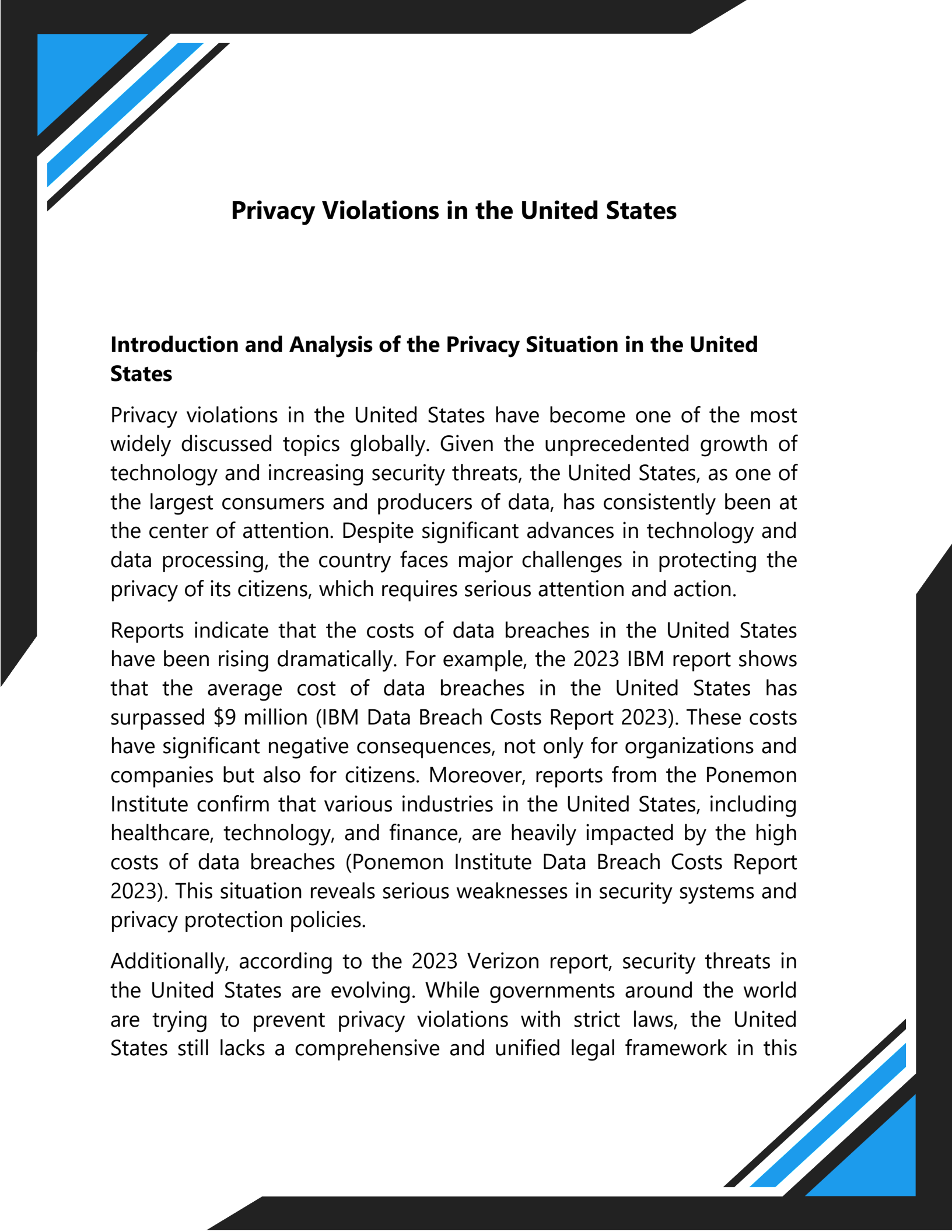




Privacy Violations in the United States

Introduction and Analysis of the Privacy Situation in the United States

Privacy violations in the United States have become one of the most widely discussed topics globally. Given the unprecedented growth of technology and increasing security threats, the United States, as one of the largest consumers and producers of data, has consistently been at the center of attention. Despite significant advances in technology and data processing, the country faces major challenges in protecting the privacy of its citizens, which requires serious attention and action.

Reports indicate that the costs of data breaches in the United States have been rising dramatically. For example, the 2023 IBM report shows that the average cost of data breaches in the United States has surpassed \$9 million (IBM Data Breach Costs Report 2023). These costs have significant negative consequences, not only for organizations and companies but also for citizens. Moreover, reports from the Ponemon Institute confirm that various industries in the United States, including healthcare, technology, and finance, are heavily impacted by the high costs of data breaches (Ponemon Institute Data Breach Costs Report 2023). This situation reveals serious weaknesses in security systems and privacy protection policies.

Additionally, according to the 2023 Verizon report, security threats in the United States are evolving. While governments around the world are trying to prevent privacy violations with strict laws, the United States still lacks a comprehensive and unified legal framework in this

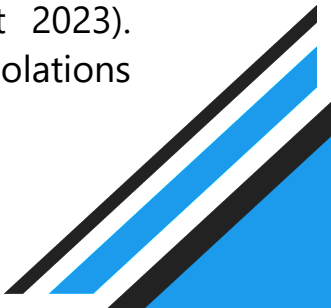


area. This gap increases users' vulnerability to cyberattacks and data breaches (Verizon Data Breach Investigations Report 2023). This is particularly true in the tech industry, where major companies like Google and Facebook collect billions of user data annually, putting them at risk.

Furthermore, various reports, including Symantec's 2023 report, indicate that cyberattacks and security threats against companies and government entities in the United States are on the rise. These attacks not only harm citizens' personal and financial information but also pose a threat to national security (Symantec Cybersecurity Threats Report 2023). In this regard, analysts believe that the U.S. government needs to adopt stricter policies for data protection and privacy.

The U.S. government, however, is clearly facing challenges in addressing privacy violations and cyber threats. While various agencies have introduced regulations to protect data, these laws are still not robust or effective enough. According to the McAfee Labs 2023 report, the U.S. lacks a comprehensive and coordinated policy in the field of privacy protection compared to other countries (McAfee Labs Cybersecurity Threats Report 2023). Furthermore, some companies and organizations, due to insufficient oversight, exploit users' data and sell it without users' knowledge or consent.

Such approaches not only violate citizens' privacy but also weaken public trust in government systems and large companies. In this context, the Kaspersky Security Bulletin 2023 and Trend Micro's Annual Cybersecurity and Privacy Report 2023 emphasize the need for preventive security measures and the strengthening of defense infrastructure to combat cyber threats (Kaspersky Security Bulletin 2023 and Trend Micro Cybersecurity and Privacy Annual Report 2023). Ultimately, to prevent the recurrence of widespread privacy violations





and mitigate their consequences, the United States must undertake a serious review of its policies and take necessary actions to protect citizens' data and address cyber threats.

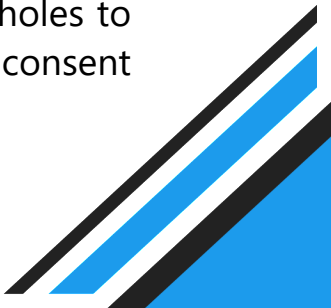
Given the data and reports available, the United States must pay more attention to the issue of privacy and reform its policies to protect it. Otherwise, security threats and privacy violations will continue to remain a serious challenge for citizens and organizations.

Legal and Regulatory Challenges in the United States

One of the biggest challenges the United States faces regarding privacy violations is the weakness of laws and regulations concerning data protection and privacy. While efforts have been made in recent years to improve the situation, the country still lacks a comprehensive and unified legal framework on this issue. This problem stems from the absence of a national law for privacy protection, which leaves the U.S. in a vulnerable position compared to many other developed countries.

One of the most notable laws in the U.S. concerning privacy is the Children's Online Privacy Protection Act (COPPA), which applies to children under the age of 13 and regulates the collection of data from them. However, this law is inadequate for addressing many of today's digital world needs, especially in the context of big data collection and processing. Major tech companies like Google, Amazon, and Facebook collect vast amounts of data from users and use it for various purposes. Such usage without transparency and adequate oversight constitutes a significant violation of privacy.

Existing reports also show that many companies exploit the weaknesses in current laws. For example, a report by the Ponemon Institute in 2023 indicates that many organizations in the U.S. exploit legal loopholes to collect and sell personal data or use it without users' consent





(Ponemon Institute Data Breach Costs Report, 2023). Such behaviors clearly highlight the lack of enforcement and oversight, which can exacerbate privacy violations and erode public trust in U.S. information and technology systems.

It is also important to note that despite repeated calls for legal reforms and increased oversight, the U.S. remains behind in establishing a comprehensive privacy law. Currently, many laws exist at the state and local levels, as well as in specific industries, addressing only certain aspects of privacy. There is no cohesive national framework for the protection of personal data. For example, only California has successfully enacted the California Consumer Privacy Act (CCPA), which allows users more control over their personal data. However, this law is limited to California and has not yet become a national model that applies across the U.S.

This situation prevents the U.S. from fully protecting its citizens' privacy, and both public and private organizations are unable to effectively combat cyber threats. According to various reports, many large tech companies still use users' data for advertising or sales purposes, and in many cases, this data is transferred without authorization to third parties. This issue, especially in social media platforms, where user data is extensively collected and analyzed, has raised serious concerns (Verizon Data Breach Investigations Report, 2023).

Furthermore, the existing laws and regulations in the U.S. cannot effectively address the increasing and complex cyber threats. According to Symantec's 2023 report, new security threats continue to emerge in cyberspace, and in some cases, even governments and state institutions are involved in creating security threats (Symantec Cyber Threat Report, 2023). This situation undermines public trust in governmental systems and prevents individuals from fully protecting





their personal data.

In conclusion, the U.S. government urgently needs to implement reforms in privacy laws and regulations. These reforms should include the adoption of a comprehensive, nationwide data protection law that ensures more effective oversight and control over tech companies and other public and private entities. Moreover, these reforms should aim at safeguarding user rights and preventing recurring privacy violations to restore public trust and minimize new security risks.

Security Threats and Privacy Violations in the Era of Big Data

In today's world, where information technology is rapidly advancing, one of the biggest threats to privacy is the increasing collection and use of big data by companies and government entities. This data includes sensitive and personal information of citizens that is widely stored, processed, and analyzed in the virtual space. The United States, as one of the leaders in technology, is exposed to numerous security threats that lead to privacy violations.

One of the main issues in this context is the weakness in protecting personal data. According to the IBM 2023 report, the costs associated with data breaches in the United States remain high, and many organizations are unable to effectively protect the data of their customers and users (IBM Data Breach Cost Report 2023). Data breaches not only directly harm organizations but also reduce users' trust in online services and digital technologies. Especially when sensitive data such as financial, medical, or identity information is exposed, it causes irreparable harm to individuals.

Furthermore, security threats from sophisticated and up-to-date cyberattacks have created serious problems for maintaining privacy. Cyberattacks, malware, and other cyber threats that infiltrate data



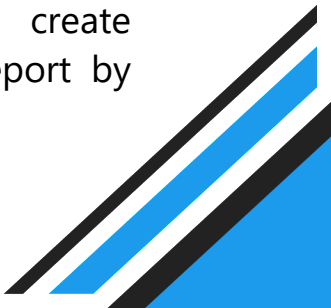


storage and processing systems result in the theft and disclosure of users' personal information. According to the Kaspersky Security Bulletin 2023, the frequency of cyberattacks has significantly increased, with hackers using more complex methods to infiltrate systems (Kaspersky Security Bulletin 2023). These threats are often targeted and based on information collected from users, which itself represents a serious violation of privacy.

One of the most important issues raised in this regard is the lack of transparency in the collection and use of data. In many cases, large tech companies collect user data but fail to provide effective communication about how this data is used. This lack of transparency prevents users from knowing where and how their personal information is being transferred. In this regard, reports indicate that most companies, especially in the technology industry, use user data for advertising and commercial purposes without obtaining full user consent (Verizon Data Breach Investigations Report 2023).

This situation is not only a threat to individuals' privacy but also undermines public trust in tech companies and even governments. For example, the U.S. government, as a regulatory entity, is unable to effectively track privacy violations. Recent reports show that even some U.S. government agencies have been involved in collecting and using personal data of citizens. This raises concerns about privacy rights violations and abuse of governmental power (McAfee Labs Security Threats Report 2023).

Meanwhile, some tech companies, such as Google and Facebook, continue to face criticism due to their widespread data collection and use for commercial and advertising purposes. These companies process users' data without their explicit consent and use it to create advertising and commercial profiles. For instance, a 2023 report by





Trend Micro indicates that some of these companies intentionally overlook privacy settings to gather more information from users and direct them to targeted ads (Trend Micro Cybersecurity and Privacy Annual Report 2023).

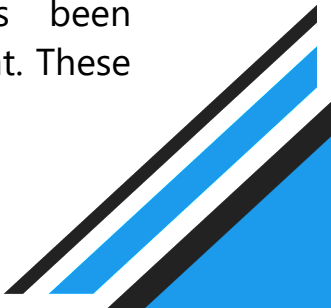
Ultimately, cyber threats and the unauthorized use of data in the era of big data have turned privacy violations into a serious crisis in the United States. These issues indicate that the United States still requires fundamental changes in addressing these threats and enhancing privacy in the digital world. Current policies in data protection and transparency in its use have proven insufficient and need significant legal and regulatory reforms.

Socio-Cultural Dimensions of Privacy Violations or Violations of Social Mental Health

Privacy violations in the United States are not just a technical or economic issue; they have significant socio-cultural and psychological consequences that can severely impact the mental health of individuals in society.

One of the negative impacts of privacy violations on culture is the erosion of public trust. When people feel that their personal data is being collected and used without their consent, their trust in both the government and private companies diminishes. This loss of trust leads to weaker social bonds, as individuals become more cautious in their social relationships and online interactions. This erosion of trust ultimately weakens social cohesion, causing people to be less willing to share or engage in public spaces.

From a societal perspective, privacy violations can lead to increased stress and anxiety. Many individuals whose data has been compromised or exposed may feel they are always under threat. These





concerns foster feelings of insecurity and psychological tension. The anxiety stemming from these issues can lead to mental health problems such as depression, severe stress, and a growing sense of distrust toward others.

Moreover, privacy violations cause people to feel that their personal boundaries are no longer secure. This directly impacts the quality of their social and psychological lives, stripping them of the freedom and autonomy they once had. When individuals perceive that they are constantly being surveilled or controlled, they are more likely to withdraw from public spaces and social interactions.

Ultimately, these issues can result in cultural and social harm. As people realize that their privacy is being violated and extensive surveillance is happening in their lives, they may gradually retreat into a state of cultural passivity, distancing themselves from active participation in society and cultural trends. These effects are particularly noticeable among younger generations, who may increasingly seek more privacy in their personal lives and distance themselves from online spaces and social engagement.

Recommendations

1. Establishing a Comprehensive Federal Data Protection Framework

Despite its advocacy for human rights, the United States lacks a GDPR-like framework to guarantee privacy rights. Such a framework would demonstrate a genuine commitment to citizens' rights, addressing the glaring contradiction between its human rights rhetoric and current practices.

2. Imposing Severe Penalties on Violating Companies





American tech corporations, which have become de facto data cartels, continue to violate privacy on a large scale due to insufficient legal deterrents. Significant financial penalties must be imposed to ensure these companies cannot repeatedly engage in such misconduct.

3. Creating an Independent Oversight Body

The U.S. cannot claim to uphold human rights while its oversight organizations are heavily influenced by the government or corporate interests. An independent regulatory body with sufficient authority is essential to prevent abuses.

4. Enhancing Public Awareness

If the United States truly values its citizens' rights, it should invest in public awareness programs about privacy rather than focusing on surveillance and intelligence projects.

It must act as a shield against data monopolies, rather than falling victim to these companies' misleading narratives.

5. Prohibition of Data Sales Without Explicit Consent

The sale of users' personal data by corporations is a blatant betrayal of privacy. In the U.S., this practice is not only legal but effectively encouraged. Implementing strict laws to prohibit such actions is essential to demonstrate that the value of its citizens transcends being "commodities for sale."

6. Enhancing Transparency in Corporate Practices

Transparency in the United States, despite its importance, has become a mere marketing tool, losing its true significance. Technology companies often provide misleading or incomplete information through promotional reports. To address this issue, strict regulations





must be implemented to require companies to publish accurate and factual reports. These reports should be reviewed by independent bodies to ensure their authenticity and transparency. Only through such measures can public trust be restored and potential abuses prevented.

7. Advancing the Development of Safer Technologies

Despite its reputation as a global leader in technological innovation, the United States remains one of the weakest nations in protecting the personal data of its citizens. Rather than prioritizing military projects or profit-driven objectives, investments should be redirected toward research and development of safer technologies. This shift would not only enhance user security but also establish the United States as a model for other nations in the field of privacy protection.

8. International Collaboration

The U.S., which often claims global leadership, lags behind other developed nations in personal data protection standards. Active participation in establishing global data protection norms is the only way for the country to substantiate its human rights advocacy claims.

References

1. IBM. (2023). Cost of a Data Breach Report 2023.
 2. Ponemon Institute. (2023). Cost of a Data Breach Report 2023.
 3. Verizon. (2023). 2023 Data Breach Investigations Report.
 4. Symantec. (2023). Internet Security Threat Report 2023. Symantec (now part of Broadcom).
 5. McAfee Labs. (2023). 2023 Threats Report.
- 



6. Kaspersky. (2023). Kaspersky Security Bulletin 2023.

7. Trend Micro. (2023). Annual Cybersecurity and Privacy Report 2023.

