Michael Amoo

2/09/25

James Talley

Balancing Social Commerce and User Data Protection

Social commerce has transformed the e-commerce industry due to the fast development of integrating social media platforms with online shopping. This transformation helps companies to obtain huge quantities of user data to improve advertising, personalize product suggestions and increase user interaction. Nevertheless, these data collection practices are the subject of ethical concerns regarding user privacy, consent, and security. The major ethical questions are whether social media companies should be allowed to gather user data with or without the users’ consent, how often societies should be informed about such practices, and how to achieve the equilibrium between business requirements and individual privacy rights. This paper aims at discussing these ethical issues, reviewing the conflict between business and consumer privacy, and providing recommendations on how to address ethical issues in data collection while encouraging the growth of social commerce.

Social commerce uses the gathering of large amounts of data to provide personalized shopping experiences. To enhance customer engagement, businesses use social commerce platforms to analyze user behavior, preferences, and purchase history to improve their advertising strategies. This is a problem of consent and transparency, which is a major concern for businesses and users. As noted by Ranjan (2023), this is because most users are not aware of the amount of data that is collected from them, thus making them become digital surveillance victims or having their data misused.

Another major ethical concern is the non-informed consent of users in data collection. Social network sites and other social media platforms have privacy policies that are unclear and complex, thus it is challenging for users to know how their data is being used. Casaca and Rosário (2024) explain that businesses employ imprecise terms to justify the large amount of data collection, thus constraining users’ choices. This lack of transparency erodes the trust of consumers and makes them worry about their data being compromised in breaches or used for unsavory purposes by third parties.

Also, data breaches are another threat in social commerce. This is because when businesses store and gather a large amount of personal information, they attract the attention of cybercriminals. The occurrence of unauthorized access to user’s sensitive data can lead to identity theft, financial fraud, and damage to an organization’s reputation. From an ethical perspective, companies should ensure that they implement proper cybersecurity measures to protect the users’ information and prevent unauthorized access.

The major issue of conflict between business and user privacy is the treatment of personal data as a business asset. Social media companies have a large source of income from targeted advertising, which is based on the creation of user profiles. This is because companies focus more on data collection than on user privacy to protect their interests. Though businesses claim that data-driven marketing improves customer experiences and creates economic value, privacy advocates argue that more needs to be done to protect users’ rights and ensure responsible data handling.

This conflict can be seen in the example of Facebook and the data-sharing controversy where third-party firms accessed users’ information without their knowledge. This has happened in the past, and it shows why data collection should not go unregulated, and why there needs to be more oversight. The issue here is whether the protection of user privacy should take precedence over the financial benefits of businesses or whether businesses should be legally and morally compelled to put consumer interests ahead of their profits.

However, consumers are often unable to make their own decisions regarding their data privacy. Most social networks require registration, and to use them, users have to agree to the data collection policy, which leaves users with no choice but to allow their data to be collected. This is an ethical problem of digital coercion where people are forced to give up their privacy to use social commerce. This imbalance needs to be addressed by having policies that give power to users to make decisions about their data.

For social commerce to grow while protecting ethical standards of data, companies should ensure openness, user consent, rules, and technologies that respect privacy. Improved privacy by using simple and easily understandable privacy policies helps consumers to make decisions on their data. User-centric consent mechanisms include opt-in models, through which people give consent to data collection as opposed to being tracked by default. Legal frameworks, for example, the General Data Protection Regulation (GDPR), provide a legal framework that regulates the correct use of data and penalizes violations. Also, the use of privacy technologies such as encryption and anonymization allow businesses to analyze consumer behavior without revealing the identity of the consumer. According to Casaca and Rosário (2024), companies that adhere to ethical standards in data management not only meet legal requirements but also gain the trust of their customers, which is advantageous to both the companies and the customers.

Social commerce linked with social media has revolutionized how businesses engage with customers, raising important issues of data protection and privacy. However, as businesses are benefiting from the data, the ethical issues of user privacy and consent cannot be ignored.

As a result, businesses need to understand that ethical data management is not just a legal compliance issue, but a sustainable business model that fosters consumer confidence. Therefore, social commerce platforms can grow and thrive while upholding user privacy standards through the adoption of sound data protection policies. As Ranjan (2023) pointed out, there is a need to find a balance between the privacy safeguards and the commercial innovation to build a digital economy that will be beneficial to both the business community and the consumer.

**References**

Casaca, J. A., & Rosário, A. T. (2024). The Impact of Personal Information in E-Commerce: Balancing Privacy, Security, and Ethics. In *Data-Driven Marketing for Strategic Success* (pp. 222-255). IGI Global.

Ranjan, D. (2023). *The Evolving Landscape of Social Media and Privacy: Balancing Connectivity and Personal Data Protection.* Commerce & Management, 34.