Data Ownership in the Digital Age

Mr. Vimal Bhaliya
Assistant Professor in BCA

Mr. TahaTravadi
Lecturer in BCA
Smt. B. V. Dhanak College,
Bagasara

In today's quickly changing digital world, data has become a valuable resource for both businesses and people. Recently, companies are always creating chat programs and other tools that gather user information to help them grow and make money. But during this process, they often forget that using user data can put data security and privacy at risk, making it easier for cyber attacks and data leaks to happen. That's where data ownership becomes important.

What is Data Ownership?

Data ownership means the rules and guidelines that app developers or businesses must follow when they work with or manage user data. It also means that you, as the person in charge, are responsible for handling all data, whether you are storing, changing, or deleting it, from your own server or cloud storage.

Why do you need data ownership?

As a business, owning an app means a complete responsibility to own user data, right from their detailing to deleting. And below are some of the reasons as to why you need to own your app data:

1. Data Portability

Data portability means you can take your app data and move it from one place to another, either physically or digitally, whenever you choose. Many apps now have to let users export their data as a way to protect their privacy.

This was started when Google gave users the option to delete or move their contacts, files, search history, emails, and other information stored in Google's services a decade ago. Since then, other apps like Twitter and Facebook had to follow suit and offer similar options. It's also required that every business allows users to move their data from a dedicated cloud storage system to their own on-premise server or to another competing platform, and they should only charge for the bandwidth that was actually used.

One of the main reasons data portability matters is because of the flexibility it offers. If you're not happy with your service provider or a third-party vendor, or if you think your data could be better used elsewhere, you can easily switch. But be careful not to get locked in. The term 'lock-in' has become a common strategy used by many B2B providers to keep customers dependent on their services.

2. Privacy

In the past, data privacy wasn't something most people talked about. It was mainly discussed by activists and a few experts. But things changed quickly when the public started learning about how companies use personal information. A recent study by Pew found that 79% of Americans are unhappy with how their data is being used.

This means that if you have an app that stores user data, people are trusting you with their personal details. That includes not just private information, but also things like your e-commerce sales, customer feedback, and even financial data. If your app has a payment system, it might also be storing sensitive info like credit card numbers, expiration dates, and billing addresses. So, privacy is a big issue now. App owners and businesses should understand that data isn't something you can treat as a product you can sell or share whenever you want. Even a small mistake or a leak can damage trust, lose respect, and hurt your business in the long run.

3. Security

Just like a small privacy mistake can become a big news story, companies are taking strict steps to protect user data. The internet is protected by many security rules and standards that help collect and manage data safely. Some of these standards, like SOC2, are made by private companies, while others, such as GDPR, HIPAA, and US laws, are created by lawmakers and government agencies to make sure people's data stays private and secure.

Following these rules carefully when launching an app can really help improve how the app is used. Because of this, many SaaS and cloud service businesses build their plans around these standards. However, top in-app chat API providers like Stream and Sendbird charge extra for compliance with these standards. So, it's up to you to choose the standards that fit your business and take the right steps.

Data ownership, security, and keeping data accurate are very important in today's digital world. To deal with these issues, businesses can also use data warehouse tools. A data warehouse tool stores data in one place and has strong security features. This makes it a safe and dependable way to keep data secure, ensures that data stays accurate, and helps manage it more efficiently. Using such a tool can greatly improve data security and accuracy for businesses in today's fast-changing digital environment. Now that we've seen why businesses need to understand the basics of data ownership, our next topic is why it's a formal role in every company.

Why is Data Ownership important?

Data ownership and data stewardship are the two important topics that many businesses often tend to miss from their schedule.

As people talk about different jobs, processes, systems, and market resources, they often ignore their data for years or months. However, setting up clear data ownership is an important step that all companies should take. Here are two main reasons why data ownership matters.

1. Manage Data Integrity: In this case, data integrity means keeping data trustworthy and correct throughout its entire life. It means checking if the data is still valid or if it has become outdated. Even when companies use data engineering tools, they often don't make decisions based on data regularly without paying attention to its integrity. These kinds of decisions can greatly affect business goals. A recent KPMG report shows that most senior executives are unhappy with how companies handle user data. This shows that customer feedback is becoming more important in shaping data privacy rules and making business operations more transparent.

2. Data is a Competitive Advantage: Many businesses today use data to help achieve their goals. Through data ownership, companies can clearly define, measure, and check the success of any project they are working on using their own data. You Can Take Action From Your Data: To understand what actions you can take from your data, you need to know the main purpose of the data you hold in each area.

For example, if you are a manufacturing company, your focus would be on machine performance, while for B2B companies, it would be on increasing leads. Similar logic applies to other types of businesses. Once you know your goals, you can focus on how to use your data to help your business grow. So, we've covered the three main reasons why data ownership is important. But you might be wondering if keeping data accurate is really that simple.

Different Data Ownership Rights/ Paradigms

Below we will see 10 different data ownership paradigms that best explain whether the data holds single ownership or multiple ownership.

1. Data owner is someone who creates data – If an organization, entity, group, or individual creates or generates data, then they must be the owner of that particular data which is indicative of **single ownership.**

2. When a consumer of data is its owner – This refers to multiple groups or entities like Walmart, Lowes, or Home Depot who collect user information from various sources to predict their metrics. This is indicative of **multiple ownership.**

3. Data owner is someone who compiles data: This is yet another example of **multiple ownership** where entities like Google, Yahoo, and LinkedIn gather data from different sources and make it available on their search engines.

4. An enterprise that accumulates data – Here, enterprises can claim ownership of data that they would have accumulated over time. And it is indicative of **multiple ownership.**

5. Fundraisers or organizations as data owners: This is an example of **single ownership** that depicts funding organizations that would have commissioned the creation of data for ownership.

6. Decoder of data as owner – Any person or entity who decodes the encoded data is said to be a rightful owner of that information and it is an example of **single ownership.**

7. Packager of data as an owner – Any person or entity who packages an individual's or group's product can claim ownership of data and it is an example of **multiple ownership.**

8. Reader of data as an owner – A person who reads and gains knowledge of any information from the repository and uses it for their future work is said to be an owner. It is an indicator of **multiple data ownership.**

9. Licenser of the data as the owner – A buyer or licenser who purchases or licenses data, respectively, could claim data ownership because of the investment. It is indicative of **multiple data ownership.**

10. All are data owners – This is a scenario of global or **multiple data ownership.**

Privacy Concerns in the Digital Age

Privacy issues are a big topic when it comes to who owns our personal information. In today's digital world, a lot of our personal data is being collected, kept, and studied by many different groups. This data can show a lot about our lives, which is why protecting our privacy is really important.

One main worry is the possibility of data breaches, where private information can be leaked or taken by bad people. Also, companies often use data mining and profiling to learn about us, which can lead to our personal details being used in ways we might not agree with. This can affect our privacy and the freedom we have over our own information. Another issue is how clear companies are about how they collect and use our data. Many people don't know just how much information is being gathered or what it's being used for. This lack of clarity can make people feel like they're losing control of their personal data, which can make them less trusting of the websites and services they use.

Responsibilities of Data Custodians

Data custodians, like businesses and groups that collect and manage information, have important duties to make sure people's data stays private and secure. These duties include:

1. Being clear about how they collect data, why they collect it, and how they plan to use it. They should explain this to the people whose data they handle.

2. Keeping data safe by using strong protection methods to stop hackers and people without permission from accessing it.

3. Following rules and laws that protect data, such as the GDPR in Europe or the California Consumer Privacy Act in the U.S.

4. Taking responsibility for the data they work with, which means regularly checking their systems and making sure they follow all data protection standards.

5. Using data in a fair and responsible way, making sure they respect people's rights and privacy, and not doing anything that could hurt people or the community.