

Ethics Paper

COINS415

Marina Skegro

Charleston Southern University: CSCI.415

12/1/2025

Ethics Paper

The quick development of digital technology has changed how personal data is gathered, kept, and utilized, posing serious ethical issues in addition to providing previously unheard-of ease. Concerns over privacy and anonymity have become significant public discussions since the mid-1900s, when big government databases first appeared. This is especially true as computing has become more widely available and pervasive in daily life. Alongside these technical developments, the idea of privacy has changed, forcing academics and decision-makers to reevaluate what protections are required in a world where data is easily sent over international networks. Society continues to wonder how much personal information should be available and who should have access to it, as seen by the historical discussions concerning public identifiers in the 1960s and the more current disputes about data-mining, click-tracking, and online anonymity. It is crucial to comprehend the ethical implications of privacy and anonymity, particularly as contemporary digital technologies offer advantages as well as risks to users traveling online spaces.

The purpose of this paper is to investigate the ethical concerns surrounding privacy and anonymity in computers using key academic ideas, current discussions, and looking at the consequences these difficulties have for each person's autonomy and security. This paper will attempt to offer a thorough ethical viewpoint on how society should handle privacy protections in a technologically complex world by examining the development of privacy concepts, assessing philosophical disputes, and investigating advantages and disadvantages of digital anonymity.

The notion of privacy in computers initially developed as a public issue during the 1960s when governments began to gather vast amounts of sensitive data, including tax records, military data, and welfare statistics. As detailed in the assignment text, congressional attempts to give each citizen a universal personal identification number prompted widespread fears about “big brother government.” This reaction underscores an essential ethical principle: individuals dread the possible abuse of personal information when organizations obtain excessive monitoring powers. Westin (1967) defined privacy as an individual's control over the collection and use of their personal information. This definition greatly influenced early laws like the U.S. Privacy Act of 1974.

However, as technology developed, academics began to wonder if control was sufficient to describe the essence of privacy. According to Moor (1997) and Tavani & Moor (2001), privacy is best described as “restricted access,” which means that restrictions exist when people are unable to regulate the flow of information. This difference is important because actual control is sometimes difficult in current digital environments. People could, for instance, agree to data gathering without fully comprehending the extent to which their information can be aggregated or analyzed by third parties. Data-mining technologies, behavioral monitoring, and online click-trail recording limit user control, making the restricted access model increasingly relevant for evaluating privacy measures. Research reinforces this worry, indicating that customers often misjudged how much data corporations gather, and how it’s utilized (Acquisti, Brandimarte, & Loewenstein, 2015).

By contending that privacy exists even in public settings when people have expectations about how their information will be utilized, Nissenbaum (1998) significantly broadened the philosophical scope of privacy. According to her “contextual integrity” thesis, privacy violations

happen when information flows in ways that go against the standards of a certain context. For example, even if they are technically in a public virtual area, a person may legitimately demand confidentiality when researching sensitive issues online. This approach shows why privacy is a major ethical concern today, as digital technologies often cross boundaries without being recognized by users.

Anonymity serves a key role in strengthening privacy rights, particularly in online situations. People can explore political views, get medical advice, get psychiatric help, or talk about controversial subjects without worrying about criticism or backlash when they participate anonymously. According to Marx (1999), anonymity is a defense mechanism that promotes mental health, autonomy, and free speech. Anonymity's usefulness is especially clear for disadvantaged groups who may face discrimination or societal damage if their identities are disclosed.

However, because the same safeguards that protect lawful acts can sometimes encourage bad ones, anonymity also poses ethical questions. Criminal activities, including fraud, money laundering, and the exploitation of vulnerable groups, can be carried out using anonymous networks. The difficulty is striking a balance between society's duty to avoid damage and the requirement for anonymity. This conflict is a reflection of a larger ethical discussion in computing about how to create systems that reduce abuse chances while optimizing individual security measures.

Therefore, the rise of privacy and anonymity in technology reveals a constant ethical battle. The possibility for spying grows as computers develop, occasionally going beyond established moral and legal bounds. Ethical frameworks that stress autonomy, informed consent, and contextual integrity highlight the need for better protections, more open data processes, and

improved public knowledge. The objective should be to protect human values of privacy and anonymity in quickly developing technology systems rather than to completely stop collecting data.

Overall, privacy and anonymity are essential ethical challenges in the digital era, driven by decades of technical progress and philosophical debate. Early worries about government overreach have developed into sophisticated considerations about data-mining, internet tracking, and the limitations of private control over personal information. Scholars such as Westin, Moor, Nissenbaum, and Tavani have offered critical viewpoints that expose privacy as a multidimensional notion that includes control, restricted access, and contextual expectations. While providing vital safeguards for individual liberty and freedom of speech, anonymity also offers moral dilemmas when abused for negative objectives. Navigating these conflicts, ethically and making sure that digital technologies uphold rather than compromise individual autonomy, security, and dignity is the ethical issue facing modern civilization. Careful privacy safeguards and reasonable anonymity regulations will continue to be crucial for maintaining trust and moral integrity in the digital world as computer systems develop.

References

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509–514. <https://doi.org/10.1126/science.aaa1465>
- Marx, G. T. (1999). What's in a name? Some reflections on the sociology of anonymity. *The Information Society*, 15(2), 99–112. <https://doi.org/10.1080/019722499128565>
- Nissenbaum, H. (1998). Protecting privacy in an information age: The problem of privacy in public. *Law & Philosophy*, 17(5–6), 559–596. <https://doi.org/10.1023/A:1006184504201>
- Tavani, H. T., & Moor, J. H. (2001). Privacy protection, control of information, and privacy-enhancing technologies. *ACM SIGCAS Computers and Society*, 31(1), 6–11. <https://doi.org/10.1145/572260.572263>
- Westin, A. F. (1967). *Privacy and freedom*. Atheneum Press.