KOBIE REVIEW

CUSTOMER DATA:

LIABILITY BEFORE ASSET.

A KOBIE PUBLICATION

Q2, 2018

Contents

Executive Summary

Trust that personal data will be handled appropriately is gaining in importance as a brand differentiator. While companies are becoming increasingly effective at collecting and harvesting customer data to enhance the customer experience and drive profitability, they must also elevate their game when it comes to safeguarding that data. Customer privacy expectations are rising and companies will need to develop strategies that address key elements of this value exchange.

Brands that successfully harness customer data to create personalized experiences and communications to drive customer relationships, separate themselves from the competitive pack. A recent study by the Harvard Business Review indicates that personalization can lift revenues by up to 15 percent, and increase the efficiency of marketing spend by 10 to 30 percent.[1] Delivering data-driven personalized experiences based on trust gets to the heart of all emotional loyalty efforts.

Given the mounting data security problems experienced by leading brands such as Facebook, Home Depot, and Panera, along with the new General Data Protection Regulation (GDPR) legislation in the European Union, it would be premature to dive into how companies are turning data into insight and effective communications without first addressing data privacy and security. Unless a brand has proven, and continues to prove, they are good stewards of their customers' data, they run a growing risk of losing trust with their customers and ruining the very relationships they are seeking to develop. According to a September 2017 study by PwC, only 12% of consumers said they trust companies more than they did a year ago.[2]

This paper covers the importance of brand trust and how customer data is, in fact, a liability that requires proper stewardship well before it becomes an asset. We will explore the risks of ruining customer trust from careless or inappropriate use of customer data, and how to develop and safeguard that trust.

Value Exchange

57%

OF CONSUMERS

WILL STOP DOING BUSINESS WITH A COMPANY THAT HAS BROKEN THEIR TRUST

In general, consumers have accepted the value proposition – I will give you certain information about myself and in return you will provide additional value in the products or services I buy from you, usually in the form of added customization or convenience. Supporting this mutual value exchange is the requirement that the customers' data is kept secure and their privacy is respected. If these requirements are missing, the customer backlash can be staggering – 57% of consumers will stop doing business with a company that has broken their trust and 40% plan to switch to the competition due to trust issues[3], and 8 out of 10 consumers won't do business with companies they do not trust.[4] Trust and loyalty from a customer is something that brands cultivate and build up over time, but it can also be wiped out in a matter of seconds.

Consumers are Jaded AND Demanding More

The customer data landscape is getting more and more treacherous. Major data breaches and stories of improper uses of customer data are almost a daily occurrence now. The steady drumbeat of data privacy and security problems from well-known brands that millions of consumers shop and use every day is having a very real impact on consumer perception and behavior. Recent surveys conducted by Cognizant and Gemalto indicate the alarming degree to which consumers are concerned about the use of their personal data and the limited control they feel they have over it.

Recent surveys conducted state:

- ***91%** of respondents are "concerned" or "very concerned" about the privacy of their data online.*[3]
- ***53%** do not believe companies do what they say they will do to protect their customers' private data.*[3]
- *Data breaches affect many consumers – **31%** have been a victim of a data breach and **27%** have been a victim of fraudulent use of personally identifiable (PI) information.*[5]
- *Breakdown of trust – **75%** of consumers surveyed believe companies do not take the protection and security of their data very seriously.*[5]

This consumer skepticism is rooted in the harsh reality that many companies are not properly safeguarding their customer data. They are playing catch up – trying to balance aggressive data collection, personalization and monetization strategies with growing consumer concerns and expectations about the data being collected on them. These expectations change based on the type of data and the uses of the data. Let's take a closer look at these differences in consumer expectations.

91% ARE CONCERNED ABOUT THE PRIVACY OF THEIR DATA ONLINE

NOT ALL DATA IS CREATED EQUAL

and different data gets used in different ways. Both of these are important for understanding how consumers think about the data you are collecting on them. The differences are important to know before building an action plan for protecting, managing, and harnessing customer data as part of your business strategy.

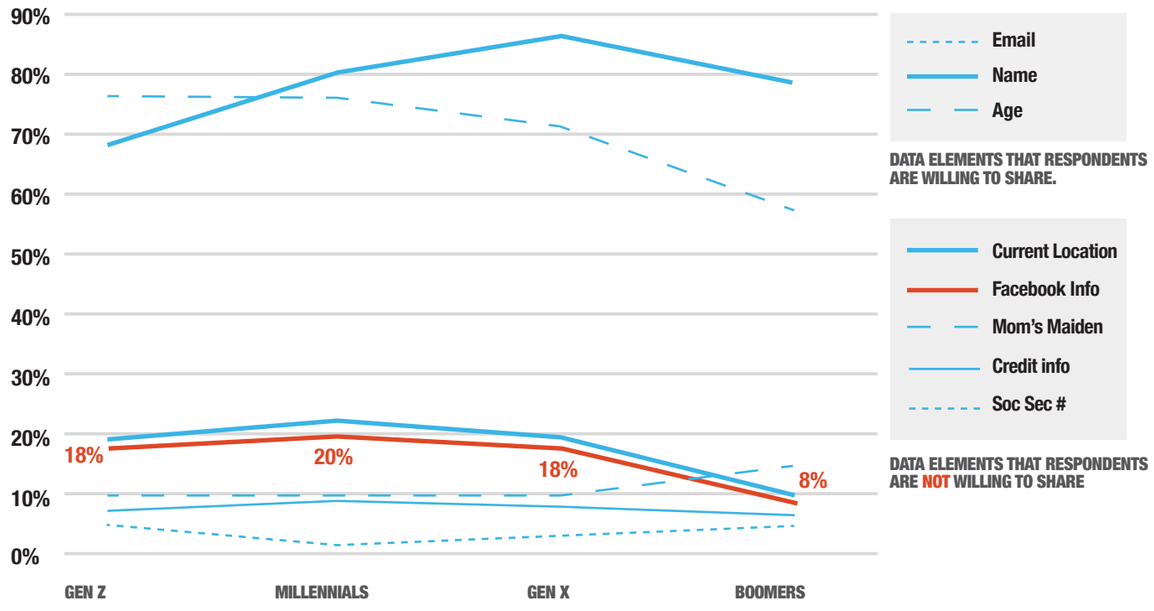
Consumer Expectations

There are four main sources of data with varying levels of value that consumers attach to each:

1) **Self-Reported Data** – information that your customers volunteer about themselves such as gender, purchase preferences, and some types of contact information. This data is usually the least sensitive for customers. However, that attitude can change radically depending on the type of data requested.
2) **Third Party Data** – usually demographic or firmagraphic data purchased from providers such as Experian or Alliance Data. Consumers are usually not even aware that a brand has access to this data.
3) **Digital Footprint and Location Data** – this refers to customer/user behavioral data with two of the main sources being web browsing and social media engagement history. Customers know this is happening at one level as they embrace mapping apps, from store locators to ride services; they seldom take action to prevent the data use unless they perceive a personal security threat, especially to their home.
4) **Predictive Data** – combining data from many different sources to form profiles and predicted areas of interest and expected customer behaviors. This data is highly sensitive and consumers value this the most when they are aware that it is happening.

The issue of context for data use needs to be underscored. Kobie conducted a survey in late 2017 that produced findings that indicate that consumers, regardless of their age, are particularly sensitive about sharing their social media profiles and location data even if the data is being used to improve their customer experience.

FIGURE 1: WHAT DATA WILL OR WON'T THEY SHARE?



After sourcing the customer data, there are four main uses of that data, with the important distinguishing characteristic being how beneficial it is to either the consumer or to the company:

1) Enhancing a brand's products or services – consumer privacy expectations with this form of data use is the lowest since it directly adds value for the customer. An example of this is when a company surveys its members and builds improvements into the product as a result of the customer feedback from the survey.

2) Creating personalized experiences and/or removing friction with the brand – for example, customers can take photos of furniture they see and Wayfair can identify similar products on their website.

3) Creating personalized communications and marketing – for example, Starbucks tailors communications and incentives on purchase behavior.

4) Direct monetization by selling data and lists to third parties – this form of data use is the least beneficial to the customer and, therefore, has the highest privacy sensitivity.

.....

Related to #4 above, there is another way customer data gets "used" – either by, knowingly or unknowingly, disclosing or leaking user data to third parties who specifically and consciously use that data.

As the perceived value of data increases and/or the uses of data become less beneficial and valuable to the consumer, the brand must provide consumers transparency and control, and find new sources of value to pass on to the customer in return. Companies should proactively develop comprehensive data security and privacy policies and processes that account for all types and uses of customer data.

Understanding these data nuances will allow a company to provide their customers with the appropriate level of disclosure and control, and enable them to provide the appropriate value exchange while managing consumer expectations.

Consumers ARE THE Products

An example of these dynamics in action is, of course, Facebook - where customers' perceived privacy violations are for both the most sensitive source of data and the most sensitive use of data.

Facebook's entire business model is fueled by customer data, and they continue to use that data very effectively for many of the reasons listed. However, they found out just how sensitive consumers are to a company that aggressively monetizes and profits from their data. In early 2018, Facebook consumers abruptly found out they are not just the users of the Facebook product, but they and their use of Facebook are, in fact, the product itself. For Facebook, the impact to brand trust has been staggering.

Facebook offers users privacy controls that are supposed to limit who has access to their data. However, these privacy controls and processes were not successful in safeguarding the data for approximately 87 million users.

Between 2013 and 2015, Cambridge Analytica harvested profile data from millions of Facebook users and their friends with the help of an app creator third party that collected it via a survey, without those users' permission, and then used that data to build a huge highly-targeted marketing database. Third party access to this data came with a stipulation that the data would not be marketed or sold, however that is exactly what happened. In this example, we see that a sensitive source of data was used without the consumers' consent. Although the data was not directly sold to a third party, it was carelessly (indirectly) leaked toa different third party.

Privacy controls were not successful in safeguarding the data for

87M USERS

These developments, combined with the high expectations of consumers to keep data safe and private, resulted in a significant blow to the trust of the Facebook brand.

In light of the example above and other growing privacy issues that Facebook has been experiencing, the company announced a series of steps and policy changes as their first line of action. Given the subsequent congressional hearings with Facebook, this positive self-regulation will likely not be enough and will give way to additional federal regulation – government trust is important too!

Success Elements

There are three main areas where loyalty and CRM leaders can take action to address rising consumer privacy concerns and help secure brand trust.

CONTROL AND CONSENT

Consumers want the ability to control the experience they have with the brand, including what communications they receive, the frequency of those communications, what data is being collected about them, how brands use data to customize the experience, and the ability to choose whether or not their data gets shared. Unfortunately, only **10% of consumers feel they have complete control over their personal information.**[2]

Companies would be wise to provide their customers with tools they need to feel in control and to collect clear, documented, and easy-to-update consent. One way to accomplish this is through the use of a Preference Center where customers control how they are marketed to, what data is collected, and how their data is used. This modern version of a Preference Center should be prominent and easy to find, with contextual links to provide timely and in-the-experience navigation.

VALUE

If a company is going to collect and use information about customers they should be careful to use it in such a way that it provides real value to the customer. This may be in several forms: deliver customized recommendations or relevant offers tailored to their needs and preferences, make doing business with the company easier and solve customer problems, or simply develop and enhance their product and services based on feedback from the customer.

If the customer perceives that the "gives" outweigh the "gets," they will not see a worthwhile tradeoff and may even believe that the company is not acting honestly or with their best interests in mind.

At that point, creating or maintaining trust will become impossible.

TRANSPARENCY

In a 2016 survey by Cognizant, respondents were asked which factors were important or extremely important for determining their level of trust in a company. **Open and transparent communication was the top factor at 67%.**[3] Transparency is a fundamental element for building trust with customers and is closely tied to both Control and Value. A customer may accept or not accept a company's terms and conditions with their accompanying privacy statement, but if those terms and conditions are hidden or are written in a way that only a lawyer can understand, or are only presented upon initial sign up and not throughout their experience with the brand, then you are not providing the consumer with adequate disclosure.

Transparency means being specific, clear, and open about what data is being collected and tracked, how it is being used, and how a user can manage their consent. A good example of this is Pandora. In this plainly-worded privacy statement, Pandora hits on all key Control, Consent, Value, and Transparency tenets and provides examples that help explain and educate users on Pandora's approach to managing and using customer data.

As part of the journey toward creating personalized customer experiences, consider your organization's stewardship of customer data to ensure brand trust is maintained and safeguarded. Until government regulation catches up to the technology and innovation, companies will be challenged by self-regulation and the need to institute ethical controls over customer data management. The companies that get ahead of this are the ones that will earn and keep the trust of their customers and lock-in brand loyalty.

1. Harvard Business Review, November 23, 2015. http://www.certona.com/value-of-personalization- across-the-customer-lifecycle/
2. PwC study, September, 2017: https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html
4. https://www.accenture.com/_acnmedia/PDF-47/Accenture-Trust-Digital-Age.pdf
5. https://safenet.gemalto.com/resources/data-protection/customer-loyalty-data-breaches-infographic/

ABOUT ***Kobie is a loyalty marketing company that designs, builds, supports and optimizes customer experiences for many of the world's most successful brands. Kobie believes in building relationships by deepening the emotional and behavioral connections brands have with their customers. Our integrated and innovative loyalty solutions deliver the most impactful results for our clients' bottom line.*** ***To learn more, visit kobie.com.***

KOBIE MARKETING, INC.

1-800-821-7892

100 2nd Ave South
Suite 1000
St. Petersburg, FL 33701

info@kobie.com

KOBIE REVIEW

kobie.com

LOYALTY

We help companies increase enterprise value by measurably growing loyalty.

Whatever your business issue may be, it's likely we've addressed it and have a perspective. While industries may change, and trends come and go, insights can always inspire. Check out our expert advice from Kobie thought leaders on kobie.com.

Industries:

Retail, Membership & Subscription Services, Financial Services, Travel & Hospitality, Telecom, Entertainment and more.