raises significant ethical issues, primarily the violation of personal information. Such unauthorized access can lead to misuse, such as stalking or harassment, heightening the risk for users. Moreover, these third-party tools may compromise security, exposing users to potential scams or malware. The case underscores the broader implications of how social media companies manage user data and the necessity for robust privacy protections. It also highlights the ethical responsibilities of these companies to protect individuals from privacy invasions and the potential harms of data misuse. This discussion aims to give a deeper understanding of the importance of ethical practices in the management of user data by social media platforms.

**Ethical lens**

If we observe the case of Instagram and unauthorized third-party viewer tools based on the privacy invasion that happened, the Rights-Based Ethics lens is the most applicable one. This approach mainly focuses on respecting and protecting the rights of individuals, particularly the right to privacy.

**The reason that the Rights-Based Ethics lens is applied here is:**

Rights-based ethics stresses that everyone has basic rights that others, including companies, must respect and protect.

In this situation, **using unauthorized tools to view private Instagram content violates people's privacy rights.** This approach argues that individuals should have the fundamental right to decide who can see their personal and sensitive information.

**Violation of User Consent**: Third-party tools are frequently used without the clear agreement of the individuals whose data is being accessed. *Rights-based ethics highlights how crucial consent is* because it respects individuals' independence. Accessing private information without this consent breaches ethical rules about respecting and valuing a person's privacy.

**Responsibility of Companies**: According to rights-based ethics, companies have a responsibility to protect their users' rights. This includes *keeping their private information safe from unauthorized access and misuse*. The situation with Instagram shows that these platforms haven't done enough to protect these rights, indicating a need for more robust policies and actions that put user privacy first.

**Legal and Ethical Aspects**: Rights-based ethics matches well with laws that protect privacy, like the General Data Protection Regulation (GDPR) in Europe and other privacy laws around the world. This connection strengthens the ethical reasons for protecting privacy and shows that **s***ocial media platforms have a legal duty to safeguard user data.*  
 As per the case, the violations that are committed are more similar to the right-based ethical lens perspective, which offers a strong way to examine and tackle the ethical problems in the case. It stresses that user privacy is a basic right that must be respected and protected, which shows the importance of getting user consent. It urges companies to meet their ethical and legal responsibilities to safeguard these rights. This approach not only deals with the issue of unauthorized data access but also helps us understand more broadly how digital platforms should handle user data responsibly.

**Concerns raised in the case**

**Why do social media companies fail to ensure user privacy and data protection?**

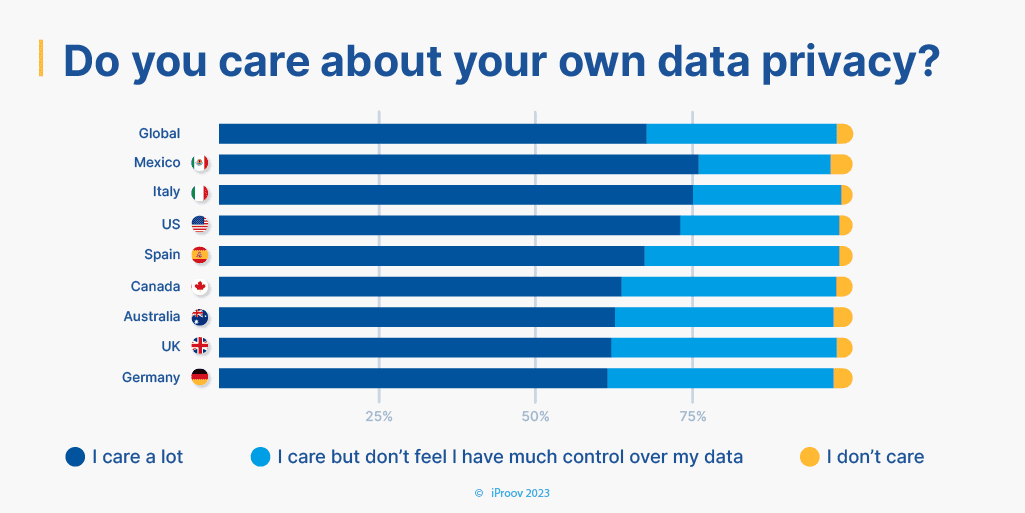
One significant issue is the **lack of strict measures to control or regulate third-party applications** that can access and exploit user data without consent. These tools can view private profiles and content, which undermines the privacy settings users have set up.

There's a perceived **prioritization of profit over privacy**. Social media platforms heavily rely on advertising revenue, which involves extensive data collection and user tracking. This business model can sometimes conflict with the strict privacy protections users expect, leading to decisions that favor data access over user confidentiality.

There is a lack of **technical safeguards** necessary to protect user data completely, and there may be policies that are too lenient on data access by third parties. This could be due to the complex nature of digital environments where data is massively interconnected and continuously flowing.

There might be a delay in responding to emerging privacy threats or in updating privacy policies to reflect new challenges. This **slow response to privacy concerns** can leave users vulnerable to privacy breaches for prolonged periods.

Companies may not provide sufficient tools or transparent information that empowers users to effectively manage their privacy settings. Users often find themselves **unaware of how their data is being used or how to protect it adequately.**



The above graph is taken from a survey done by iproov (a fast-growing global technology company and the world leader in biometric verification and authentication), which questioned consumers about whether they care about their privacy. (the survey was done in 2023)

Iproov asked the consumers the same question in 2020, and 25% of them cared but did not feel much control over their own data. The same question was asked in 2023, and 30% of consumers said that they were losing control over their own data.

From this information, we can say that even though people care about their privacy, there is an increase in the loss of control over data. We can say that social media companies are not giving priority to the user’s privacy, or they lack the power to provide privacy protection and seek profit from third-party companies.

**Is it fair for companies to track our online behavior for personalized ads?**

If we observe the case where unauthorized third-party tools are accessing private Instagram content, it's clear that tracking online behavior for personalized ads raises significant ethical issues.

So, It's not fair, mainly when it compromises user privacy and lacks transparency, as seen with Instagram. Users often do not fully understand or consent to the extent of tracking and data usage that occurs. This lack of informed consent undermines the fairness and ethicality of such practices.

Social media sites like Instagram should give proper consent to users in an understandable way by any means possible, as there is a lack of awareness among them. By doing this, the users will know how their data is being used.

A graph with blue and white bars

Description automatically generated

The above graph is taken from the YouGov survey where 63.16% of the people thought of personalized ads as an invasion of privacy, according to the Author[[Zia Muhammad](https://www.digitalinformationworld.com/p/zia-muhammad.html)](2023)

**What are the ethical implications of targeting ads with personal data on sensitive topics?**

Using personal data to target ads on sensitive topics like health or family matters is ethically problematic. It can invade privacy and break trust, especially if people don't know their sensitive information is being used for ads. This can also cause emotional distress when personal details are used for profit. Additionally, it suggests that social media companies might care more about making money than protecting user privacy. This highlights the need for more vital privacy rules and clear agreements to prevent the misuse of sensitive information in advertising.

**By following these steps, we can reduce the risk of our privacy being invaded and being tracked online at all times:**

We need to clear our cookies in the system or from the devices used daily, so the third-party company can’t track our personal information.

We need to reset our advertising ID. In addition to cookies, almost every mobile device has its own advertising ID, which stores our data. We must reset it or give access to only the necessary terms.

Google gives us an opt-out option where we can delete our personal ad history by visiting myactivity.google.com.

Everybody must install an adblocker to avoid visiting or clicking the links we are not supposed to, as it can track or monitor our activity.

Using private browsers like Firefox or DuckDuckGo, etc., can make our personal information more secure. These private browsers are very useful when working on something more personal.

We can install tracker blockers that observe the site code and prevent the loading of unwanted sites. We always have an opt-out option.

According to the author[[**Brian X. Chen**](http://www.nytimes.com/by/brian-x-chen)](2018), All we need to do is follow these steps and try to reduce the risk of being monitored every time.

**Strategy**

According to the case, ethical issues such as unauthorized access and privacy invasion over sensitive content on Instagram, a strategic approach according to the Right-based Lens is,

Instagram should create better privacy settings that let users quickly decide who can see their content. This means making tools for **managing privacy more clear and easy to use.**

Social media Companies should Set up and enforce **strict rules that third-party apps must follow to access user data**. This should include thorough checks, frequent inspections, and fines.

Keeping users updated on **how their data is being used and who can access it**. This can be done through clear privacy notices and straightforward disclosures.

Ensure that **users clearly agree to data sharing, understand what they're agreeing to, and can withdraw their consent at any time**. Provide an easy way for users to opt out if they change their minds.

By Running **educational campaigns** to help users understand their rights and how to protect their privacy. This can empower users to make informed decisions about their data.

Working closely with privacy regulators to ensure compliance with existing laws like GDPR and to help shape future regulations that protect user data. Invest in advanced security technologies that prevent unauthorized data breaches and detect vulnerabilities in the platform's ecosystem.

**Conclusion**

We conclude that Addressing privacy issues on Instagram and with third-party tools requires a thorough approach based on rights-based ethics. By improving privacy settings, regulating third-party apps, enhancing transparency, better-managing user consent, educating users, and working with regulatory bodies, Instagram can greatly strengthen its user data protection.

These actions comply with laws like GDPR and boost user trust in the platform. Essentially, protecting user privacy is crucial for social media platforms to maintain their reliability and ethical standards. This broad strategy helps ensure that users can manage their personal information securely and confidently engage online, emphasizing the responsibility of digital platforms to protect user privacy.

**Group Debrief**

Throughout this case study, we collectively explored the ethical implications and challenges surrounding Instagram's use of data and the issues with unauthorized third-party viewer tools.

Our process began with a thorough research phase where we gathered and analyzed various sources to understand the scope of the issue. We held regular meetings to discuss our findings and frame our arguments, which proved invaluable in enhancing our understanding and refining our focus. One of the key strategies we employed was dividing the work based on individual strengths, which allowed us to efficiently tackle different aspects of the project, such as legal implications, ethical theories, and technological safeguards.

We also made it a point to critically challenge each other's viewpoints to ensure a well-rounded analysis. Reflecting on our group's work, we feel that this collaborative and structured approach has enriched our paper.

**How This Case Study Helped us Understand Ethical Theories:**

**Bala Ram:** Throughout this project, I learned the significance of considering multiple ethical perspectives when analyzing a case study. Exploring how Instagram’s data practices could be viewed under different ethical lenses was particularly enlightening. This experience has taught me the importance of ethics in understanding and resolving complex issues, reinforcing my appreciation for thorough analysis in making informed decisions.

**Avinash:** My involvement in this project deepened my understanding of the practical implications of ethical theories.

After reading the case , I remembered that my friends were using some tools that were available online to see the DP and photos of others even though their accounts were private. It happened when I was an undergrad. So I thought even if we have trusted software where we can keep our personal info safe, there is a chance of intrusion. So, from our side as individuals, we have to be careful about what we upload online. If we are seeking attention or have a goal of being an influencer, it is fine, but if it’s not the goal, is it necessary to upload our personal info or our daily activities online as there is no need for it?

Applying right-based ethics to our case study was especially compelling, as it underscored the importance of respecting user consent and privacy. This has made me more conscious of my own digital footprint and the ethical responsibilities of companies I interact with as a consumer.

**Karthik:** This project challenged me to think critically about the balance between business objectives and ethical considerations. Engaging in debates and discussions with my teammates was invaluable, as it pushed me to refine my arguments and better articulate my views. I’ve gained a greater appreciation for the complexity of ethical decision-making in a business context, particularly in the fast-evolving tech industry.

**References**

Eldridge, A. (2024, March 30). *Britannica Money.* Www.britannica.com. <https://www.britannica.com/money/Instagram>

Roose, K. (2019, May 9). *Instagram Is Trying to Curb Bullying. First, It Needs to Define Bullying.* The New York Times. <https://www.nytimes.com/2019/05/09/technology/instagram-bullying-teenagers.html>

*Top 5 Common Sites For Social Media Cyberbullying*. (n.d.). Www.dispartilaw.com. <https://www.dispartilaw.com/common-sites-for-social-media-cyberbullying/>

‌*Nearly 80% of Social Media Users have Adjusted their Privacy Settings in the Last Year!* (n.d.). <https://www.digitalinformationworld.com/2019/10/research-shows-internet-users-taking-action-on-privacy.html>

*Do Consumers Dislike Targeted Personalized Ads?* (2019). EMarketer. <https://www.emarketer.com/content/do-people-actually-want-personalized-ads>

GCF Global. (n.d.). *The Now: What is Targeted Advertising?* GCFGlobal.org. [https://edu.gcfglobal.org/en/thenow/what-is-targeted-advertising/1/#](https://edu.gcfglobal.org/en/thenow/what-is-targeted-advertising/1/)

Chen, B. X. (2018, August 15). Are Targeted Ads Stalking You? Here’s How to Make Them Stop. *The New York Times*. <https://www.nytimes.com/2018/08/15/technology/personaltech/stop-targeted-stalker-ads.html>

*Biometrics & Data Privacy | Data Privacy Statistics [2023]*. (2023, January 25). Www.iproov.com. <https://www.iproov.com/blog/data-privacy-statistics-biometrics>

Markkula Center for Applied Ethics. (2021, November 8). *A Framework for Ethical Decision Making*. Santa Clara University; Santa Clara University. <https://www.scu.edu/ethics/ethics-resources/a-framework-for-ethical-decision-making/>

‌*Over 37% of Users Hate Targeted Ads*. (n.d.). <https://www.digitalinformationworld.com/2023/02/over-37-of-users-hate-targeted-ads.html>