BIZCOMMUNITY

The balance between customer privacy and intimacy

By Paula Sartini

18 Jan 2021

Whilst the role of the marketing department appears to have evolved significantly over the past few years, fundamentally it is still about building relationships.

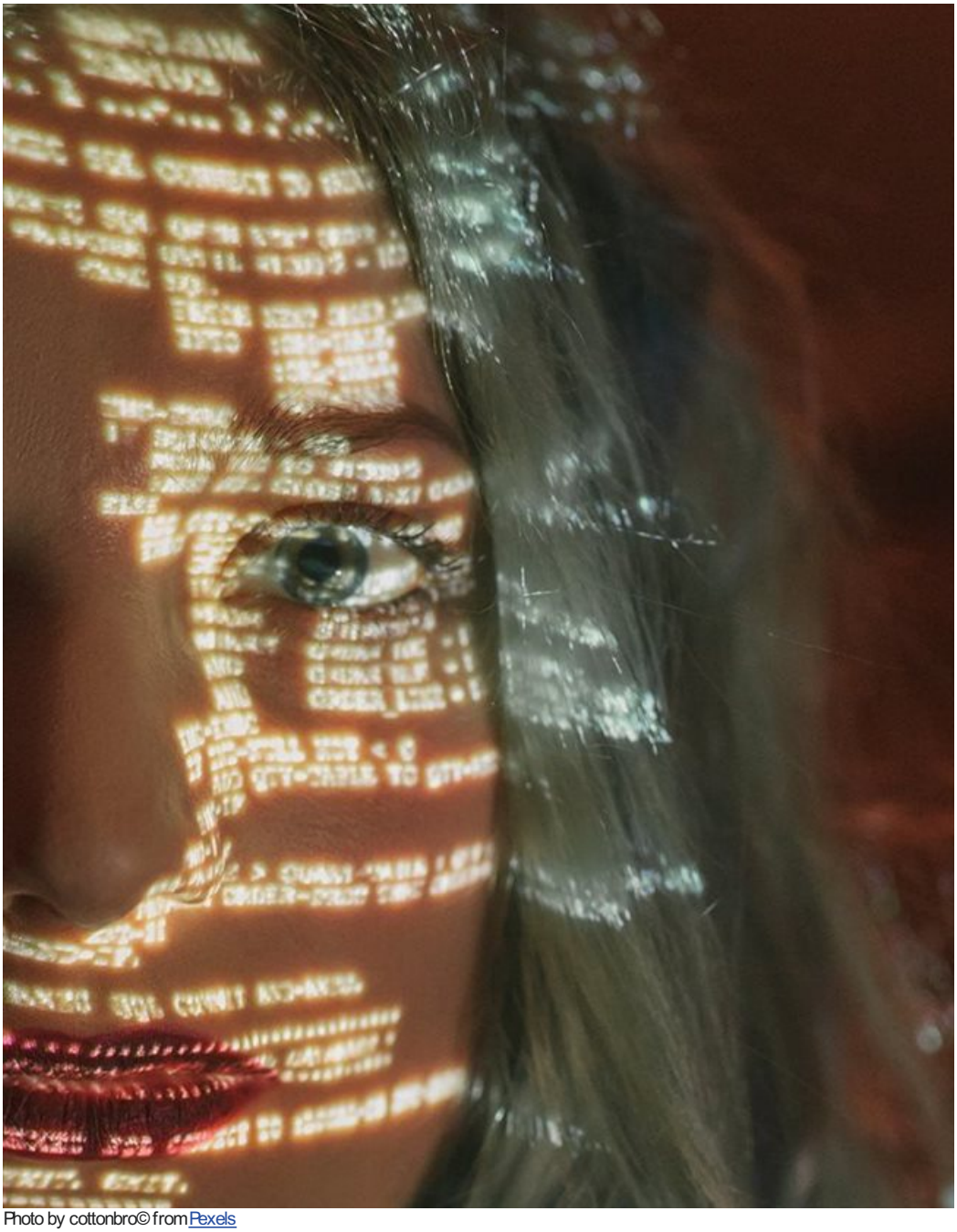

Photo by cottonbro© from Pexels

With the rise of social media and other digital platforms, this has increasingly meant that relationships are based less on human contact and more on personalised digital communication. Consumers are aware of the inevitable trade-off between privacy and personalisation, aptly termed the privacy paradox. Earlier research into the paradox of what consumers say and do was attributed to consumers simply not knowing enough about the pitfalls of sharing personal information too readily.

More recent research in the US shows that many consumers have resigned themselves to the fact that their information has been traded as a commodity, yet privacy concerns remain a key consideration when disclosing online. This is supported

by the Digital Marketing Institute which states that privacy is a top concern for online consumers with 86% taking steps to improve their online safety. With this in mind, companies need to prioritise customer privacy and control by implementing security and privacy standards as well as customer control over their personal information and communication preferences.

As marketers have traditionally been responsible for establishing relationships with customers and implementing initiatives to build trust, they also need to take responsibility for customer data. This includes customer data protection as well as providing customers with means to control their own data - regardless of where in the lifecycle of the relationship they may be.

Whilst Information Technology teams can and should be held accountable for ensuring that customer information is not compromised by data breaches or intrusions into the company environment, it is marketing's responsibility to ensure that customer information does not "get out" and is treated with the utmost respect.

This is supported by the DMA which states that marketers have a responsibility to take good care of consumer data and cannot take this for granted. There is a difference between security and privacy and more often than not, these terms are used interchangeably.

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

Paula Sartini 1 Oct 2020

Securing customer data

IT has the responsibility of keeping data secure and ensuring that data cannot be accessed by potential hackers. A key responsibility is to prepare for possible security breaches and ensure that there are security measures in place to protect customer data. According to the Institute of Digital Marketing, IT departments need to focus on where data is stored as well as implement security measures along every step of the process of data acquisition through to use and storage.

This is an important first step to keeping customer data secure and meeting customer expectations. This is a big responsibility as according to an Accenture study, 75% of consumers consider personal data as their second-biggest concern after increasing costs. However, according to PWC, 75% of consumers do not believe that companies handle their data responsibly. So whilst consumers expect companies to keep their information safe, they don't often believe that companies do. This gap is a trust gap.

Customer privacy

Over the years, marketers have collected massive amounts of customer data to provide positive, personalised experiences. While customers have come to appreciate the personalisation, they are concerned about their data falling into the wrong

hands.

For this reason, marketing departments need to take responsibility for customer data and how it is handled. This is supported by The Federal Trade Commission which states that marketers are legally obligated to treat customers' private data respectfully and fairly. Based on this customers require transparency in how their data is being used for marketing activities. A key concern is that many marketing departments outsource various initiatives to third-party agencies which require that private customer data is shared with companies outside of the business.

According to *Financial Post*, if companies transfer private customer information to third parties, the onus remains on the company to keep the data safe. With this in mind, customers are reliant on the relationship they have with selected companies to keep their data secure regardless of whether they use third party companies or not.

While marketers may trust their partners and suppliers, it is important to verify them and confirm how they use the data you provide them with as well as understand how their data policies align with regulatory requirements. After all, if your customers trust your organisation and their data lands in the wrong hands, you will ultimately be left with holding the bag.

Customer trust

According to the DMA, attitudes towards data may be evolving, but trust remains the constant and key factor when it comes to understanding what people feel is most important about data. Adding to this, brands that fail to take responsibility for their customer data ultimately lose customers, goodwill and shareholder value.

Based on this, trust is the most valuable component in the customer relationship. Before a customer will give you their data, they have to trust you and believe that you have their best interests at heart. Once they have given you their data you have to prove that you are trustworthy and will use their data as agreed.

This can be achieved by putting measures in place such as permission-based access to customer data which limits the number of employees that can access the customer data. However, beyond internal measures, companies would benefit from empowering customers with verification tools to protect themselves from potential threats such as email verification tools that can help prevent customers from falling from spoofing or phishing emails.

Trust is earned. It takes time. It's only through repeated interactions that trust is built. It is also fragile and easily lost. Just because a customer shares information does not mean that they trust the organisation or that it is an open invitation to receive unsolicited communication. It is merely the first step in a journey. Customers should always feel that they are in control. If organisations want to build trust, they need to visibly show the evidence of the measures that have been put in place to ensure that customers remain in charge of their information. This includes, but is not limited to privacy policies, customer control over the personal information they have provided, how it is stored and its deletion. This should also extend to behavioural data.

In all your interactions with your customers, your brand tells a story, it says whether or not you're consistent and trustworthy or flighty and unreliable. By focusing on brand consistency across all documents, presentations, emails, and more, customers establish trust and believe that if you are willing to focus that much attention on the smaller details, you are credible and will pay attention to the bigger issues such as customer data security and privacy.

While secure IT infrastructure is a key component to keeping customer data secure, customers expect more than adherence to regulations and the latest technologies to help protect their data from falling into the wrong hands, they are relying on the brands they trust to live up to their expectations and put measures in place to ensure that their data will be used responsibly and safely. Without customer trust, brands will not survive.

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 bottomline. 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...