International Journal of Multidisciplinary Research and Growth Evaluation.

IoT and data privacy management: a microscopic view of the United States Gigantic data Economy

Lekan Afolabi
Information Systems and Data Privacy Professional**,** Department of Information Systems, Auburn University, AL**,** USA

* Corresponding Author: **Lekan Afolabi**

Article Info

ISSN (online): 2582-7138
Impact Factor: 5.307 (SJIF)
Volume: 05
Issue: 02
March-April 2024
Received: 10-02-2024;
Accepted: 13-03-2024
Page No: 891-897

Abstract
The number and complexity of data sets have exploded because of Internet of Things (IoT) revolutionizing data collection and sharing. However, this expansion has also led to significant worries about data security and privacy, particularly in the United States where the data economy is quite large. This study seeks to offer a detailed look at the enormous data economy in the US and explore the effects of IoT on data privacy management.

To do this, a thorough analysis of the body of research on IoT and data privacy management will be carried out. This will cover research on the IoT's effect on data privacy, the situation of data privacy regulations in the US today, and the implementation of data privacy management methods by enterprises. Analysis of data breach cases that have occurred in the US will also be part of the research, with a focus on the data types compromised and the industries impacted.

The study will include recommendations for how businesses may strengthen their data privacy management procedures to safeguard sensitive data against breaches and unauthorized access based on its results. The research will add to the expanding body of information on IoT and data privacy management and educate policymakers about the need to control the data economy in the US.

What are the main difficulties businesses face in safeguarding sensitive data from breaches and illegal access, and how has the use of IoT technology affected data privacy management in the United States? What are the country's present data privacy rules and regulations, and how well do they work to control the data economy? These are the questions that will be answered based on the study topic "IoT and Data Privacy Management: A Microscopic View of the Giant Data Economy in the United States".

Keywords: data privacy, internet of things, data breach, GDPR, data security, CCPA

Introduction

The United States has the world's largest data economy, and data is critical to many aspects of life, including healthcare, banking, and retail. The proliferation of the Internet of Things (IoT) has altered how data is collected, analyzed, and shared, resulting in an explosion in the volume and complexity of data sets. However, IoT implementation has prompted substantial concerns about data security and privacy, particularly in the United States, which has a large data economy.

Due to the enormous amounts of data created by IoT devices, securing sensitive data from breaches and illegal access has become a rising problem for data security. As IoT usage increases, it is critical to comprehend how this technology affects data privacy management in the US.

The goal of this study is to evaluate the effects of IoT on data privacy management and to offer a microscopic view of the enormous data economy that exists in the United States. This study will involve a thorough analysis of the body of research on IoT and data privacy management, including studies that look at how IoT affects data privacy, the state of data privacy laws in the US today, and the ways in which organizations can put data privacy management strategies into practice.

Sensitive data from a variety of businesses have been compromised in a growing number of data breaches in the United States in recent years. Over 600 million sensitive data records were exposed because of the more than 1,100 data breaches announced in the United States alone in 2021. Better data privacy management solutions are now more crucial than ever in protecting sensitive data from breaches and unauthorized access.

The study's findings will provide firms with ideas on how to tighten their data privacy management systems and better protect sensitive data from leaks.

The study's findings will contribute to the body of knowledge on IoT and data privacy management, educate policymakers about the need to regulate the data economy in the United States and assist organizations in implementing efficient strategies to protect sensitive data from breaches and ensure ethical and responsible data use.

Research Methodology

A qualitative research approach with an exploratory study design will be used in this research article. This strategy aims to gain a better understanding of the influence of IoT on data privacy management in the US economy. This will be accomplished by completing a thorough analysis of existing research, publications, and reports on IoT and data privacy management in the US economy.

Primary data will be gathered through online surveys of US citizens and residents to learn about their understanding of IoT and data privacy management. The survey results will be evaluated to discover trends and provide additional insight into the influence of IoT on data privacy management in the US economy.

Secondary data will be gathered from scholarly journals, papers, and publications from respectable organizations such as the Federal Trade Commission, the National Institute of Standards and Technology, and the International Association of Privacy Professionals. The secondary data will give a thorough examination of the present IoT and data privacy management landscape in the United States, including trends, policies, and best practices.

Examples of recent data breach incidents will also be conducted as part of the research to better understand how data privacy management policies and procedures may be modified to prevent future problems. These will examine the circumstances surrounding the breach and the cause of the breach.

Overall, the approach of this research will provide a thorough understanding of the influence of IoT on data privacy management in the US economy, as well as recommendations for best practices to improve data privacy management in the future.

Literature Review

The Internet of Things (IoT) has completely revolutionized how we use technology and is now a crucial aspect of our daily life. IoT device growth has raised further worries about data security and privacy. We will look at the effects of IoT on data privacy management in the US economy in this literature review.

In a study by Elisa Bertion, Department of Computer Science Purdue University, in addition to identifying the crucial aspects of data security, availability, and quality in IoT, the study makes contributions by detailing the difficulties in assuring security, privacy, and safety in IoT systems and summarizing future research paths for protecting IoT data. The examines software protection strategies for small devices, effective and scalable encryption algorithms, and fine- grained data packet loss analysis for sensor networks.

The management of IoT data privacy has been improved by several laws and best practices enacted in the US. Consumers now have the right to seek the deletion of any personal information that has been gathered on them thanks to the California Consumer Privacy Act (CCPA), which was passed in 2018. The CCPA has been praised as a major advancement in the US's data privacy management.

To enhance IoT cybersecurity, the National Institute of Standards and Technology (NIST) has also created a framework. The framework offers recommendations for businesses to follow when putting security measures in place to guard against IoT-related cyber threats.

The importance of managing digital privacy in the current era of the digital economy can't be overemphasized. It highlights the interdisciplinary nature of privacy-related issues and proposes an ontology of digital privacy to foster interdisciplinary research progress. The paper also emphasizes the need for more effective privacy management and regulations to help individuals navigate the digital economy. The development of big data technologies poses severe threats to privacy, but advancements in these technologies also provide new instruments for monitoring and managing digital privacy. Overall, the paper aims to untangle the convoluted discussions about digital privacy and provide a foundation for merged view and practice-focused solutions.

The US economy now heavily depends on IoT devices. However, because IoT devices capture so much data, worries about data security and privacy have grown. The CCPA and NIST framework are just two of the laws and best practices that the US has put into place to enhance IoT data privacy management. The effects of these rules and recommended practices are still being examined, though. Risk management procedures should be used to lessen the impact of data breaches, which continue to pose a danger to the management of IoT data privacy.

Introduction to IoT and definitions

The development of the Internet of Things (IoT) as a technological paradigm has fundamentally altered how we interact with everything around us. The Internet of Things (IoT) is a network of physical items that may link to one another and share data online. IoT is becoming increasingly common in a range of industries, including manufacturing, transportation, agriculture, and healthcare.

IoT's introduction has fundamentally altered how businesses run, resulting in higher productivity, cost savings, and operational efficiency. IoT adoption, however, also has its drawbacks, particularly in terms of infrastructure requirements, interoperability, and data security and privacy. The Internet of Things provides benefits such as greater operational effectiveness, real-time data processing, and remote monitoring and management. The disadvantages of IoT include its vulnerability to assaults, the requirement for sophisticated knowledge, and the need for significant infrastructure investments. The ability to improve client experiences and the opportunity for increased creativity are two opportunities for IoT. IoT hazards include the possibility of data breaches, privacy concerns, and regulatory

compliance issues.

The Internet of Things (IoT) is a network of interconnected physical things, gadgets, vehicles, buildings, and other items embedded with sensors, software, and other technologies that allow data exchange and communication over the internet. IoT devices can gather, analyze, and transfer data in real time, allowing them to optimize and automate various jobs and processes.

The International Telecommunication Union (ITU) provides a commonly accepted definition of IoT as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies".

IoT is becoming more common in a variety of areas, including healthcare, agriculture, transportation, and manufacturing, to mention a few. The potential benefits of IoT are numerous, including higher efficiency, cost savings, increased productivity, and improved customer experiences. However, IoT adoption comes with several obstacles, particularly in terms of data privacy and security, interoperability, and infrastructure requirements.

Market, Trends and Forecast

The Internet of Things (IoT) industry has grown rapidly in recent years, owing to advancements in wireless technology, cloud computing, and data analytics. According to Marketsand Markets, the global IoT market in terms of revenue will be $650b by 2026 presenting a CAPR of %16.7. The United States is the most important market for IoT solutions, accounting for a sizable portion of the global market.

IoT devices are being used in a variety of industries, including manufacturing, healthcare, transportation, and energy. IoT is being used in the industrial industry to optimize production processes, minimize downtime, and improve quality control. IoT devices are being utilized in healthcare to monitor patient health, track medical equipment, and improve care delivery. IoT is being utilized in transportation to improve logistics, cut fuel use, and increase driver safety. IoT is being utilized in the energy sector to optimize power consumption, monitor energy usage, and increase the efficiency of renewable energy sources.

The rising usage of edge computing, which involves processing data at the network's edge, closer to the devices generating the data, is one of several important trends in the IoT sector. This reduces latency, improves security, and reduces the amount of data transported to the cloud for processing. Another trend is the increasing use of artificial intelligence (AI) and machine learning
(ML) technologies to analyze vast amounts of IoT data and extract insights to optimize processes and make better decisions.

Some notable examples of popular IoT inventions include smart houses, wearable devices, smart appliances, and autonomous cars. IoT devices are used in smart homes to control various parts of the home, such as lighting, temperature, and security, whilst wearable gadgets are utilized to monitor health and fitness metrics. IoT sensors are used in smart appliances to minimize energy usage and improve efficiency, while AI algorithms are used in autonomous vehicles to navigate highways and avoid collisions.

According to the survey shared among thirty-five (35) US citizens and fifty-five (55) non-US citizens living in the US, majority of the IoT devices exposed to are personal and household items such as smart tv, smartphone, sound systems etc. 50% of the respondents said their most frequently used IoT device is a smart tv, 29% said they owned an apple watch specifically, 15% said a smart car, 11% went for sound systems.

Fig 1: Types of IoT devices listed by 90 respondents mixed between US citizens and non- citizens

Looking ahead, the IoT market will continue to expand further, driven by rising demand for IoT solutions across a wide range of industries. Industrial IoT (IIoT), which involves the use of IoT devices in manufacturing and industrial settings, and smart cities, which use IoT devices to optimize urban infrastructure and improve quality of life, are two rising areas of interest. However, IoT adoption presents some obstacles, particularly in terms of data privacy and security, which must be addressed to ensure the IoT market's future growth and success.

Data-driven us economy and the invasion of IOT

The United States has a data-driven economy dependent on massive amounts of data collecting, processing, and analysis. The country has been at the forefront of technical innovation and digital transformation, resulting in widespread adoption of IoT devices across a variety of industries. The incorporation of IoT devices into the US economy has resulted in more efficiency, lower costs, and better consumer experiences. This integration, however, has raised concerns about data privacy and security.

The economy of the United States is heavily reliant on data-driven businesses such as finance, healthcare, and technology. Data is utilized in the finance industry to influence investment decisions, control risk, and develop new financial products. Data is utilized in healthcare to improve patient outcomes, lower expenses, and discover novel therapies. Data is utilized in the technology industry to develop new products and services, improve consumer experiences, and optimize operations. The widespread usage

of IoT devices has expanded these industries' ability to collect and analyze data in real-time, resulting in increased efficiency and innovation.

The spread of IoT devices into the US economy has also raised worries about data privacy and security. IoT devices capture a large quantity of data on their users, such as personal information, location data, and behavioral patterns. This information can be used to build detailed profiles of individuals and groups that can subsequently be utilized for targeted advertising or other reasons. However, this raises the possibility of data breaches, identity theft, and other forms of cybercrime.

Aside from these challenges, there are also concerns about the ethical usage of IoT data. As

IoT devices become becoming more prevalent, there is rising concern about the potential for data exploitation. IoT data, for example, could be used to discriminate against specific groups or to violate individual rights and freedoms.

When asked, 80% of the respondents said they were familiar with the notion of data privacy, 58% said they knew just about enough while just 13% said they knew very much about data privacy. 61% said they cared very much about their privacy while 29% said just about enough care is given to it. 60% said they are very informed about their rights towards data privacy. When asked how many were concerned about their privacy specifically using IoT devices, 43% opted for "somewhat concerned" while 32% said they were very concerned with just 2% saying they are very unconcerned.

Overall, the spread of IoT devices into the US economy has had a significant impact on how data is gathered, processed, and evaluated. While technology has improved efficiency and innovation, it has also created serious concerns about data privacy and security. As the Internet of Things industry expands, it will be critical to address these concerns and ensure that the benefits of IoT technology are realized in responsible and ethical manner.

Popular Names in the IOT Industry

The IoT sector is a quickly growing and dynamic field, with numerous firms and organizations leading the way in terms of IoT technology research, development, and implementation. Some of the most well-known and prominent industry names in the IoT field are:

1. AWS (Amazon Web Services)
2. Google
3. IBM
4. Microsoft
5. GE (General Electric)

These firms are active in a variety of IoT-related activities, ranging from providing cloud-based IoT platforms and infrastructure to producing hardware and software solutions for IoT devices. Start-ups, research institutes, and government organizations are other prominent actors in the IoT market, all of which are contributing to the growth and development of this interesting field.

Key Challenges

Companies in the IoT industry face a few challenges when it comes to protecting sensitive information of US residents from breaches.

1. Security Risks: IoT devices frequently lack the security procedures required to protect against cyber-attacks. As a result, they are subject to hacking and other types of cyber assaults, which can compromise user data and expose personal information.
2. Data Collection and Storage: IoT devices generate massive volumes of data, which must be securely kept. This is a challenge for businesses since they must ensure that data is securely stored and only available to authorized individuals.
3. Data Sharing: IoT devices frequently share data with other devices and applications, posing privacy concerns. Companies must ensure that data is shared securely and only with those who need it.
4. Regulation Compliance: Companies working in the IoT field must adhere to data privacy and security rules. This might be difficult because regulations are continually changing and differ by jurisdiction.

Impact of IOT on data privacy management

The growing use of IoT devices in the United States has had a substantial impact on data privacy management. Data is collected in real- time and analyzed to make decisions using IoT devices, which presents both benefits and concerns for data privacy. With a microscopic view of the US population and data-obsessed economy, the following are some of the most significant consequences of IoT on data privacy management:

1. Increased Data Collection: IoT devices capture massive amounts of data about its users, such as personal information, location data, and behavioral patterns. This information is then used to build detailed profiles of individuals and groups that can be utilized for targeted advertising or other reasons. This expanded data collection creates privacy and security issues.
2. New Privacy Risks: IoT devices can introduce previously unknown privacy risks. Smart home gadgets, for example, can monitor activities and conversations within a home, allowing for the creation of a complete picture of a person's daily life. Advertisers or malevolent actors may find this information useful.
3. Cybersecurity Threats: IoT devices are frequently insecure, making them subject to hacking and other types of cyber assaults. This jeopardizes personal information and has serious ramifications for data privacy management.
4. Ethical Concerns: As IoT devices become more common, there is rising worry about the possibility for data exploitation. IoT data, for example, could be used to discriminate against specific groups or to violate individual rights and freedoms.
5. Legal Disputes: The increased use of IoT devices has given rise to legal issues about data privacy and security. Clear standards and guidelines are required to preserve user privacy and ensure that IoT data is collected and used appropriately.

Because of the country's data-obsessed economy, the impact of IoT on data privacy management in the US is of special importance. The United States has a data-driven economy that relies largely on data-driven businesses including finance, healthcare, and technology. The incorporation of IoT devices into various businesses has resulted in greater efficiency, lower costs, and better consumer experiences. This integration, however, has raised worries about data privacy and security.

To address these concerns, attempts have been made to create

new norms and regulations concerning IoT and data privacy management. The California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR) in Europe, are examples of rules aimed at preserving user privacy in the context of IoT.

Overall, the Internet of Things' impact on data privacy management in the United States is complex and multidimensional. While the integration of IoT devices has resulted in tremendous benefits, it has also introduced new obstacles and concerns in terms of data privacy and security. It is critical to address these problems by clear regulations and guidelines to ensure that the benefits of IoT technology are exploited in a responsible and ethical manner.

IOT and data breaches

The Internet of Things (IoT) is becoming more common in our daily lives and commercial operations. However, because of the large volume of data captured and communicated by IoT devices, it has also become a prominent target for hackers. As a result, numerous data breaches have occurred in the United States over the last decade, emphasizing the vulnerability of

IoT devices and the significance of data privacy management

A regular IoT user in the US isn't aware if their privacy has been breached. According to the survey, 81% said they aren't aware of any breach by their IoT device even though security intelligence reported that just by half of 2021, over 1.5 billion attacks on smart devices with hackers looking to steal sensitive data.

Several high-profile data breaches in the United States over the last decade have resulted in the loss of millions of people's personal and financial information. Many of these breaches have been related to Internet of Things (IoT) devices, which are growing more common in American homes and companies. In this section, we will look at some of the most notable data breaches that have happened in the United States over the last decade, as well as the preventive actions that may be used to strengthen the security of IoT devices.

In 2018, a vulnerability in a third-party software utilized by MyFitnessPal, a popular fitness and health monitoring app, resulted in the exposing of 150 million user accounts. Usernames, email addresses, and passwords were all compromised.

A vulnerability in the Ring, a popular smart doorbell system owned by Amazon, exposed users' Wi-Fi credentials in 2019. Hackers were able to gain access to Ring subscribers' home networks, potentially exposing other linked devices to cyber threats.

These incidents highlight the need for robust data privacy management practices in the IoT industry. It is crucial for companies to implement security measures such as regular software updates, password policies, and encryption to protect users' sensitive information from being compromised. Moreover, the recent data privacy laws such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR) mandate the implementation of security controls and proactive risk management by the companies that handle sensitive user data.

The use of IoT devices expands the risk of data breaches will remain a major worry. Companies must take proactive steps to deploy security measures and ensure that users' sensitive information is protected. The consequences of these breaches might be disastrous for both individuals and corporations.

Through measures like as the Cybersecurity Information Sharing Act of 2015 and the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the US government has taken steps to increase IoT security (National Institute of Standards and Technology, 2018). These programs provide best practices and guidelines for strengthening the security of IoT devices and networks, and they can be a significant resource for people and companies looking to improve their own security posture.

Data Privacy Laws

To protect consumers' personal information, the United States has many data privacy rules and regulations in place, including those relevant to the IoT business. These laws and regulations are intended to safeguard the confidentiality, integrity, and availability of sensitive data acquired by IoT devices.

The General Data Protection Regulation (GDPR), which went into effect in 2018, is one of the most important global data privacy legislations recognized in the United States. The GDPR establishes stringent regulations for organizations operating in the EU, including those collecting and processing personal data via IoT devices. The GDPR compels businesses to seek explicit agreement from users before collecting personal data, and to put strong security measures in place to protect that data.

In addition to the GDPR, the United States has various other data privacy and security rules and regulations, including

1. California Consumer Privacy Act (CCPA): This law, which went into effect in 2020, applies to businesses that do business in California and collect personal information from citizens of California. Consumers have the right under the CCPA to know what information is being collected about them, to request that their information be erased, and to opt out of the sale of their personal information. The California Consumer Privacy Act (CCPA) is a broad data privacy law that took effect on January 1, 2020. To comply with the law, the CCPA gives California consumers more control over their personal information and compels firms operating in California to establish new data privacy practices. The CCPA applies to Internet of Things devices that collect personal data from California citizens. Consumers have the right under the CCPA to know what personal information is being collected about them, to request that their information be deleted, and to opt out of the sale of their personal information. Businesses must also give consumers with a privacy policy that discloses their data collection procedures, and they must seek consumers' explicit consent before collecting or selling their personal information. The CCPA outlines various data privacy management challenges for IoT devices. Consumers' personal information is frequently collected by IoT devices, including location data, device IDs, and use statistics. This data can be used to create extensive consumer profiles, which can then be sold to third parties for marketing and advertising purposes. To comply with the CCPA, IoT companies must implement new data privacy policies, such as gaining explicit agreement from customers before collecting their personal information

and giving consumers the choice to opt-out of the selling of their personal information. The CCPA also includes data security regulations, which require enterprises to employ reasonable security measures to protect consumers' personal information from unlawful access, disclosure, or destruction. This includes adopting robust encryption and authentication methods for IoT devices to ensure that data is sent and kept securely. Overall, the CCPA poses major obstacles for California-based IoT companies, as they must comply with new data privacy and security regulations to avoid legal and financial fines. The regulation also protects customers' personal information by allowing them more control over how corporations gather and utilize their data.

2. HIPAA: The Health Insurance Portability and Accountability Act governs the use and disclosure of personal health information. HIPAA restrictions apply to IoT devices that collect health information.
3. The Children's Online Privacy Protection Act (COPPA) governs the acquisition of personal information from children under the age of 13. Internet of Things devices that capture personal information from children are subject to COPPA regulations.
4. Federal Trade Commission Act (FTC Act): The FTC Act empowers the Federal Trade Commission (FTC) to investigate and act against organizations that engage in unfair or deceptive data privacy and security practices.

Overall, these laws and regulations serve to protect consumers' personal information while also holding IoT companies accountable for maintaining solid data privacy and security policies. Companies in the IoT market must follow these standards to avoid legal and financial penalties, as well as to keep their consumers' trust.

However, 52% of the respondents said they are not aware of any government regulations and policies related to data privacy and security concerning the use of IoT devices.

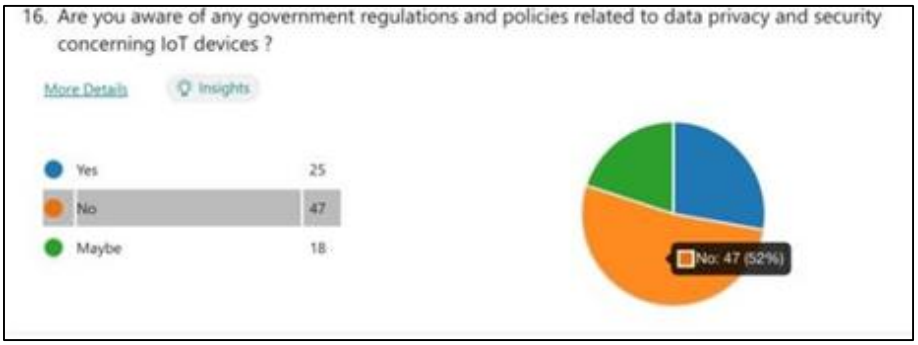

Fig 2: A screenshot of the response from survey participants

Best practices for data privacy management in the iot industry

It is not surprising that when asked, 49% of the respondents said they don't trust their IoT product or service companies to adequately protect their privacy.

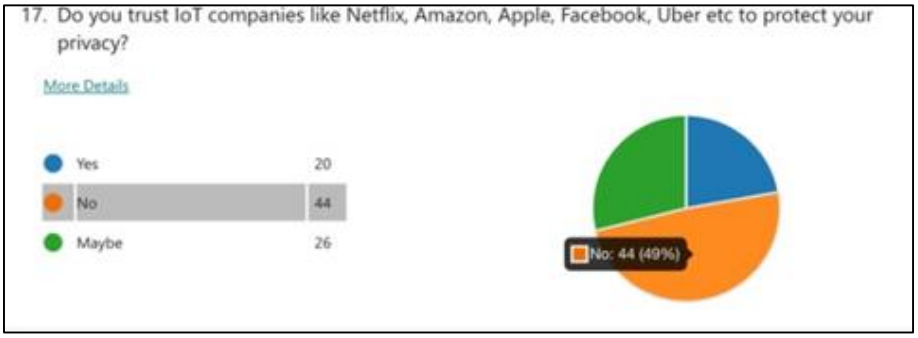

Fig 3: A screenshot of the response from survey participants.

Effective data privacy management is required to ensure the security and privacy of sensitive data gathered by IoT devices and this will help them build trust with their customers. Some of the best practices for managing data privacy with IoT are:

1. Data Protection Impact Assessment: Before installing an IoT system, firms should undertake a PIA to identify potential privacy issues and devise mitigation solutions.
2. Put in place robust data security measures: IoT devices should be built with strong encryption and authentication methods to ensure that data is securely delivered and stored.
3. Data Minimization: Businesses should only gather the information required to offer the intended service and should avoid collecting sensitive personal information unless essential.
4. Obtain express consent from customers: Before collecting personal information from consumers, businesses should obtain explicit consent from them and offer them with the option to opt-out of data collection.
5. Establish clear privacy policies: Businesses should establish comprehensive privacy policies that clearly outline their data gathering processes and teach consumers about their rights.
6. Educate employees on data privacy: To avoid inadvertent data breaches, all employees who handle sensitive information acquired by IoT devices should be trained on data privacy best practices.

7. Update IoT devices on a regular basis: Businesses should update IoT devices on a regular basis to address security vulnerabilities and maintain compliance with data privacy rules.
8. Conduct Third-Party Audits: Businesses should conduct third-party audits of their data privacy and security procedures to detect potential risks and assure compliance with applicable requirements.
9. Perform Regular Security Audits: Businesses should perform regular security audits to detect and remediate possible vulnerabilities in their systems. This can aid in the prevention of data breaches as well as the compliance of businesses with data privacy rules such as HIPAA.
10. Establish Data Retention Policies: Businesses should establish data retention policies that indicate how long data should be stored and when it should be removed. This can help lower the risk of data breaches while also assisting businesses in complying with data privacy rules such as the GDPR.
11. Give Customers management Over Their Data: Businesses should give customers the ability to manage how their data is collected and used. This can include allowing customers to opt out of data collecting or request that their data be removed.

Implementing these best practices can assist organizations in protecting the privacy and security of sensitive data acquired by IoT devices, as well as in increasing customer trust in IoT technology. Finally, there are various best practices that businesses may use to ensure that consumers' personal information is protected. Companies can help mitigate the risks associated with data privacy and security in the IoT space by implementing strong encryption and authentication protocols, minimizing data collection, implementing data retention policies, giving consumers control over their data, conducting regular security audits, providing employee data privacy training, and conducting third-party audits.

Conclusion

Finally, the Internet of Things (IoT) has become a vital aspect of the data-driven economy in the United States, with widespread adoption in a variety of sectors. The growth of IoT devices, on the other hand, poses a substantial challenge to data privacy management, with the potential hazards of data breaches, cyber-attacks, and other security concerns. Recent data breach instances in the United States have highlighted the need for better data privacy management practices and robust security systems to protect sensitive information of US individuals.
This research study investigated the effects of IoT on data privacy management in the United States, highlighting the significant issues encountered by IoT companies and the legislative framework in place to control the industry. We identified best practices for data privacy management with IoT through a comprehensive literature study and offered strategies for US organizations to align their IoT infrastructure to comply with GDPR/data protection rules and improve their data management practices.
The data privacy landscape is clearly shifting, and businesses must keep up with emerging trends and technology to appropriately protect client data. This necessitates a comprehensive approach to data privacy management that includes not only technological solutions but also organizational policies, staff training, and risk management measures that are effective.
To summarize, the potential benefits of IoT are enormous, but so are the risks. As a result, it is critical for US businesses to prioritize data privacy management and invest in strong security measures to safeguard sensitive information. Companies can create trust with their customers and preserve a competitive edge in the data-driven economy by doing so.

References

1. Al-Fuqaha M, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials. 2015; 17:2347.
2. Biswas S. Data breaches in the United States: Trends and implications. Journal of Cybersecurity. 2022; 7:45.
3. Bertino E. Data Security and Privacy in IoT. Open Proceedings. 2016.
4. Chi HR. Editorial: Edge Computing for the Internet of Things. Journal of Sensor and Actuator Networks. 2023; 12:17.
5. Salam. Internet of Things for Sustainability: Perspectives in Privacy, Cybersecurity, and Future Trends. Purdue e-Pubs. 2020.
6. Johnson RW, Smith KM, Williams AD. Regulating the data economy: Current issues and emerging trends. Journal of Policy Analysis and Management. 2019; 38:433.
7. Kumar JS, Patel DR. A survey on internet of things: Security and privacy issues. International Journal of Computer Applications. 2014; 90.
8. Mocrii D, Chen Y, Musilek P. IoT-based smart homes: A review of system architecture, software, communications, privacy and security. Internet of Things. 2018; 81.
9. Mohsen, Niraj K. A Comprehensive Study of Security of Internet-of-Things. IEEE Xplore Digital Library. 2016.
10. Wang, Zhan N, Wang C. Managing Privacy in the Digital Economy. Fundamental Research. 2021; 1.
11. Zhou W, Jia Y, Peng A, Zhang Y, Liu P. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. IEEE Internet of Things Journal. 2019; 6:1606.
12. https://leginfo.legislature.ca.gov/faces/ billTextClient.xhtml?bill_id=201720180 AB375
13. https://nvlpubs.nist.gov/nistpubs/CSW P/NIST.CSWP.01162020.pdf
14. https://techcrunch.com/2019/11/07/a mazon-ring-doorbells-wifi-hackers/
15. https://securityintelligence.com/article s/iot-security-internet-forgotten-thing/
16. https://www.cnbc.com/2018/03/29/un der-armour-stock-falls-after-company- admits-data-breach.html
17. https://www.marketsandmarkets.com/ Market-Reports/internet-of-things- market-573.html