Does big data invade your privacy?

According to Gartner*, by 2015, 4.4 million IT jobs will be created globally to support big data, a clear indication that big data continues to make a large impact on organisations - but have you asked your customers for permission to analyse their data?

Big data has literally taken the world by storm and promises a number of opportunities for any organisation; such as competitive advantages, operational efficiency, and originality. As such, more and more organisations are already implementing big data. However, it seems that many local businesses are doing so without having done the necessary research to see if their business actually needs it.

In fact, Frank Rizzo, director, IT Advisory of KPMG said: "Knowing what data to collect is one of the biggest obstacles to implementing a data-and-analytics strategy across the business, and many businesses don't realise this. The result is that often big data tends not to work for a particular business need. However, what matters more is the value that huge amounts of data can bring to the business, and the veracity of that information."

In a world inundated with data, veracity allows the correlation of single pieces of data that, if separated, do not provide anything meaningful; however, when put together, offer an incredibly accurate picture that allows organisations to identify the behaviours and profiles of potential customers. This, then, gives companies the ability to understand their data better and put an accurate and strategic analytics strategy together - one that will work.

Additional challenges are coming to the fore

However, Gerhard Botha, CTO of the PBT Group, which specialises in big data, has noticed that additional challenges are coming to the fore. "While big data can certainly add significance to an organisation, it can also leave customers feeling slightly vulnerable, as organisations typically tend not always to ask customers for consent to analyse various data collected," said Botha.

Most companies implement big data while undertaking brand activations to see which products or services their target

market prefers. "While doing this, however, if companies approach this task in the wrong way and do not undertake the necessary steps, they can end up ruining their brand's reputation indefinitely," continued Botha.

Vicente Diaz, Principal Security Researcher, GReAT of Kaspersky Lab, agrees, especially as customers are becoming more conscious around security and the privacy of information. "The correlation of this data and the resulting intelligence is one of the main concerns when it comes to privacy, because the use of many services individually should have never allowed identifying the behaviour of individual users - however the correlation of data allows this." Kaspersky Lab notes that this is an ethical dilemma that can lead to commercial difficulties, given that there have already been a number of incidents where the reputation and dealings of organisations have suffered when their clients learnt of data that was used without their consent.

Diaz also added that many IT specialists and companies that are focusing on big data tend to do so with little to no consideration towards that actual security of the physical data. Big data is mainly used for the analysis of data from many different sources. These sources can have any format, including archives, which is common ground in terms of security with cloud storage. As the data can come from anywhere, it can be vulnerable to malicious threats and, if infected, can impact on a company's server or data storage system. In light of the debate around big data, security vendors have created solutions that enable organisations to scan all the data collected and source any data that may have malicious software or be encrypted by unwanted third parties.

Reluctantly tolerated

Additionally, analysis on various data collected has also been reluctantly tolerated by society, as, historically, legislation did not protect them against the commercialisation of data commoditisation and marketing practices.

"This has changed with the introduction of the Protection of Personal Information Bill (POPI), as indicated in November 2013. In fact, in a recent example of exactly this, Facebook faced a lawsuit**, stating it had violated customers' privacy and shared it with advertisers, marketers and other data aggregators for their business gain, which had huge repercussions for organisations," added Botha.

Big data is here to stay but it needs to be managed effectively if organisations are going to get it right and reap the ample business opportunities it provides - with no detriment to their privacy.

"Going forward, companies should be mindful of ensuring their business leaders understand POPI, implement the right strategies and, above all, that they put the right procedures in place to protect personal data. Big data can not merely be a technology decision, but one that the entire executive team needs to ensure that not only the opportunity is seized, but that any risks or complexity can be mitigated," concluded Rizzo.

* *Why You'll Need A Big Data Ethics Expert*
**Facebook faces privacy suit*