information management

FEATURE

The Battle Between Data Analytics and Privacy

Kon Leong

OCT 3, 2016 6:30am ET

Data analytics and privacy are by their nature antithetical to one another. Analytics initiatives accumulate as much data as possible in order to provide the greatest possible insight into their subject; in the case of employee analytics this is largely unstructured data, comprising electronic communications and files, sometimes containing personal information.

If employed recklessly, it is therefore almost certain that these initiatives will trespass on employee privacy.

We are presently at a crossroads. The new breed of unstructured analytics carries with it the capability of providing great insight into our working and communication habits: It's realistic to say this knowledge could dramatically reshape the way we think about workplace behavior.

Unstructured analytics is capable of tracking everything from organizational networks to information distribution paths to correlations between behavior patterns and productivity. The future of analytics lies in using these conclusions to reform the workplace and optimize workflow. However, if we don't proceed cautiously, analytics initiatives will fall flat.

Worse, they will expose employee data to privacy and security threats. For example, if marketing decides to start an employee analytics initiative to gauge sentiment on a new product, how do they ensure that C-level emails are not being thrown into the mix? If information is mismanaged, the simple answer is they can't.

In order to protect employee privacy, the wrong people must be prevented from touching it. Deceptively difficult.

The only solution is an ongoing information governance strategy that sets the ground rules for responsible data initiatives and ensures that sensitive data doesn't end up in the wrong hands. Despite what you may think, the most intrusive governance system is in fact the most private.

Access Denied

Information governance is about control. It's a given that emails and files will be kept well after the date that they're created, not just for the sake of gathering data for eDiscovery, compliance, or data analytics—it's also about utility. Employees must save data for future use, but without defined policies in place they often do so insecurely.

Some companies say, “Let’s lock up all our information in Fort Knox to protect it.” The problem then is that no one uses it because they have to hike all the way to Fort Knox to get it. Data utility and security must be reconciled.

Easier said than done.

Data must be mapped and classified, and have appropriate policy-based actions applied for deletion, de-duplication, and retention. Moreover, appropriate access privileges must be assigned, with particular data being quarantined. This requires ongoing information governance.

Emails are one thing, but files have crept into the blind spot of today’s enterprises. Unlike emails, they aren’t subject to industry regulations for storing and monitoring, so they don’t carry the same pressing urge to govern. Don’t let this deter you: they can still cause big problems.

A typical company may have masses of dark data spread across their servers, scattered in inappropriate repositories, without defined access privileges or retention policies, or a clear process of remediation.

File mismanagement is an insidious problem, for which there is no instant fix. Metadata and content analysis is needed to take effective remediation actions, in what must be a highly coordinated initiative. Input from all stakeholders is essential—legal, compliance, IT, records, etc.—to ensuring vital data is prioritized.

Harnessing Analytics

Employees often have a cynical perception of data analytics as well as information governance, despite their clear necessity. In some ways, this is rightfully so; the idea of someone looking through personal files and emails carries dystopian connotations. Because distrust within an organization grows quickly, stakeholders must be wary of sparking it.

To avoid doing so, governance and analytics initiatives should be made transparent, and consistent and practical policies must be applied.

Ultimately, it is only when an organization has a definitive process for governing information that there can be true accountability. We are now at a crossroads: We have in our hands tools that could be unimaginably empowering; yet without governance, the boundless expansion of unstructured analytics will have devastating repercussions.

(About the author: Kon Leong is president, CEO and co-founder of ZL Technologies)
