Strategic Services Marketing

Prof. Kalpak Kulkarni

Department of Management Studies,

Indian Institute of Technology, Roorkee

Week – 05

Lecture - 25

Ethical Considerations in Handling Customer Data

Hello everyone. In this session, let's recognize the ethical considerations in handling customer data with respect to services. Handling customer data comes with significant ethical responsibilities, and it is crucial for businesses or service providers to prioritize the protection and fair treatment of this sensitive information. Ethical considerations in handling customer data encompass a range of principles and practices to ensure transparency, respect for privacy, and overall responsible data management. But before going forward, let's understand what is customer data. Customer data is information held on file about customers by a store or any other business, usually including names, contact details, and buying habits.

There are different types of customer data that service providers encounter with or collects in process of either promoting services or delivering the services as well. So, the four basic types of customer data includes number one basic data, interaction data, behavioral data, and attitudinal data. Let's understand these in detail. First type is basic or identity data.

The basic customer data includes a customer's, for example, name, postal address, email address, gender, phone number, age and birthday, and so on. So, basic or identity data is just that it's the basic information you gather from your customers that identifies them as unique individuals. Second type is interaction or engagement data. Interaction or engagement data refers to data related to how your customers interact with your business across various touchpoints. Customer engagement and interaction data comes in the form of website visits, click through rates or CTRs, bounce rate, website visiting and then leaving the website in between or midway.

Convergence, we have ad engagements like reach, click, and interactions. Social media post and video engagement and even engagement with the emails. Third type of data is behavioral data. Behavioral customer data is similar to customer interactions data, but a little more defined. Behavioral data looks at customers direct engagement with your business.

This includes, for example, purchase history, abandoned shopping carts, subscription renewals and cancellations, product order values, user duration on your website, or heat maps for mouse movement data like clicks and scrolling like where on the exactly website the customer is spending more time, which are the product pages where he is spending more time on. So, that kind of data falls under behavioral data. Then comes attitudinal data. Attitudinal data is comprised of first-hand opinions from customers on your business, services or even products. Unlike the previous three types of customer data, attitudinal data is a bit harder to process.

For example, it comes in the form of customer and client reviews, online survey responses, in-person interactions with the customers, and even word of mouth reviews. So, before going forward, let's understand the second component of the session that is ethics. So, we are dealing with customer data and how to handle it with some ethical considerations. So, but what is ethics then? Ethics refers to a set of principles or moral guidelines that govern the conduct of individuals, groups, or even organizations. Ethics provides a framework for distinguishing between right and wrong, and it guides decision making based on values such as honesty, integrity, fairness, and respect for others.

Ethics can be applied to various aspects of human behavior, including personal conduct, professional practices, and societal norms. And that is where also it comes how you are going to collect and handle the data of your customers. There are also some ethical responsibilities exist. So, let's understand how ethics with respect to let us say one stage of collecting data is most important for other organizations as well. So, have a look at this particular video wherein we saw how ethics plays a crucial role while collecting and processing customer data.

Just because all this data can be collected, is it ethical to do so? And how do you think that people in this room and elsewhere should think about, we will get into some of what the new data sets out there are, but how do you think about that? I think there is a kind of orthogonal. I mean, you know, why are we hitting big data? We are hitting big data age. We are hitting big data age for basically one big reason, which is that as our life is increasingly measurable, and that started with the internet, which could measure what we did, is now our lives. In your pockets, you have basically a data acquisition device, your phone, which has the capacity to generate more data about every day than you have had in your entire life from your doctors and medical history. This is the phrase called data exhaust.

You know every one of you right now is generating actionable data about your own personal health, your body temperature, your chemical effluents, your heart rates, where you are, all this kind of stuff, your neurological system, it's all measurable. The phone in your pocket could do a little bit of it right now, but ultimately it will do more. So, there is nothing unethical about collecting this data. Your phone could do it. The questions are all about how do we use it.

Is it something that you yourself use to make better choices about your life, or is it something that institutions, including possible insurance companies, would use about you? We've seen that picture. It's called the internet. What we know about, because the internet also had the ability to track everything you do, we had to work through things. What we learned about it is that one size doesn't fit all. That you can't apply a global standard of privacy.

That is fundamentally one generation has different views than the others. The Facebook generation has different views than the pre-Facebook generation. But fundamentally, to get back to vet counters point, it's all about transparency. Everybody should have a very clear dial that sort of says, where do I want to set my personal transparency, if you will, my personal privacy. And I should have the consequences of turning it up to 11.

And if I don't want it there, I should be able to turn it down to two. And just being able to communicate what the consequences of that decision is, is the hardest problem. Going further, now let's understand there are five basic principles of data ethics. These are ownership, transparency, privacy, intention, and outcomes. Let's discuss each one of these one by one.

First principle of data ethics deals with ownership. The first principle of data ethics is that an individual has ownership over their personal information. Just as it's considered stealing to take an item that doesn't belong to you, it's unlawful and unethical to collect someone's personal data without their consent. So that is the principle of ownership. Next principle deals with transparency.

In addition to owning their personal information, data subjects have a right to know how you are planning to collect, store, and use that data. When gathering data, exercise transparency. Let your customers know how their information is going to be used by you as a service provider. Another principle is privacy. So this ethical responsibility that comes with handling data is ensuring data subjects privacy.

Even if a customer gives you a company a consent to collect, store, and analyze their personality identifiable information, that is PII, that doesn't mean they want it publicly available. So you as a service provider needs to take care of that privacy concerns. Next principle is about intention. When discussing any branch of ethics, intentions matter. Before collecting data, ask yourself why you need that particular data, what you'll gain from that, and what changes you'll be able to make after analyzing that kind of data.

If your intention is to hurt others or make some profit from your subjects weaknesses or any other malicious goal, it's not ethical to collect that kind of data from those customers. And the final principle deals with outcomes. Even when intentions are good, the outcome of data analysis can cause inadavament harm to the consumers or individuals. This is called a desperate impact, which is outlined in the Civil Rights Act as unlawful act. So make sure that you are taking care of outcomes which are again falling in terms of ethical responsibilities.

So in order to understand the data ethics and its impact on customer service, have a look at this particular video that talks more about this in detail. Going forward, now let's discuss some best practices for ethical handling of customer data with respect to services. So the first best practice is to go for transparency and consent. So the best practice is to clearly communicate customers how their data will be used and seek their explicit consent to use that kind of data. For example, when a user signs up for a new online service, the platform provides a detailed privacy policy explaining what data will be collected, how it will be used, and gives the user the option to agree or disagree as well.

Second best practice is with respect to data minimization. So collect only the best data that is necessary for the particular internet purpose and avoid excessive or irrelevant information gathering. For example, an e-commerce platform collects only essential information for processing and delivering an order to the customer. For example, address, name, mobile number, and so on. Third best practice is to go for security measures.

Implement robust security measures to protect customer data from unauthorized access, breaches, or even cyber attacks. For example, a financial institution uses encryption, firewalls, and even multi-factor authentication to secure customer financial information and prevent unauthorized access for that particular data. Another best practice is regular audits and assessments. So the best practice here is to conduct regular assessments and audits of data, handling practices to identify and address potential vulnerabilities and even compliance gaps. So for example, an online service periodically engages third-party cybersecurity firms to conduct penetration tests and audits to ensure the security of their systems.

Next best practice is with respect to data accuracy. Try to ensure that the accuracy of the customer data by regularly updating and validating those information. For example, an email marketing platform routinely cleanses its subscriber list by removing inactive or incorrect email addresses to maintain accurate contact information of their customers. Another best practice is to go for data retention policies. Establish clear policies for how long customer data will be retained and securely dispose of data if it is no longer required or necessary.

For example, a health care provider follows industry regulations by retaining patient records for a specific period and then securely destroys them after the retention period has passed. Another best practice is customer access and control. Give customers control over their own data, allowing them to access, update and even delete their information. For example, a social media platform enables users to review and modify their privacy settings, including choosing who can see their post and what personal information should be visible to others and so on. Another best practice is to go for third-party data handling.

With and establish clear agreements with third-party vendors or even partners regarding the handling of customer data. For example, a cloud-based customer relationship management system provider ensures that their subcontractors adhere to the same high standards of data security and privacy. Another best practice is with respect to employee training and awareness. So the best practice is to provide ongoing training to employees regarding data protection policies and the ethical handling of customer data. For example, a tech company conducts regular privacy and security training sessions for their employees, just to keep them informed about the latest best practices and regulations as well.

Next best practice is with respect to incident response plan. Develop and regularly update an incident response plan to address data breaches promptly and transparently. For example, a retail company has a detailed incident response plan that outlines the steps to take in the event of data breach. This includes notifying affected customers and authorities in a timely manner. So, in this session, we try to understand the ethical considerations specifically with respect to customer data and with special reference to services marketing and how it is important to adhere to these ethical responsibilities while handling customer data. Thank you.