Data Privacy: Ethical Responsibilities in a Digital Age

Drew Jones

Department of Computer Science, Southern Wesleyan University

CPSC 4202: Computer Science Senior Capstone

Dr. Paul Jordan

September 23rd, 2025

Data Privacy: Ethical Responsibilities in a Digital Age

Data privacy concerns who is responsible for handling the personal information that is collected, stored, and shared about users. As technology becomes more integrated into daily life, individuals generate increasing amounts of personal data through everyday activities. This rapid expansion has led to public uncertainty and fear regarding how data is used and whether it is adequately protected. Many people feel they lack control over their own information and express distrust toward corporations and government institutions tasked with protecting their privacy. Although various laws exist to safeguard sensitive data, many loopholes remain. The lack of uniform standards—especially within the United States, where each state may establish its own rules—makes consistent enforcement difficult. Some argue that national privacy laws would provide clarity, while others maintain that privacy must be built directly into technological systems rather than treated as a secondary concern. Ultimately, data privacy extends beyond legislation; it represents a matter of trust, fairness, and safeguarding individuals from misuse of their personal information.

Data privacy has become one of the most important ethical issues in modern technology. As digital systems expand, individuals are increasingly tracked, analyzed, and categorized based on the data they produce. This information can include browsing history, purchasing habits, location data, health records, and biometric identifiers. The ethical question centers on how this information should be managed and who holds responsibility for ensuring it remains protected.

A major concern is that individuals often do not fully understand how much data they are generating or where it ultimately goes. Companies frequently collect more data

than consumers realize, and many organizations share or sell this information to third parties without transparent disclosure. This creates a power imbalance in which users have little control over their own digital identities, raising ethical concerns regarding informed consent and fairness.

Legislation attempts to address these concerns, but the landscape remains inconsistent. While regulations such as HIPAA protect certain types of medical information, other categories of personal data fall into gray areas where protections are weak or nonexistent. The United States faces additional complexity because privacy laws differ from state to state. This patchwork framework makes compliance difficult and leaves gaps that can be exploited by organizations handling user data.

To move toward a more ethical model, many experts argue that privacy should be embedded directly into technological systems. This concept, known as 'privacy by design,' emphasizes proactive planning, transparency, and minimizing data collection whenever possible.

Ultimately, data privacy is about trust. Users must be able to rely on organizations to handle their information responsibly. Ethical digital practices require more than legal compliance—they demand fairness, transparency, and the protection of human dignity.

References

Buckley, M., Guariglia, M., Cohen, L., Klosowski, T., & Richman, J. (n.d.). Privacy. Electronic Frontier Foundation. https://www.eff.org/issues/privacy