International Journal of Arts and Humanities Studies
ISSN: 2754-4311
DOI: 10.32996/ijahs
Journal Homepage: www.al-kindipublisher.com/index.php/Ijahs

IJAHS
AL-KINDI CENTER FOR RESEARCH
AND DEVELOPMENT

| **RESEARCH ARTICLE**

Human Rights and Technology: Exploring How Technological Advancements Impact Human Rights, Particularly in Surveillance and Data Collection

Md Wasim Ahmed[1] , Md Fahim Ahammed[2]
[1]*Masters in Law, Green University, Bangladesh*
[2]*Masters in Information Assurance and Cybersecurity, Gannon University, Erie, PA, USA*
Corresponding Author: Md Wasim Ahmed, E-mail: ad.wasimahmed@gmail.com

| ABSTRACT

Technological advancements, particularly in surveillance and data collection, have transformed how societies function and how governments and corporations interact with individuals. While technology has brought substantial benefits in communication, healthcare, and public safety, it has also raised profound concerns about human rights, particularly in privacy, freedom of expression, and security. This paper explores the impact of technology on human rights, focusing on the ethical and legal implications of surveillance and data collection practices. We analyze how different technologies, including facial recognition, artificial intelligence, and big data analytics, affect individual freedoms and privacy, offering policy recommendations for a more balanced approach to technology that respects human rights.

| KEYWORDS

Human rights, technology, surveillance, data collection, privacy, artificial intelligence, ethics.

| ARTICLE INFORMATION

ACCEPTED: 01 November 2024 **PUBLISHED:** 19 November 2024 **DOI:** 10.32996/Ijahs.2024.4.4.4

1. Introduction

Background and Context

As technological innovation accelerates, the intersection between technology and human rights has become a critical area of study. Advancements in digital technology have reshaped the global landscape, enabling unprecedented data collection, rapid communication, and enhanced surveillance capabilities. Governments and private organizations increasingly employ technologies like facial recognition, biometric data, and AI-driven analytics to monitor and analyze individuals, often without their explicit consent. While these technologies serve various purposes, including national security and business intelligence, they also pose significant risks to fundamental human rights.

Purpose and Scope

This paper examines how technological advancements in surveillance and data collection impact human rights, specifically focusing on privacy and freedom of expression. By exploring specific cases and analyzing current regulations, the study aims to shed light on the ethical challenges and potential regulatory solutions necessary to ensure technology serves as a tool for positive social change without compromising individual freedoms.

Research Questions

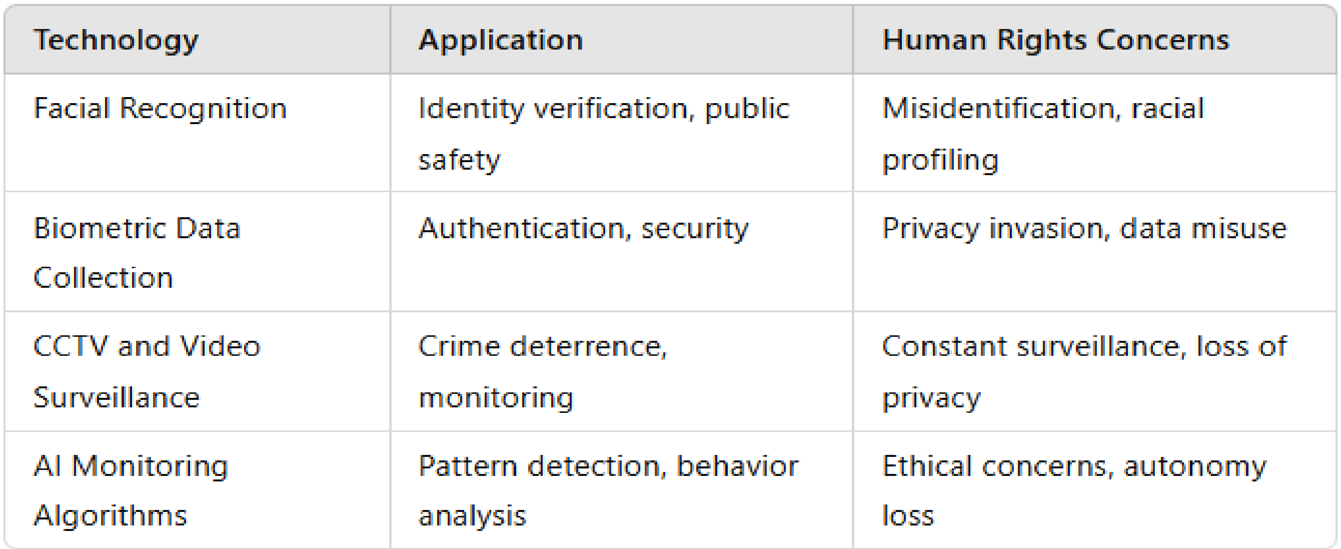
1. How do technological advancements in surveillance and data collection affect human rights, particularly privacy and freedom of expression?
2. What ethical challenges arise from using these technologies?
3. How can legal frameworks evolve to protect human rights in the age of pervasive technology?

2. Surveillance Technology and Human Rights

2.1 Surveillance Technology Overview

Surveillance technology encompasses a range of tools designed to monitor, record, and analyze human activities. These include facial recognition software, biometric data collection systems, CCTV networks, and AI-driven monitoring algorithms. Governments worldwide have increasingly adopted these technologies to bolster national security, deter crime, and enhance public safety. However, while surveillance can improve security, it often infringes upon privacy rights, creating an environment where individuals feel monitored and restricted.

Table 1: Types of Surveillance Technologies and Potential Human Rights Impacts



Technology	Application	Human Rights Concerns
Facial Recognition	Identity verification, public safety	Misidentification, racial profiling
Biometric Data Collection	Authentication, security	Privacy invasion, data misuse
CCTV and Video Surveillance	Crime deterrence, monitoring	Constant surveillance, loss of privacy
AI Monitoring Algorithms	Pattern detection, behavior analysis	Ethical concerns, autonomy loss

This table highlights common surveillance technologies and the potential threats they pose to human rights. The misuse of these tools can lead to violations of privacy, discrimination, and, in extreme cases, loss of freedom of expression.

2.2 Case Studies in Surveillance Technology

1. **China's Social Credit System**

The Chinese government's use of surveillance technology as part of its social credit system represents one of the most comprehensive examples of technology's impact on human rights. Through widespread monitoring, including facial recognition and behavioral analysis, the government assigns social credit scores based on citizens' activities and compliance with social norms. Low scores can result in penalties, such as restricted access to travel, employment, and social services. This system exemplifies how surveillance technology can be used to control and limit individual freedoms, effectively compromising citizens' autonomy and privacy.

2. **U.S. Government Surveillance Programs**

In the United States, post-9/11 security measures expanded government surveillance capabilities through initiatives like the Patriot Act, which allows intelligence agencies to collect data without traditional legal oversight. The Snowden revelations in 2013 exposed the extent of government surveillance on citizens and foreign nationals, sparking widespread debate about the balance between national security and individual rights. Surveillance technologies used by government agencies, including mass data collection and location tracking, have raised serious privacy concerns and prompted discussions about necessary reforms.

3. **European Union's GDPR Regulations and Facial Recognition**

The European Union's General Data Protection Regulation (GDPR) emphasizes the protection of personal data and privacy. In some cases, GDPR has led to restrictions on the use of facial recognition technology, particularly in public spaces. For example, in 2020, France's data protection authority ruled against the use of facial recognition in schools, citing privacy concerns and a lack of necessity. The GDPR serves as a model for protecting individual rights in the digital age, highlighting the importance of stringent regulations in limiting excessive surveillance practices.

3. Data Collection and Privacy Concerns

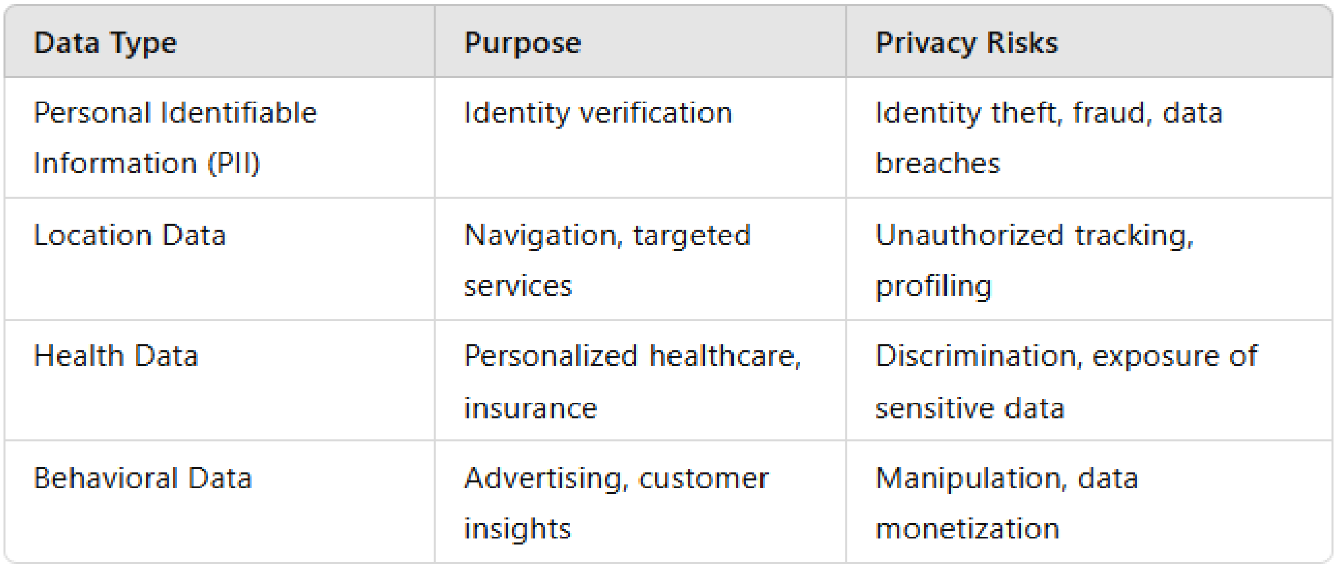
As technology advances, the scale and scope of data collection have grown exponentially. Data is now gathered from almost every aspect of life, spanning personal information, online behaviors, physical location, health metrics, and social interactions. While this data can drive innovation, improve services, and foster economic growth, it also brings significant privacy risks. The volume of data collected and the ways it is processed by algorithms can lead to unintended consequences, including data breaches, unauthorized tracking, and privacy violations. This section explores the types of data collected, associated privacy risks, and key case studies illustrating the impact of inadequate data privacy protections.

3.1 Case Studies in Surveillance Technology

Modern data collection is pervasive and includes detailed records of user activities, preferences, and interactions, often without explicit user awareness or consent. Key data types collected from users include:

1. **Personal Identifiable Information (PII):** Data that can identify an individual, such as name, date of birth, address, and social security numbers. This information is essential for identity verification but poses a significant risk if exposed.
2. **Location Data:** Real-time GPS data is used in navigation, location-based services, and targeted advertising, but raises concerns about tracking and profiling.
3. **Health Data:** Health-related information is gathered through fitness apps, wearable devices, and healthcare services. While valuable for personalized healthcare, it is highly sensitive and can lead to discrimination if misused.
4. **Behavioral Data:** This includes browsing history, app usage, purchase history, and other patterns that reveal user interests and behaviors, which are often used for targeted advertising.

Table 2: Types of Data Collected and Associated Privacy Risks



Data Type	Purpose	Privacy Risks
Personal Identifiable Information (PII)	Identity verification	Identity theft, fraud, data breaches
Location Data	Navigation, targeted services	Unauthorized tracking, profiling
Health Data	Personalized healthcare, insurance	Discrimination, exposure of sensitive data
Behavioral Data	Advertising, customer insights	Manipulation, data monetization

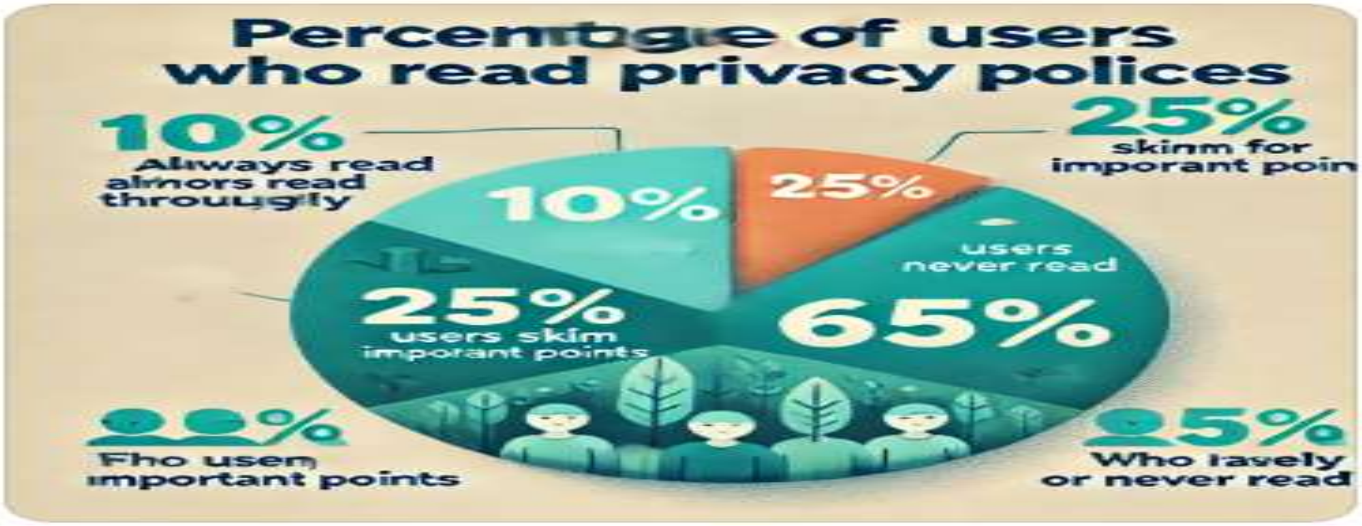
This table highlights how each type of data is used, alongside specific privacy risks associated with unauthorized access or misuse.

3.2 The Role of Consent in Data Collection

The concept of user consent is fundamental in data privacy law. Regulations like the GDPR in the European Union require explicit consent from users before collecting and processing their data. However, in practice, obtaining meaningful consent is challenging due to opaque terms and conditions, which users may not fully understand. As a result, many individuals consent to data collection without realizing the extent to which their data will be used, shared, or stored.

Graph 1: Percentage of Users Who Read Privacy Policies

The graph below illustrates that only a small percentage of users read privacy policies thoroughly, while most either skim them or skip them entirely. This lack of engagement is often due to complex legal language and lengthy documents, which results in users granting consent without fully understanding its implications.



3.3 Privacy Risks in Large-Scale Data Collection

Large-scale data collection poses multiple risks to individual privacy, particularly when companies and organizations do not have stringent data protection measures in place. Privacy risks associated with data collection include:

1. **Data Breaches:** Unauthorized access to databases can lead to the exposure of sensitive information. High-profile breaches have shown that even well-resourced organizations can be vulnerable to data theft.
2. **Profiling and Surveillance:** Data collected from users can be used to build detailed profiles, including information about preferences, behavior, and location. These profiles can be used by companies for targeted advertising or by governments for surveillance.
3. **Discrimination:** Certain types of data, such as health information or location data, can be used to discriminate against individuals. For example, health data could be used to deny insurance coverage, and location data could reveal patterns that expose marginalized groups to additional scrutiny.

Bar Chart: Frequency of Data Breaches in Different Sectors (2015-2023)

This bar chart visualizes the frequency of data breaches in sectors such as healthcare, finance, retail, and technology, illustrating how widespread and impactful these breaches are across industries.

3.4 Case Studies in Data Privacy Violations

1. **Cambridge Analytica and Facebook:** The Cambridge Analytica scandal, where the data of millions of Facebook users was improperly accessed, revealed the potential for misuse of personal information on social media platforms. Cambridge Analytica used data to create psychological profiles, influencing political campaigns in both the U.S. and the UK. This case highlighted the need for stronger regulations on data sharing and third-party access.
2. **Healthcare Data and AI in Predictive Analytics:** As AI integrates into healthcare, hospitals and companies are increasingly using predictive analytics based on patient data. However, without strict data protection policies, sensitive health data can be exposed, impacting individuals' privacy and security. For example, data could be used to predict health risks without the patient's knowledge or consent, raising ethical questions about privacy and data usage.

3.5 Policy Recommendations for Data Privacy Protection

1. **Clear and Simple Privacy Policies:** Companies should provide privacy policies in simple language, enabling users to understand how their data will be used. Transparency in data collection practices allows individuals to make informed choices about consenting to data collection.
2. **Minimization of Data Collection:** Data minimization involves collecting only the data that is necessary for a specific purpose. This principle, embedded in regulations like GDPR, can help reduce privacy risks by limiting the scope of data available for misuse or theft.
3. **Regular Data Audits and Security Measures:** Regular security audits and updates to data protection measures are essential to safeguard personal information. Companies should implement encryption, secure storage, and access controls to prevent unauthorized access to sensitive data.

4. Ethical Implications of Surveillance and Data Collection

The rise of advanced surveillance and data collection technologies has introduced complex ethical dilemmas that influence individual privacy, autonomy, freedom of expression, and the nature of societal trust. As governments and corporations increase their capabilities to monitor, collect, and analyze personal data, it raises questions about how these powers impact human rights and freedoms. Ethical considerations in this realm focus on issues of informed consent, data ownership, potential discrimination, and the moral obligations of entities collecting and utilizing personal data. This section delves into the primary ethical implications associated with surveillance and data collection, emphasizing their broader societal impacts.

4.1 Autonomy and Freedom of Expression

One of the core ethical concerns with surveillance technology and pervasive data collection is the effect on individual autonomy and freedom of expression. When individuals are aware that their actions, communications, and behaviors are monitored, it can lead to a phenomenon known as the "chilling effect." This concept suggests that people may alter their behaviors or restrict their expressions to avoid potential scrutiny or judgment, even if they are not engaged in any unlawful activities.

Impacts on Autonomy and Freedom:

1. **Self-Censorship:** When individuals know they are being watched or tracked, they may self-censor, avoiding statements or actions that could be misinterpreted or judged. This undermines the essence of free expression, as individuals may avoid voicing dissenting opinions, criticisms, or ideas that challenge social norms or authority.
2. **Behavior Modification:** Surveillance creates environments where individuals unconsciously or consciously modify their behaviors to align with perceived norms. This limits genuine self-expression and can impact creativity, social interactions, and cultural diversity.
3. **Psychological Effects:** Constant surveillance can cause stress, anxiety, and distrust, as individuals feel their autonomy and privacy are compromised. Over time, this state of hyper-awareness can erode mental well-being and alter societal behavior at large.

4.2 Privacy and Consent

Privacy is a fundamental human right that is compromised when data is collected without explicit, informed consent. Ethical frameworks emphasize the importance of consent, suggesting that individuals should have the right to know what data is collected about them, how it is used, and with whom it is shared. However, in practice, data collection is often performed without genuine consent or with only superficial consent (e.g., checking a box to agree to terms and conditions). Ethical issues arise from this imbalance in information and power.

Issues Related to Privacy and Consent:

1. **Informed Consent:** Many users are not fully aware of the extent of data collected or how it will be used. Lengthy privacy policies filled with technical jargon deter users from reading them thoroughly. As a result, consent is often uninformed, undermining the ethical validity of data collection practices.
2. **Data Ownership:** There is an ongoing debate about who truly "owns" personal data once it is collected. From an ethical standpoint, individuals should have rights over their data and control its use. However, many companies treat personal data as an asset, monetizing it without fair compensation or acknowledgment to the individuals from whom it originates.
3. **Surveillance Without Consent**: In some regions, governments and corporations implement surveillance measures without explicit consent, often justifying it for security or public interest reasons. However, this raises ethical issues as individuals may be monitored without awareness, infringing upon their privacy and freedom.

4.3 Discrimination and Bias

Surveillance and data collection systems often use algorithms and machine learning to make decisions, classify individuals, or predict behaviors. However, these algorithms are not free from biases, and the data they use can reflect historical or systemic inequalities. When surveillance technology incorporates biased data, it can perpetuate or even amplify discrimination, leading to unfair treatment and marginalization of specific groups.

Ethical Concerns Related to Discrimination:

1. **Algorithmic Bias:** Surveillance systems, particularly facial recognition and behavioral analysis algorithms, have been shown to exhibit higher error rates for certain demographics, such as people of color or women. This can lead to disproportionate targeting or misidentification, impacting individual lives and perpetuating discrimination.
2. **Targeting Vulnerable Populations:** Certain communities may be subject to more intensive surveillance based on factors such as socioeconomic status, ethnicity, or nationality. For example, law enforcement may deploy more surveillance resources in economically disadvantaged neighborhoods, leading to ethical issues around equality and fairness.
3. **Predictive Policing and Profiling:** Data collection is sometimes used to predict criminal behavior through "predictive policing," where algorithms attempt to forecast where crime may occur or who might be involved. This can lead to profiling, where individuals are treated as suspects based on predictive patterns rather than actual behavior, raising serious ethical concerns.

4.4 Transparency and Accountability

An essential ethical obligation for entities engaged in data collection and surveillance is transparency. However, many organizations fail to disclose the extent of their surveillance or the specific data collected. Ethical principles suggest that individuals should be informed about data practices and given the opportunity to opt out if they disagree. Without transparency, it is challenging to hold organizations accountable for misuse or abuse of data.

Transparency and Accountability Challenges:

1. **Openness About Surveillance Practices:** Transparency requires that organizations disclose their surveillance activities, the data collected, and the purposes for which it will be used. Many organizations, however, lack adequate transparency, leading to ethical concerns about informed consent and individual rights.
2. **Data Misuse and Lack of Oversight:** When there are no clear accountability measures, organizations may misuse data without repercussions. This can include using data beyond the scope for which it was initially collected or selling it to third parties without user knowledge. Ethical frameworks argue for stringent oversight to ensure that data practices align with consent and privacy rights.
3. **Right to Redress:** In cases where data misuse occurs, individuals often lack mechanisms for redress. From an ethical perspective, organizations should implement clear pathways for individuals to address grievances, seek corrections to data inaccuracies, or request deletion of their data.

4.5 Societal Impacts and the Role of Technology Companies

Technology companies play a significant role in shaping the ethics of surveillance and data collection. As entities with the power to influence policy, develop innovative solutions, and implement privacy controls, technology companies bear responsibility for protecting individual rights and maintaining ethical standards.

Corporate Responsibility in Ethical Data Practices:

1. **Development of Privacy-Preserving Technologies:** Technology companies are encouraged to prioritize privacy-preserving innovations, such as anonymization techniques, data encryption, and differential privacy. These technologies allow companies to harness data without compromising individual privacy.

2. **Implementation of Ethical Frameworks:** To mitigate risks, companies should adopt ethical frameworks that prioritize user privacy, data security, and respect for individual rights. Ethical AI principles and guidelines, including transparency, fairness, and accountability, should be embedded in corporate policy and product development processes.
3. **Commitment to Ethical Data Usage:** Corporations have a social responsibility to use data in ways that benefit society, avoiding practices that exploit or harm users. Ethical data usage means prioritizing user consent, limiting data collection to necessary information, and actively working to prevent discrimination or harm.

5. Policy Recommendations

As the ethical and privacy implications of surveillance and data collection become increasingly evident, comprehensive policy interventions are essential to protect individual rights and uphold public trust. Effective policy recommendations should address the root ethical concerns while providing practical, enforceable solutions that adapt to the rapidly evolving technological landscape. Key areas of focus for policy recommendations include transparency and accountability, limitations on data use, strengthening data protection laws, and promoting ethical standards within technology companies.

5.1 Transparency and Accountability Measures

Ensuring transparency and accountability in surveillance and data collection is a fundamental step toward maintaining ethical data practices. These measures allow individuals to make informed decisions about how their data is used and create pathways to hold organizations responsible for misuse or unethical practices.

1. **Mandatory Data Disclosure Policies**

- **Description:** Companies and organizations engaged in data collection should be required to disclose their data practices, including the types of data they collect, the purposes of data collection, and how the data will be used and stored.
- **Rationale:** Transparency is essential for building public trust. When individuals are informed about data practices, they can make educated choices about consenting to data collection and can better understand the potential impact on their privacy and rights.
- **Implementation:** Policies should mandate the publication of clear, accessible privacy notices and terms of service that avoid legal jargon, allowing all users to understand data practices without needing specialized knowledge.

2. **Regular Accountability Audits**

- **Description:** Organizations that collect and process large volumes of personal data should undergo regular accountability audits to assess compliance with data privacy laws, ethical standards, and user consent requirements.
- **Rationale:** Regular audits can identify gaps in data protection practices and address potential issues before they result in violations or breaches. They also reinforce the organization's commitment to data ethics.
- **Implementation:** These audits could be conducted by independent third-party organizations to ensure unbiased assessments, with results made available to regulatory bodies and the public.

5.2 Limitations on Data Collection and Use

One of the main ethical concerns in data collection is the sheer volume of data collected, often far exceeding what is necessary for a given purpose. To address this, policies should enforce the principles of data minimization, purpose limitation, and appropriate usage.

1. **Data Minimization Principle**

- **Description:** Data minimization restricts data collection to only what is necessary for the stated purpose, preventing organizations from gathering excessive or irrelevant information.
- **Rationale:** Collecting only the essential data reduces the risk of privacy breaches and ensures that users' personal information is not unnecessarily exposed or exploited.
- **Implementation:** Regulatory guidelines could define what constitutes "necessary" data for specific services and applications. Violations of data minimization could lead to penalties or sanctions.

2. **Purpose Limitation for Data Usage**

- **Description:** Purpose limitation policies would require organizations to use collected data solely for the purposes for which it was gathered, prohibiting secondary uses without additional consent.
- **Rationale:** Restricting data usage to its original purpose protects individuals from exploitation, preventing companies from repurposing data in ways that users did not agree to.
- **Implementation:** Organizations would need to specify purposes at the time of data collection and be held legally accountable if data is later repurposed without renewed user consent.

3. **Strict Control over Biometric and Health Data**

    - **Description:** Given the sensitive nature of biometric and health data, policies should impose strict limits on their collection, storage, and sharing. Organizations should only collect this data when absolutely necessary and with explicit, informed consent.

- **Rationale:** Biometric and health data are highly personal, and misuse could lead to discrimination, health-related stigma, or unauthorized access to sensitive information.
- **Implementation:** Policies could mandate heightened protections, including additional consent requirements, encrypted storage, and severe penalties for unauthorized sharing or breaches.

5.3 Strengthening Data Protection Laws

While many countries have adopted data protection laws, such as the General Data Protection Regulation (GDPR) in the EU, there is a need for uniform, global standards to address data privacy comprehensively and consistently across borders.

1. **Harmonization of International Data Privacy Standards**

- **Description:** Data privacy laws should be harmonized globally to create uniform standards for data collection, sharing, and storage practices, facilitating cross-border data protection.
- **Rationale:** Harmonization would prevent loopholes that companies could exploit by operating in jurisdictions with weaker data protection laws. Uniform standards also ease compliance for organizations operating internationally.
- **Implementation:** International regulatory bodies could work together to establish minimum standards, similar to the GDPR, and encourage countries to adopt these guidelines into national laws.

2. **Mandatory Reporting of Data Breaches**

- **Description:** Data breaches should be reported to both affected individuals and regulatory authorities immediately, enabling swift action to minimize harm.
- **Rationale:** Timely reporting allows individuals to take precautionary steps, such as changing passwords or monitoring financial accounts, and reinforces accountability for organizations.
- **Implementation:** Laws should require companies to report breaches within a specified timeframe (e.g., 72 hours) and impose penalties for delays or failures to disclose incidents.

3. **Data Portability Rights for Users**

- **Description:** Data portability rights allow users to transfer their data between service providers, giving them greater control over their information.
- **Rationale:** Data portability fosters competition among service providers, empowering individuals to choose companies that respect their privacy without losing access to their personal data.
- **Implementation:** Users should be able to download or transfer their data in a standardized, machine-readable format, similar to what is provided under GDPR in the EU.

5.4 Promoting Ethical Standards within Technology Companies

Technology companies play a crucial role in shaping the ethical landscape of data collection and surveillance. Policymakers should encourage companies to adopt ethical standards that prioritize user privacy, fairness, and transparency.

1. **Implementation of Privacy-by-Design Practices**

- **Description:** Privacy-by-design requires organizations to integrate data protection measures into the development of their products and services, rather than treating them as afterthoughts.
- **Rationale:** Designing systems with privacy as a core component reduces risks and ensures data protection at every stage of product development.
- **Implementation:** Companies could be required to submit privacy impact assessments (PIAs) for new products, demonstrating how privacy is maintained in their design.

2. **Ethics Training for Developers and Engineers**

- **Description:** Ethical training programs for employees involved in data handling, development, and analysis would emphasize the importance of responsible data practices and familiarize them with the potential consequences of misuse.
- **Rationale:** Awareness among employees helps prevent unethical practices, reduces bias, and instills a culture of respect for user privacy within organizations.
- **Implementation:** Companies could collaborate with academic institutions to develop standardized ethics training programs, offering certifications and ongoing education on data ethics and privacy.

3. **Establishment of Independent Ethics Committees**

- **Description:** Large technology companies could establish independent ethics committees to review data practices, monitor compliance, and provide guidance on ethical dilemmas.
- **Rationale:** Independent committees create checks and balances, ensuring decisions are aligned with ethical standards and not solely driven by profit motives.
- **Implementation:** Ethics committees could be required to include external stakeholders, such as human rights advocates, data privacy experts, and community representatives, to provide diverse perspectives on ethical challenges.

6. Conclusion

Technological advancements in surveillance and data collection offer tremendous benefits but also pose significant risks to human rights, particularly in terms of privacy, freedom of expression, and discrimination. By examining these risks and considering case studies, it becomes clear that the unchecked use of these technologies can lead to ethical and legal challenges that threaten individual freedoms. This paper advocates for robust legal frameworks, transparency, and accountability to ensure that technology enhances, rather than erodes, human rights in the digital age.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] A. Khan, Rashid, Hassan Qudrat-Ullah, Rashid A. Khan, and Hassan Qudrat-Ullah. "Technology adoption theories and models." Adoption of LMS in Higher Educational Institutions of the Middle East (2021): 27-48.

[2] Sanjida Nowshin Mou. (2024). Women's Empowerment through Higher Education and Employment in Bangladesh. Journal of Gender, Culture and Society, 4(2), 39–66. https://doi.org/10.32996/jgcs.2024.4.2.6

[3] Khan, Rashid, Akash Dania, Dialdin Osman, and Dexter Gettins. "Diffusion of innovation: Adoption of learning management system technology in emerging market economies." Accounting and Finance Research 10, no. 1 (2021): 1-1.

[4] Ahammed, Md Fahim, and Md Rasheduzzaman Labu. "Privacy-Preserving Data Sharing in Healthcare: Advances in Secure Multiparty Computation." Journal of Medical and Health Studies 5.2 (2024): 37-47.

[5] Md Wasim Ahmed. (2024). Artificial Intelligence and Legal Ethics. International Journal of Law and Politics Studies, 6(5), 226–237. https://doi.org/10.32996/ijlps.2024.6.5.12

[6] Labu, Md Rasheduzzaman, and Md Fahim Ahammed. "Next-Generation cyber threat detection and mitigation strategies: a focus on artificial intelligence and machine learning." Journal of Computer Science and Technology Studies 6.1 (2024): 179-188.