Privacy and Ethics in People Analytics

INTRODUCTION

Companies now have access to more employee data than ever before, ranging from data on job performance and pay to data on employee e-mails, location and travel, employee comments and feedback, even videos from monitoring systems. While all this data is intended to help companies make work life better, it has the potential to be abused. Today, as data collection becomes easier—some tools, for example, collect data on all e-mails, meetings, and documents created—it's more important than ever for HR to take a position on ethical data use, privacy and security, and employee communications related to data-related policies.

The market for HR data and analysis tools is over $2 billion annually and will likely double by 2025; research by Sierra-Cedar shows that the average number of HR systems of record in an organization increased from eight systems to 11 in 2019. Companies today collect data about employee well-being, learning activity, social communications and even mood.

Even while companies continue to implement more and newer systems to drive productivity, a majority (79 percent) of Americans are concerned about the way their data is being used. And they don't feel they're in control: 59 percent say that they have little or no control over how employees use their personal information. Your employees don't need to feel this helpless.

Communicating how your company treats the data it collects from them (and from their use of the tools you provide them) is part of the employee experience. This paper offers a perspective on how to bring an ethical approach to data collected from employees that respects their privacy, ensures security and minimizes bias.

RISKS OF THE DATA-DRIVEN ORGANIZATION

The amount of information being collected by companies is staggering, and regulations are not keeping up. While technology vendors may have the best of intentions, they often fail to consider how the data in their systems could be abused. As the use of artificial intelligence (AI) becomes more common, the behavior of their systems will change based on the company's use, and this will force vendors to better understand how their algorithms may or may not work fairly in a real company.

In the old days of HR analytics, the vendor sold a system that did reporting, leaving most of the analysis up to the customer. Today, AI provides recommendations, suggestions, and assessments automatically, so vendors don't always know how their system will perform in the real world.

Technology and the Impact on Employees

Measuring and managing workers by technology alone can backfire when done poorly. The three following examples could have benefited from a healthy dose of design thinking that considered employee and company interests. Granted, these are worst-case scenarios, but they do illustrate how what might seem as the logical use of technology and data can go wrong.

APRIL 2020

PRODUCED BY

SHRM EXECUTIVE NETWORK

WRITTEN BY
Josh Bersin

A data-driven approach should respect and account for human needs—whether it's their biological needs, the autonomy to manage one's life outside of work, or the sensitivity of employees to customer needs. An ethical system treats employees like humans, not robots.

Worker Productivity

One internet company uses technology to track warehouse worker productivity, and the system automatically terminates those who can't keep up. A United Kingdom survey found that 74 percent of this company's workers avoided using the toilet for fear of being warned that they had missed their target numbers. In the United States, the company's delivery contractor drivers have been responsible for several deaths and report brutal working conditions to meet goals. The company has since cut ties with the contractors, resulting in thousands of layoffs, lawsuits and bad press.

Employee Scheduling

In 2014, one retail company suffered a public relations hit when The New York Times reported about the impact of their demand-driven worker scheduling system. The system notified employees about their schedules just three days in advance, eliminating the possibility of predictable scheduling and causing employees to scramble to arrange childcare or to get them to school. The company has since modified its scheduling practices to notify workers of their schedules 14 days in advance, although it is unclear if that policy is being enforced because it competes with other performance measures for which store managers are held accountable. A more considered approach would take into account the entire value chain of scheduling, including employee needs, managers' performance measures and the company's efficiency targets.

Housekeeping System

A 2018 investigation in Philadelphia found that an app-driven housekeeping system implemented by one hospitality company in 2016 created more work for housekeepers and impacted their ability to meet unpredictable guest needs. A housekeeper said the app kept her "chained to your cart with blinders on." In addition, the Wi-Fi-enabled system couldn't function in dead zones of a hotel that spanned 23 floors and a whole city block. Clearly the system would have benefited from more upfront research and user testing before a hotel-wide rollout of that scale.

In 2018, the company rolled out an alert system for housekeepers and other associates that allows them to summon help if they feel harassed in any way, need quick support or spot a guest in distress. The company said in a press release that it conducted "more than a year of field testing and modifying solutions based on input from housekeepers and safety and security experts."

Employee Data Abuse and Misuse

Without proper rules and access controls, systems are ripe for employee abuse. In other cases, a system may reveal sensitive information that managers are poorly equipped to deal with. Consider the following examples:

"God View" Software

In 2014, a journalist critical of a ride-hailing company was shown her ride records when an employee spied on her using an internal system called "God View" that can track customers rides. Not only did the company consider using the system to threaten journalists critical of the company, employees regularly used it to track celebrities and ex-lovers. Although the company said it had implemented controls over the data after the incident,

> A data-driven approach should respect and account for human needs—whether it's their biological needs, the autonomy to manage one's life outside of work, or the sensitivity of employees to customer needs. An ethical system treats employees like humans, not robots.

it was essentially an honor system and employees kept using it for their own purposes. One security employee who voiced concerns over the software and other security practices was fired and is now suing the company. In 2017, the company settled a complaint about God View with the Federal Trade Commission (FTC) and, as part of the settlement, will submit to third-party privacy audits for 20 years.

Retention Predictors

Retention predictors in software systems can sometimes become a self-fulfilling prophesy. An executive working for a company that had turned on its "retention predictor" in its human capital management (HCM) system reported that company managers do all sorts of strange things when they see data predicting an employee flight risk. Some managers limit their interactions with flight-risk employees, believing that they are going to leave regardless of any mitigating measures—in effect, willfully fulfilling the prediction. Data alone is not enough; people need to be educated on how to use it.

Candidate Data Risks

The increasing use of data in the hiring process means that candidates' data is also now exposed and ripe for misuse and subject to potential bias.

Algorithmically Trained Bias

Bias can be baked into a system. This happened at one internet company when its employees trained a software to review new applicants by looking at patterns in resumes from the last 10 years. Since most of the resumes came from men, the system "learned" that male candidates were preferable, and penalized graduates from women's colleges and words that related to

women such as "women's chess club captain." The company eventually scrapped the system.

The Mystery of Facial Recognition

HireVue, an AI-based interviewing system that tracks facial movements, is currently the subject of a complaint to the FTC by the Electronic Privacy Information Center. The video-based interviewing system is popular for entry-level roles and analyzes tens of thousands of factors, including micro-facial expressions, to come up with a score for every candidate. Science linking facial expressions to work ability is nearly non-existent, yet now career counselors coach job seekers on how to interview on camera for AI analysis. The burden of having to impress (and be rejected by) an opaque algorithm is a new addition to the list of job seekers' stress factors.
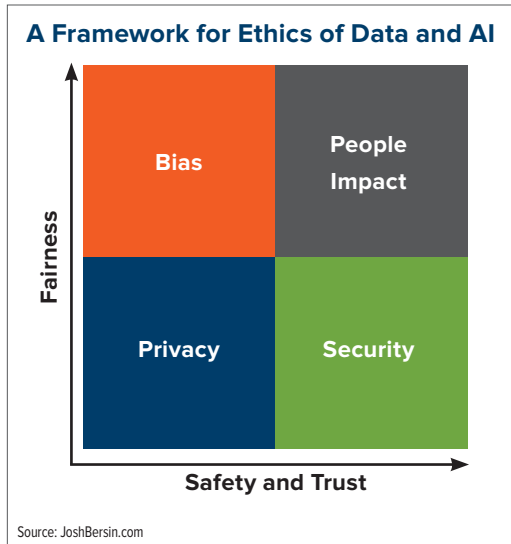
DATA AND TRUST: AN ETHICAL FRAMEWORK

Ethical use of data means that people can trust companies to protect their personal information and use it in ways that don't harm anyone. Thankfully, people do tend to trust their employers. The Edelman 2019 Trust Barometer reports that people trust their employers more than the government, the media and non-governmental organizations. At a global level, 75 percent of people trust their employers to do the right thing.

Despite this high level of trust in employers, there's a gap when people are asked to get more specific. According to the Trust Barometer, 79 percent of people say they expect management to tell the truth, but only 55 percent say that their employer actually does. This has huge implications for companies that collect and store sensitive data.

> Ethical use of data means that people can trust companies to protect their personal information and use it in ways that don't harm anyone.

I introduced the following framework for ethics of data and AI in my report, AI for HR: The New Frontier. The major themes are:

A Framework for Ethics of Data and AI

Bias	**People Impact**
Privacy	**Security**

Fairness (vertical axis)

Safety and Trust (horizontal axis)

Source: JoshBersin.com

Privacy
Employees give you rights to a lot of data—not only to their personal data, but to all the data that's captured from the tools they use on your behalf. This information must stay private and should only be accessible to specific individuals who need it to perform their jobs. The use of this data must also comply with local laws and regulations.

Security
Employee data must be treated with as much concern for security as any other data the company uses. Confidentiality, encryption and access controls are key here.

Bias
Any system that analyzes data must be controlled for bias, or else it could well maintain pre-existing biases. Accounting for bias is also central to compliance with Equal Employment Opportunity Commission (EEOC) regulations.

People Impact
Employees will trust your use of data when they understand why it is being collected and analyzed and exactly how analysis will be used. Be clear about your intent for capturing and using data, and make sure it's helping people rather than making their jobs more difficult or leaving them feeling dehumanized.

Doing It Right
As AI and data-driven HR systems become more prevalent, some companies are doing great things.

Leaders at a large consumer packaged goods company, for example, launched a system that could monitor e-mail traffic, meeting schedules, and even identify unproductive meetings by identifying people who were e-mailing during actual meeting times. After analyzing the data, though, they realized that while the data was incredibly valuable, its use could alienate employees. To be fair and open, leaders created an opt-in program that explicitly explained the new system to employees and the type of data it produced. The program also allows employees to decide whether to make their data available.

In this company's case, a transparent and open approach seemed to work. More than two-thirds of their employees opted in, and more people opt in every month. The HR department has already used the data to make meetings shorter and to give leaders better tools to save people's time—all possible because employees were treated with care.

Another example is a large retailer that uses a video interviewing system to screen candidates. Knowing the potential to create bias and discrimination in the system, the company asked the vendor to hide the candidate's face (making race and nationality impossible to identify) so screeners

> Be clear about your intent for capturing and using data, and make sure it's helping people rather than making their jobs more difficult or leaving them feeling dehumanized.

and hiring managers could review candidates in a more neutral way. Other companies anonymize the names of candidates to remove bias as well.

Policies Matter

Most of the systems for AI-based selection, assessment and productivity improvement are new. Vendors don't have a decade of experience to know how their systems will perform with different types of workers, so the systems are a bit "raw." There is a movement to create what is often called "white-box" or "explainable AI," so system users can see WHY a the software made the recommendation it did. This is still new, however, and most systems remain black boxes.

As an HR leader, you must work with your privacy officer, IT department and data governance team to ensure vigilance for bias, privacy violations and security risks. And you must make it clear to all that employees should know what data is being collected and how it is being used. Additionally, all data-driven employee decisions must be made for the benefit of the employee, not just the employer. (Even a decision not to hire is one that is a benefit to the employee.)

In areas such as recruiting, pay and promotion, it's even more important to audit systems, validate data and ask a statistician to look for validity and drivers of bias. If you decide not to hire someone, give someone a below-average raise or decide against a promotion based on data alone, you should consider how you would defend that decision in court. Just because the data indicates something is true, you must responsibly analyze such decisions to make sure they are fair and valid.

In this new world of data-driven HR, staying focused on ethical use will help you stay out of trouble.

AUDIENCE CONSIDERATIONS

As you look to implement or develop new tools that make use of employee data, it's important to review the impact across three audiences: local laws, your employees and job applicants.

The Law

The widespread generation and use of data has developed so fast that lawmakers are struggling to keep up with their role in protecting user privacy and ensuring ethical use in the general business sector. (There are clear examples to follow in the regulations imposed on industry sectors that deal with sensitive customer information such as finance and healthcare.)

In the U.S., the EEOC regulates employee concerns and the FTC regulates trade. The California Consumer Privacy Act (CCPA) is similar to Europe's General Data Protection Regulation (GDPR) and is being adopted in several dozen other states. Since companies with an online presence can't avoid doing business in California, most are voluntarily complying with the CCPA in all 50 states. Additionally, a Consumer Online Privacy Rights Act was introduced in Congress in late 2019.

When it comes to bias, EEOC guidelines include adverse impact, or the four-fifths rule.

According to the EEOC, adverse impact entails "a substantially different rate of selection in hiring, promotion or other employment decision which works to the disadvantage of members of a race, sex or ethnic group." In other words, if the selection rate for a certain group is less than 80 percent (four-fifths) of that of the group with the highest selection rate, there is an adverse impact on that group, and the organization is vulnerable to charges of discrimination.

Companies can create trust among employees and candidates when they volun-

> As an HR leader, you must work with your privacy officer, IT department and data governance team to ensure vigilance for bias, privacy violations and security risks. And you must make it clear to all that employees should know what data is being collected and how it is being used.

tarily outperform legal expectations relating to bias, privacy and ethical behavior.

Employees

At the most basic level, employees want to know that their personal information, including their home address and Social Security number, is safe. Beyond that, employees are generally aware that their use of company equipment is subject to monitoring, but they may not know how it's being monitored or for what purposes.

In 2018, a Gartner survey of 239 large corporations found that more than half of respondents use some type of non-traditional monitoring techniques, such as analyzing the text of e-mails and social media messages, scrutinizing who's meeting with whom, gathering biometric data and understanding how employees use their workspace. Gartner expects that number to increase to 80 percent in 2020.

Today's tools can vastly improve productivity by identifying impediments to business processes. Still, employees have a right to know if their data is being captured and if it's being anonymized and aggregated. They also need to trust that that their employee data is being used to improve productivity, not just as a means to spy on them. When used in a positive, participatory way, data collection can help retain employees rather than giving them the impression that they're working in a surveillance state.

Job Candidates

Candidates also need to know that their information is safe. Today's recruiting and assessment tools collect a variety of information about candidates—including their faces and psychological profiles—and they have a right to know what is being done with that information. Any testing pro-

gram should be evaluated for privacy and compliance with local regulations.

ORGANIZATIONAL CAPABILITIES FOR ETHICAL DATA USE

To practice ethical data use, your HR organization needs to have the capabilities to govern people-related data, leverage it appropriately and work with other functional areas on policies. HR leaders also need to have a strong relationship with IT to work on technology integrations and to implement enterprise-wide policies. The following are six organizational considerations.

Mindset

The potential of data to transform business is massive, but it's important to ensure that your efforts treat employees as humans, not robots. Is a data-related project going to make life better for employees? Is it going to empower them to do their jobs more efficiently and make work a better place to show up to every day? Would you submit to these practices yourself? Are practices fair and distributed equally among employees who need to be involved?

Traditionally, AI is defined as "artificial intelligence." It is increasingly being referred to as "augmented intelligence," which is actually more accurate. AI helps us make decisions; it does not replace our ability to make decisions. Going forward, we see a world where humans can make better decisions with the information provided by machine-powered tools. However, the tools are no substitute for our ingenuity, creativity or powers of collaboration.

IT-HR Partnership

The IT-HR partnership has never been more important. HR's soft skills are needed more than ever when considering the impact of technology implementations, and HR is even more dependent on IT to

> Today's tools can vastly improve productivity by identifying impediments to business processes. Still, employees have a right to know if their data is being captured and if it's being anonymized and aggregated.

---

get its job done. Make sure your teams understand each other's needs and have open lines of communication.

When defining access controls to data, carefully vet the actual business needs before granting access. One expert says that at least 25 percent of companies don't have a policy telling their IT staffs not to snoop on fellow workers.

HR and Employee Communications

Transparency is key when rolling out any new technology, and that's not possible without effective communication. Workers want to know why their data is being collected, and they will want to see the process improvements made possible by new tools and data analysis.

New Specialist Roles

Many new roles are popping up as organizations seek to comply with regulations and ensure privacy. GDPR requires organizations to have a data privacy officer. Other new roles being created include ethics and compliance manager, privacy analyst and compliance specialist. The areas around data collection and management, data analysis, data quality and data privacy are becoming enormously complex to manage and deserve full-time attention.

Recruiting

There's a lot of innovation around the use of AI for recruiting. Recruiters are increasingly interacting with AI-based tools, and candidates are becoming more aware of their use. One tech company has been using AI-based recruiting tools for some time and takes the approach of treating the AI like any new team member—one that needs onboarding and continuous feedback to operate well.

Organizational Partnerships

Whether it's an augmented customer service app or an AI to improve sales productivity, HR will need to partner with other organizational leaders. How employees react to an AI-based system is an HR issue as much as it is a team issue. Organizational leaders can work with HR to minimize the impact of implementation and to prevent pitfalls.

HOW TO EVALUATE VENDORS

Every market that's faced with rapid change sees an increase in the number of companies innovating new solutions. HR tech is no exception. Given the proliferation of vendors for HR tech, people analytics and other workplace solutions that capture employee data, it's important to have a framework for evaluating new solutions before you sign on. Use these categories to guide you.

Algorithms and Customization

No system is perfect, and we've seen that the potential to replicate pre-existing biases is huge. Ask about how the algorithm or machine learning model was developed and what assumptions it makes. Also ask how much it can be customized and which factors can be customized.

Legal Compliance

Non-compliance is costly, so it pays do your due diligence at the vendor-evaluation stage. Does the solution remove bias and comply with EEOC guidelines and the latest privacy regulations? Does it go above and beyond legal compliance in key areas that matter to your business?

Third-Party Auditing

Third-party auditing via open source or algorithm auditing firms is on the rise. Companies want (and deserve) a third party to confirm the accuracy, consistency, trans-

> Transparency is key when rolling out any new technology, and that's not possible without effective communication.

parency, fairness and legal compliance of new technologies. Ask any potential solution provider if its offering has been audited, and if not, if they would submit to one.

Relevant Customer Examples

You check references on your candidates before they become employees, and you should check the references for new technology solution vendors as well because their solutions could directly impact your employees. Look for customer references in your industry segment or that serve similar employee populations. Set up phone conversations so you can ask specific questions.

LOOKING AHEAD

The positive changes companies have made by implementing new technologies in the workplace are astounding. Processes that once seemed impossible to simplify can now be done much faster with augmented intelligence. The growing care, attention and commitment to making the workplace better for everyone is paying off in dividends, and that potential is accelerating. Companies looking for new solutions to business challenges with technology need to proceed in a way that is ethical, respects your employees' and candidates' privacy and keeps their information secure.

AUTHOR

Josh Bersin is an analyst, author, educator, and thought leader focusing on the global talent market and the challenges and trends impacting business workforces around the world. Earlier this year, Josh launched the Josh Bersin Academy, the only professional development community for HR and talent professionals. Josh is the principal research partner for SHRM Executive Network.

Resources

BuzzFeed News, Uber Executive Suggests Digging Up Dirt On Journalists, November 17, 2014

BuzzFeed News, "God View": Uber Investigates Its Top New York Executive For Privacy Violations," November 18, 2014

Edelman, 2019 Trust Barometer

Edelman, 2019 Trust Barometer

EEOC, UNIFORM GUIDELINES ON EMPLOYEE SELECTION PROCEDURES

Fast Company, Workplace tracking is growing fast. Most workers don't seem very concerned, March 20, 2019

Gartner, Employers are increasingly using nontraditional employee monitoring tools, May 3, 2019

https://joshbersin.com/2018/06/ai-in-hr-a-real-killer-app/

Marriott Press Release, Marriott International to Provide Personal Alert Devices for Housekeepers and Other Hotel Associates Across the US and Canada September 6, 2018

New York Post, Uber settles federal probe over 'God View' spy software, August 15, 2017

New York Times, Working Anything but 9 to 5, August 13, 2014

Pew Research, Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information, November 15, 2019

Philadelphia Inquirer, Hotel housekeeping on demand: Marriott cleaners say this app makes their job harder, July 2, 2018

ProPublica, Amazon Cuts Contracts With Delivery Companies Linked to Deaths October 11, 2019

ResearchandMarkets.com, Global HR Analytics Market Size, June 20, 2019

Reuters, Amazon scraps secret AI recruiting tool that showed bias against women, October 9, 2018

Reveal News, Uber said it protects you from spying. Security sources say otherwise, December 12, 2016

Seattle Times, Starbucks says its scheduling practices have improved, June 4, 2016

The Verge, Amazon warehouse workers skip bathroom breaks to keep their jobs, says report, April 16, 2018

The Verge, How Amazon automatically tracks and fires warehouse workers for 'productivity'. April 25, 2019

Washington Post, Rights group files federal complaint against AI-hiring firm HireVue, citing 'unfair and deceptive' practices, November 6, 2019