Harvard
Business
Review

TECHNOLOGY

Collect Your Employees' Data Without Invading Their Privacy

by Chantrelle Nielsen

SEPTEMBER 24, 2014

Research shows that businesses using data-driven decision-making, predictive analytics, and big data are more competitive and have higher returns than businesses that don't. Because of this, the most ambitious companies are engaged in an arms race of sorts to obtain more data, from both customers and their own employees. But gathering information from the latter group in particular can be tricky. So how should companies collect valuable data about time use, activities, and relationships at work, while also respecting their employees' boundaries and personal information?

In helping our customers adopt people analytics at their own companies, we've worked directly with legal teams from large companies around the world, including over a dozen in the Fortune 500. We've seen a wide range of cultures, processes, and attitudes about employee privacy, and learned that in every case there are seven key points that need to be addressed for any internal predictive analytics initiative to be successful:

Find a sponsor. The team that's proposing the data analysis needs to have real power and motivation to change the business based on the findings. Most need a sponsor in a senior-level position for this kind of institutional support. First, this person can help balance opportunistic quick wins with a long view of how predictive analytics fits into strategic plans. He or she should also explain why the data collection and analysis is so important to employees across the organization, and can serve as the person ultimately accountable for ensuring that the data stays private. In many cases, if a company's legal team doesn't see strong sponsorship and support, they are likely to de-prioritize approval of the initiative — to the point where it may be forgotten entirely.

Have a hypothesis. Before you start collecting data, decide why it's needed in the first place. For one, legal departments can't often approve a project without an objective. But in addition, the team proposing the project needs to be clear and transparent about what they're trying to accomplish. This includes having a tangible plan for what data is being sought, what changes will be made based on the findings, how the results of these changes will be measured, and the return on investment that justifies the time and energy put into the project.

The hypothesis can be as specific as "underperforming customer accounts are not getting as much time investment as high-performing accounts," or as general as "correlations will be found between people analytics metrics and business outcome x," but the outcome needs to *matter*. Projects without a purpose confuse people and incite skepticism, setting a bad precedent for future analytics efforts.

Default to anonymity and aggregation. There is more to be learned by examining the relationship between sales and marketing as a whole than there is by examining the relationship between James in sales and Elliott in marketing. Analytics initiatives are not the place for satisfying personal curiosity. In our work, we use metadata only, usually beginning with email and calendar. By default, we anonymize the sender and recipients' email addresses to their departments. To further protect anonymity, we aggregate reporting to a minimum grouping size so that it's not possible to drill down to a single person's data and try to guess who they are. This removes the possibility of even innocent snooping.

If you can't let employees be anonymous, let them choose how you use their data. In a few cases, business objectives can't be met with anonymous data. Some of our customers, for example, conduct social network analyses to identify the people who make important connections happen across disparate departments or geographies. After identifying these key "nodes" in the social graph, managers will interview them and then help them influence others. In a case like this, the best approach is to ask permission before gathering the data in one of two ways:

1. Using an opt-out mechanism is the simplest. Employees are sent one or more email notifications that they will be included in a study, with details on the study plan and scope. They have to take an action (usually clicking a link) to be excluded from the study.
2. Opt-in earns a bit lower participation, because recipients have to take the action in order to be included in the study. More sensitive legal teams may require an opt-in.

Whether it's opt-out or opt-in, the worker should know what's in it for them. We find that the most relevant reward is access to data — after all, most people are curious how they compare with their peers across various dimensions. We provide people with personal, confidential reports that compare their own data to organizational benchmarks, and this helps give them an incentive to participate. Real, personalized data also helps to make the message about the study interesting, cutting through the inbox noise so the opt-in gets attention. And if you don't have the ability to give people back their own personal data, you can promise future access to some form of aggregated study results to reward them for participating.

Screen for confidential information. Then screen again. Certain teams, such as legal, HR, or mergers and acquisitions, will be dealing with more sensitive matters than normal, and their data may need greater protection. Whether data will be gathered from humans, electronic sources, or both, sensitive information should be screened out in two ways:

1. Don't gather it in the first place by configuring the instrument to exclude keywords, characteristics, or participants that would indicate sensitivity.
2. Re-validate and remove any data that wasn't screened by the initial configuration, because both people and software can miss the meaning of textual information. Perform a second validation before sharing the data with the final audience.

Don't dig for personal information. Every person experiences interruptions in their workdays for personal reason — dentist appointments, children's activities, etc. At the same time, by policy, some companies protect their employees' privileges to use company systems for personal reasons. Regardless of policy, there really isn't much business value in looking analytically or programmatically at data about peoples' personal lives, and we automatically exclude it from our dataset. The bottom line is that employees have a human right to personal privacy, as well as significant legal rights that vary in different countries. Personal matters should be handled by managers, not by analytics initiatives.

For additional protection, consider using a third party. It is common in some applications for a third-party vendor to perform the data cleansing, anonymization and aggregation, so that the risk of privacy violations by employees of the enterprise is removed. This work can be performed by third

parties even within the firm's firewall, if desired. But there's an important caveat: Companies that handle sensitive data should follow security practices, like background checks for their employees who have access to the data, and should not, in general, use subcontractors to perform their work.

The opportunity in data and predictive analytics, particularly people analytics, is huge, which makes it especially important that companies take a responsible and proactive approach to privacy. By collecting and using data in a way that respects and rewards employees, leaders remove friction points in the adoption of increasingly valuable analytical capabilities. The seven practices outlined will help clear the path for pioneering programs and build an organizational culture that prizes and rewards analytical thinking at all levels.

Chantrelle Nielsen directs research and strategy for Workplace Analytics, a new organizational productivity category at Microsoft. She led product management, marketing, and several other functions at VoloMetrix as they grew and were acquired by Microsoft.

This article is about TECHNOLOGY

⊕ **FOLLOW** THIS TOPIC

Related Topics: INFORMATION & TECHNOLOGY | MANAGING PEOPLE

Comments

Leave a Comment

POST

1 COMMENTS

lokinchemburkar 3 years ago

Chantrelle, good read. I would like to add to the practice - Screen for confidential information. Then screen again. This practice should explicit also consider local HR privacy laws while screening confidential information, especially for global organizations. Privacy laws vary by country, and information that you may be allowed to collect in one country may be restricted in another.

REPLY 0 0

JOIN THE CONVERSATION