

# Risk Management – Sentiment Analysis: Are You Feeling Risky?

## Sentiment Analysis: Are You Feeling Risky?

by [Katherine Heires](#) | December 1, 2015 at 6:02 am



How do you feel when you are at work? Are you happy, sad or stressed out? Are you thinking about quitting, breaking a few rules or even committing fraud?

Be careful: Companies are increasingly using sentiment analysis technology to monitor internal communications in order to better understand employees' moods and assess any potential risks. "Sentiment analysis has become a form of risk management and is emerging as a useful risk control tool for a variety of businesses," said Vasant Dhar, a data scientist and professor at New York University's Stern School of Business and the Center for Data Science. Firms in highly regulated, compliance-

oriented or risk-focused industries, such as financial services, health care and insurance, are starting to use the technology to identify and address regulatory risk issues, compliance problems and potential fraud.

### **What Is Sentiment Analysis?**

Sentiment analysis studies the mood, opinions and attitudes expressed in written text. It aims to discover the emotions behind words in order to determine whether a communication suggests a positive, negative or neutral sentiment.

When first developed, sentiment analysis was conducted manually, but it is now being performed on corporate communication in an automated manner or in partnership with analysts. It is also being used in combination with other computer-based tools like text mining, text analytics, natural language processing, machine learning, statistical modeling, big data analytics and computational linguistics.

This analysis can help organizations quickly and easily study large quantities of unstructured data culled from employee communications, including company chat rooms, wikis, customer call logs, emails and instant messages. Such information can then be used to provide evidence of employee satisfaction levels, anticipate signs of employee churn, identify new business opportunities or sales strategies, and determine if employees are a source of serious risk.

Various factors are fueling the growth of this technology as an employee-monitoring platform. First, U.S. regulations impacting industries such as banking, financial services, insurance and pharmaceuticals often require ongoing monitoring of communications as a consequence of infractions. Regulatory frameworks such as the Foreign Corrupt Practices Act also mandate that U.S. firms operating in global markets closely monitor their global workforce for instances of bribery, fraud or money laundering.

In addition, concerns about data security in the wake of recent leaks from internal actors like Edward Snowden and Chelsea Manning have caused many firms to explore their options for preventative measures. Some companies have already used sentiment analysis tools on social media to gauge consumer brand preferences, leading many to wonder if such tools would also work internally.

With the increased focus, sentiment analysis continues to evolve and improve. Some sentiment analysis providers are starting to offer facial coding of video, speech analysis of audio streams and assessment of affective states. Others are even gearing up for the application of neuroscience and wearables to study customer or employee physiological states.

### **Limitations and Data Privacy Considerations**

Despite the enthusiasm for sentiment analysis, many are also quick to highlight its limitations.

“Sentiment analysis by itself is not really indicative of a particular risk,” said Rob Metcalf, president of Digital Reasoning. “You have to pair it with tools that can identify audience, content and tone—who and what I am talking about—and understand the context of the communication.” For example, instances of code switching—the use of substitute words or euphemisms to try to hide the true meaning of a

communication, like using “baseball” for “financial instrument”—are often indicators of risk and are dependent on context cues. Humor and sarcasm in text are also difficult for automated sentiment analysis platforms to identify and parse.

“Even in the best of circumstances, it is only 65% to 70% accurate,” said Susan Etlinger, an analyst with research firm Altimeter Group. She noted that the accuracy rate drops even further when the process is applied to text in languages other than English.

Jen Dunham, a certified fraud examiner and technology specialist with SAS Security Intelligence, agreed. “Findings from sentiment analysis can provide insights but always have to be validated with other evidence,” she explained.

Compliance is another concern. While privacy laws in the European Union prevent employers from actively monitoring the sentiment levels of employees, it is perfectly legal in the United States for companies to monitor communications that occur on their computer systems. According to Bennett Borden, chief data scientist and partner at Drinker, Biddle & Reath, in the United States, any data that is held on company servers and equipment that belongs to the company can be used for any legal purpose. Companies also have the right to monitor for misconduct or violation of corporate rules. There are ethical issues that firms must consider, however. “Just because we can do it does not necessarily mean we should,” he said.

The use of sentiment analysis and related monitoring technology may not be a solution for everyone. “Today it’s understood that any information that passes through a corporation—in an email, phone conversation or chat session—belongs to the corporation and can be used in a regulatory context,” said Seth Grimes, an analytics consultant with Alta Plana Corporation and organizer of the annual Sentiment Analytics Symposium. “But is it appropriate for a manufacturing company or a tech firm to be doing this?” What may be acceptable for a contact center aiming to improve customer service or a financial services firm trying to calibrate employees’ risk tendencies to avoid rogue trading losses may not be appropriate for other firms.

Companies have to decide whether or not they are comfortable with this level of monitoring. Could there be an adverse reaction from employees if they know they are being monitored? Will it present a challenge to recruitment? “There is a Big Brother aspect to this technology, but at the same time, we are seeing more and more stories about internal threats and instances of data loss, and traditional tools are just not cutting it,” Dunham said.

Seth Redmore, chief marketing officer at sentiment analysis technology provider Lexalytics, advocates using sentiment analysis tools for internal communications that are relatively public, like corporate wikis or chat rooms. “These are places within the corporation where there is no expectation of privacy,” he said. Others will monitor email and phone calls in a manner that aggregates and anonymizes all the data and investigate further only if and when there are risk alerts or notable sentiment levels.

Companies should review and employ data privacy guidelines, as advocated by organizations such as the Information Accountability Foundation and the Software Engineering Institute at Carnegie Mellon University. Analysts also recommend companies be transparent about the use of such technology. “It helps when employees understand that this is about prevention, proactive detection and safeguarding the organization,” Dunham said.

Nevertheless, sentiment analysis cannot function by itself—it is simply another tool. “None of these technologies should be considered ‘lights-out’ solutions,” Grimes said. “You can’t just turn them loose and expect great results. There really always has to be a human in the loop, training the tools, making sure they are used correctly and assessing and analyzing the results.”



More articles by [Katherine Heires](#) »

About the Author

**Katherine Heires** is a freelance business journalist and founder of MediaKat LLC.

- 106