Harvard
Business
Review

MANAGING PEOPLE

Is Your Company Using Employee Data Ethically?

by Kon Leong

MARCH 13, 2017

Potter Stewart, justice of the U.S. Supreme Court, once said, “Ethics is knowing the difference between what you have the right to do and what is right to do.” Associate Justice Stewart probably didn’t know how new data technologies would soon begin to blur those boundaries.

With the emergence of new information technologies, corporations can now amass and analyze unprecedented volumes of unstructured data — the data created by humans, such as the text contained in company documents, email, instant messaging, and social media. Collecting this data was originally driven by the obligation to produce evidence for litigation, to preserve business records, and to respond to regulators' demands for information, but it has now dawned on corporations that all of that data can open up new vistas of management capabilities, such as visualizing employee interactions, mapping domain expertise, replaying past events, tracking employee sentiment, and providing insights into all human activity across the organization.

These capabilities are creating much excitement, angst, and debate. While the benefits are clearly far-reaching and potentially game changing, there are ethical questions to consider. When companies collect all the data their employees generate, there's always the risk that employee privacy will be sacrificed for profit.

Consider the following ways that companies are using employee data:

Who knows whom? Who knows what? Companies use employee data to outline a network of relationships among employees, customers, vendors, and others, identifying subject matter experts. For sales and business development, this is an invaluable tool. A sales manager of a major services corporation, for example, may want to know which employees have the strongest relationships with executives at a client prior to visiting them and who best understands the subject of the meeting. But ethical conflicts can arise, say when the analysis identifies sensitive personal relationships that perhaps should not have existed on corporate servers in the first place.

Which employees are likely to quit? While it's not an uncommon request to identify employees who are flight risks within an organization, the breadth and depth of such analysis may leave employees with a disquieting sense of being under surveillance. There is a risk, too, that managers may jump to easy conclusions about the results instead of unearthing the real issues, for instance assuming a distracted employee is disengaged when actually they're going through problems at home.

Instant replay button for escalated incidents. During escalated incidents, timely and complete data can be the best defense against a surprise event, such as an internal investigation regarding an accusation of inappropriate behavior between an executive and a subordinate. Today's technology can gather all relevant information on the matter and present a complete analysis so that management can respond effectively and in a timely way. However, this requires a very large amount of data to be retained, coupled with powerful search and analytics tools, which together, if used unsparingly, can infringe on the privacy of all employees.

Is Your Company Using Employee Data Ethically?

These use cases present complex trade-offs between what companies *can* do with all of the employee data they're collecting and what they *should* do. What can individual managers do to make sure the data being collected in their organizations is being used ethically?

Understand your company's privacy comfort zone. Get a sense of where your company and employees stand with respect to privacy. Every organization and country has its own privacy culture and definition. For example, the EU has the General Data Protection Regulation, which governs and protects individuals' data privacy, while the U.S. is more lax about privacy protection. Defining this privacy comfort zone and seeking to understand what expectation of privacy exists within your department and company can help guide decisions on privacy issues.

Ask for guidance from your information governance (IG) committee. Many organizations have recognized the dangers of siloed data and have started to form a committee to coordinate an information governance strategy. This committee can offer guidance on available solutions for protecting employee privacy while staying in line with corporate objectives. Typical IG committee members include the general counsel, the chief risk officer, the chief compliance officer, the chief information officer, the chief information security officer, and the chief data officer.

Share guidance with your team, and encourage best practices. Pending guidance from the IG committee, you can start implementing best practices, such as encouraging employees to limit the use of corporate devices and resources to official business purposes. Keeping personal information off of company email and company devices whenever possible will reduce unnecessary exposure.

Invite feedback. Governments and regulatory agencies have realized the power of electronic information and have actively written "whistleblower" laws to mandate whistleblower protection. Managers should create a safe space for discussing corporate ethics and encourage employee feedback in order to maximize transparency and minimize the dangers of whistleblowing events.

Creating a forum for employees to voice their opinions might illuminate questionable practices that management has not considered. Above all, employees should never feel silenced or afraid to speak up.

As with any powerful technology, we cannot put the big data genie back in the bottle, and we ignore its risks at our peril. How we use or abuse digital technologies and the data they generate is one of the greatest ethical challenges of our time.

If Associate Justice Stewart were to define digital ethics today, he might observe that what we have a right to do is easy — it's defined by law. However, what *is* right to do is far less clear. In the world of big data, we are destined to fumble and stumble, but I believe Stewart would agree: It's time we start learning the difference.

Kon Leong is co-founder and CEO of ZL Technologies, Inc., a software and cloud vendor to large enterprises for information governance and analytics solutions. Previously, he was co-founder in several high tech startups.

This article is about MANAGING PEOPLE

⊕ **FOLLOW** THIS TOPIC

Related Topics: ANALYTICS | PERSONNEL POLICIES | ETHICS

Comments

Leave a Comment

POST

0 COMMENTS

JOIN THE CONVERSATION