BIZCOMMUNITY

Customer privacy is part of the experience and is critical to build trust

By Paula Sartini

1 Oct 2020

Customer privacy is under the spotlight as South Africa follows in the footsteps of Europe's General Data Protection Regulation (GDPR) and other privacy regulations that have come into effect across the globe. The newly implemented Protection of Personal Information Act (PoPI Act) aims to govern how organisations collect, store and use personal information and while compliance and governance have traditionally fallen under the legal department's domain, this is changing. Marketing departments can no longer ignore their role in adhering to the requirements of the PoPI Act.

Photo by Fernando Arcos from Pexels.

Privacy management is critical, not only as a compliance tool for legal and compliance practitioners but also as a tool for building trust with customers. As such marketers have to be involved in privacy programmes to establish trust and deliver the best user experience to meet customer expectations which include treating customers in a manner in which they feel respected and valued.

While customers are willing to disclose personal information and have this information used by an organisation, they want to know that the company has procedures in place to protect their individual privacy. According to Deloitte, data privacy is about more than keeping hackers at bay, it is also about assuring consumers that the trust they place in a brand is warranted.

What is privacy worth?

Customer privacy and its importance for business and profitability is gaining attention as consumers are increasingly aware that companies are collecting their data and do not know what it is being used for.

Brands with a privacy-first culture tend to be governed by ethics [report]

10 Dec 2019

Consumers are increasingly concerned about their privacy with the PWC Consumer Intelligence Series: Protect.Me citing

that as many as 85% of consumers will not do business with a company if they have concerns about its security practices. Further, if companies have privacy scandals associated with them, it eliminates the potential brand from being considered during the selection process of the buyer's journey, thereby decreasing the chances of being chosen for purchase.

However, as many customers are not experts on data privacy, they expect the brands that they trust to put their privacy at the centre of all decisions they make. In other words, the trust that consumers place in brands trickles down to the privacy measures they believe the brand has in place to keep their data secure.

Trust and customer privacy go hand-in-hand and companies need to live by their brand promise and protect their customer's data if they are to meet customer expectations and establish a relationship of trust.

Marketers anticipate greater privacy regulation in 2020 [report]

27 Jan 2020

Customer experience builds trust

Although marketers have traditionally used customer data, gained either directly or via third party sources, to develop targeted campaigns, consumers needs have changed. While customers want personalised experiences and targeted campaigns this needs to be balanced with compliance and privacy requirements.

Transparency is critical to this process. Customers are more likely to give companies their data if they know that they are collecting it and what they will be using it for. This is supported by Deloitte's 2019 US Retail Privacy Survey, investing in building trust through consumer privacy can deliver a measurable return with 73% of consumers stating they are more likely to share data with companies that have privacy policies in place and advise how their data will be used.

In essence, the customer experiences develop trust and the data companies collect should add value to the consumer. Consumers want customer-centric user experiences that deliver on the brand promise while adhering to privacy policies. To achieve this the customer has to be central to the business strategy which includes the marketing and technology strategies that need to drive brand security.

Cracking the Privacy Paradox: How to future-proof trust in the fast-growing data economy

JD Engelbrecht, Everlytic 8 Jul 2020

Implement privacy by design

Legal, marketing and IT departments need to work closely together to ensure that the proper privacy standards are adhered to, brand experiences delivered according to the brand promise and customer data is secure all times. As such marketing departments are becoming more reliant on IT departments to gather customer data and implement technology solutions to deliver on-brand experiences that adhere to brand security standards and maintain relationships of trust with customers.

Companies stand to benefit from using technologies that have been independently tested and align with European security standards to give customers and employees peace of mind that data is gathered and stored securely. Further solutions that have been designed with security upfront to include segmentation of risk, ensure that content is safeguarded and secure throughout the data storage and usage processes.

Consistency gives peace of mind

The increased focus on customer privacy means that marketing departments need to keep customers informed that they are collecting their data and how they are using it. They also need to ensure that they are engaging customers on their terms according to the data they have collected.

How the privacy debate will shift in 2020

Grant Lapping 9 Jan 2020

It is equally important that marketing departments pay close attention to brand consistency across all company platforms such as websites and emails as this reassures customers that the company takes their privacy seriously. When companies pay attention to the smallest details in their branding, it gives customers peace of mind that they take their brand seriously and will have put thought into the brand security, privacy policy and strategy.

Trust is marketing's responsibility

Customer privacy can no longer fall solely in the domain of the legal department. Customer privacy has to move beyond checking compliance boxes to ensure that the company adheres to privacy regulations that have been stipulated by the government. Rather it is about focusing on the customer and prioritising trust.

To enhance customer experiences and build relationships of trust, marketing departments need to play an active role in establishing privacy or trust policies, implementing brand security measures and putting the customer at the centre of these strategies. Customers seek transparency and confirmation that companies will protect their data while balancing this with personalised customer experiences.

Overall marketing departments need to invest in privacy and take it seriously. From the newsletters companies send to pop-ups on websites and the technology solutions they implement to help deliver customer-centric experiences, customer privacy and brand security needs to be at the core.

ABOUT PAULA SARTINI

With over 20 years' experience helping leading organisations overcome various business challenges, Paula understands the challenges that companies face in delivering a consistent brand experience and the impact this has on their bottom line. An analytical thinker that strives to solve business problems with innovative solutions, Paula believes that technology plays a major role in solving critical business and branding challenges. As such, she established BrandQuantum to help businesses overcome their branding challenges in the digital age.

- Employee branding: Critical to customer experience - 14 Sep 2022
- #BizTrends2022: Data gives marketers insights to connect with customers - 5 Jan 2022
- Gathering customer data effectively to create great customer experiences - 25 Nov 2021
- The challenge of martech and automation - 20 Sep 2021
- Why brand health matters - 5 Aug 2021

View my profile and articles...