Issue: Workplace Surveillance

Workplace Surveillance

By: Lorna Collier

Pub. Date: November 5, 2018
Access Date: November 21, 2018
DOI: 10.1177/237455680433.n1
Source URL: http://businessresearcher.sagepub.com/sbr-1946-108297-2908049/20181105/workplace-surveillance

Will new techniques spark resentment?

Executive Summary

Workplace surveillance and company monitoring of employees are expanding and evolving, aided by technological innovations and enabled by privacy laws that have not kept pace with those developments. A recent survey estimates 98 percent of U.S. and U.K. workplaces have some form of digital surveillance, such as tracking employees through sociometric badges or biometric scanners, scanning emails and social media posts, monitoring computer keystrokes, surveilling with a video camera or monitoring movement through GPS on phones. Businesses use these technologies to improve performance, efficiency and security. But they run a risk that employees will resent what they perceive to be Big Brother-style intrusiveness, and companies also must stay in compliance with a confusing mix of state and federal laws on surveillance.

Among the key takeaways:

- New “people analytics” technology uses artificial intelligence and machine learning to crunch monitoring data and put it to use; about 70 percent of companies worldwide are putting this into place.
- Experts say keeping employees informed about the reasons for monitoring is a better approach than secrecy, because it earns trust and buy-in and avoids low morale, loss of productivity and negative publicity.
- U.S. law has not kept up with technological change, but U.S. companies with employees in Europe are subject to restrictive new digital privacy laws enacted there.

Full Report

Sam Bengston has a microchip embedded in his hand before a horde of cameras last year. (Three Square Market)

When software engineer Sam Bengston, 27, told his family and tech-oriented friends that he had volunteered to have a microchip embedded in his hand as part of his job 18 months ago, they “were not too shocked about it,” he says. The reaction from strangers on Facebook and other social media platforms was a different story.

Bengston was one of the first of nearly 100 employees at Three Square Market, a technology company in River Falls, Wis., that produces

self-service kiosks, to be "chipped," with the near-painless insertion captured on camera for The Washington Post. [1] The comments then began: "People said, 'Why would you do this?' They assumed I was being tracked," he says – even though the chip does not have GPS capabilities. Some religious objectors compared the chip to the "mark of the beast," a sign of the antichrist and the end of days according to the Bible's Book of Revelation, to condemn the practice.

Today, he says, the furor has largely died down, with people more interested in the potential benefits of carrying a radio frequency identification (RFID) chip under one's skin – such as being able to open locked doors or buy snacks with the wave of a hand, rather than fumbling for a key card or cash. He especially appreciates not having to remember or create passwords when he logs on to his computer.

But bigger changes are yet to come, as Bengston helps develop Three Square Market's new chip, expected out sometime next year as part of an additional product line aimed at the medical market. This chip, built in response to requests from potential customers worldwide, is expected to include monitoring of vital signs, encrypted storage for sensitive data such as passports and – yes – GPS tracking, which the company hopes to provide to dementia patients. [2] When it is ready, Bengston expects to have the newer, bigger chip inserted, replacing the one he has now.

"The technology is exploding every day and is transforming data and the HR role."

Microchipping employees is not (yet) common in the workplace. Three Square President Patrick McMullan says since his company began chipping its employees last year, he has heard of just two other U.S. companies following suit. Three Square also was not the first: in 2006, CityWatcher.com, a surveillance firm in Cincinnati, drew headlines for embedding chips in the forearms of two employees. [3] Today, about half of Three Square's workforce has volunteered to be part of the chip experiment. The other half use RFID-enabled wristbands or badges, similar to what many other companies are using to tell who is in a building or accessing software. (McMullan says there are no repercussions for employees who choose not to be chipped. And chipping without consent is illegal in Wisconsin, as well as California, Missouri, North Dakota, and Oklahoma. [4])

Microchip development shows how advances in technology are driving changes to worker monitoring. Companies increasingly are surveilling their employees, for various reasons and in different ways. Such measures can lead to greater productivity and safety. But employers face potential pitfalls, including employee backlash, negative publicity and accusations of Orwellian intrusiveness; possible exposure of sensitive employee data to hackers; and the chance for missteps in the murky legal landscape surrounding employee privacy rights.

"Between employers and hackers, privacy is disappearing fast. I don't expect it to last beyond my lifetime," says Lewis Maltby, a lawyer who heads the National Workrights Institute, which advocates for employee rights and raises concerns about what it regards as the growing use of indiscriminate surveillance.

Today's emerging technologies allow for often-invisible, near-constant monitoring of workers' actions, speech and even moods, which can "create a lot of issues for both the employer and employee," said Paul Stephens, director of policy and advocacy at the Privacy Rights Clearinghouse, a San Diego consumer privacy watchdog group. Stephens said such practices are "unnecessarily invasive." [5]

Earlier Surveillance

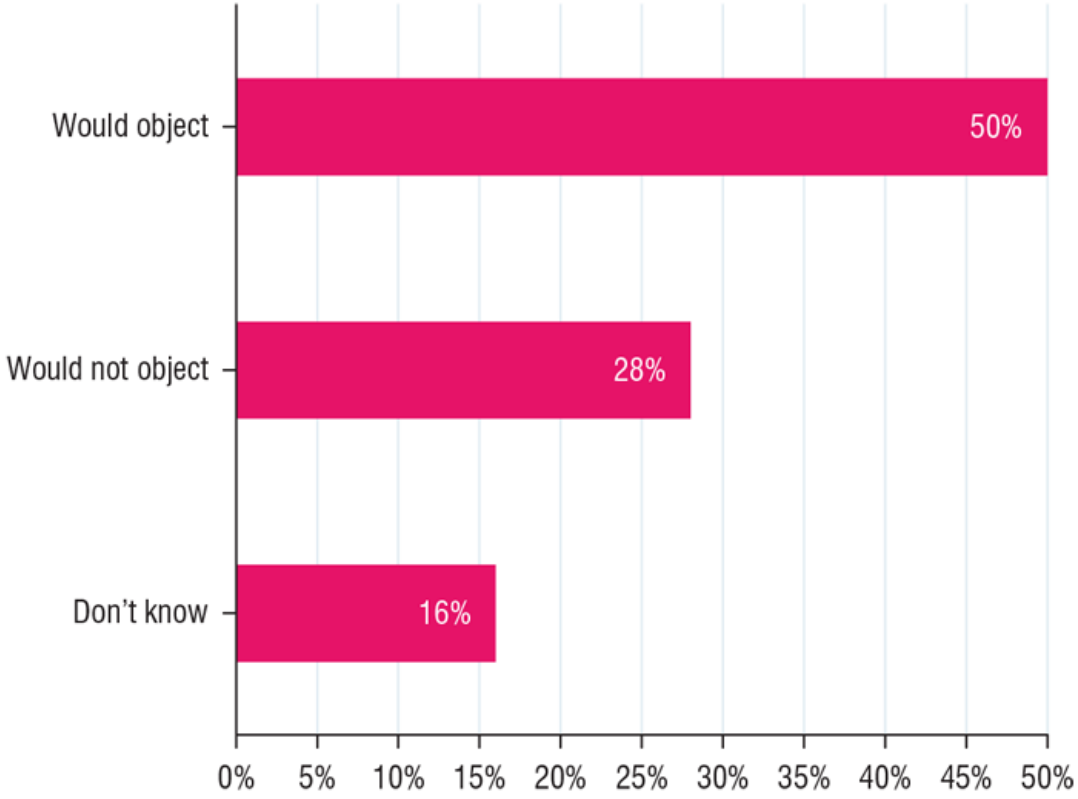
Workplace surveillance is not new. A century ago, Henry Ford used a stopwatch to track factory employees in an effort to achieve greater efficiency on the assembly line he was developing at his automotive company. Even earlier, in the 1800s, employers hired Pinkerton detectives to infiltrate and monitor union employees the companies viewed as threats. [6]

Over time, machines stepped in to automate surveillance: time clocks to see when employees punched in and out, video cameras to monitor security, answering machines to record phone calls. With the computer revolution, digital technology began streamlining these functions; today, capabilities have advanced even further, and new ones have been added.

In addition to the closed-circuit cameras of old, "computer vision" uses artificial intelligence in cameras to spot in real time whether an employee is wearing safety gear and to notify a supervisor if he or she is not. [7] Another software tool commandeers computer webcams to take pictures every 10 minutes of employees who are working from home. [8] Some companies hide tiny cameras in everything from coat hooks to air fresheners, picture frames and coffee pots. [9]

Half Oppose Wearable Tracking Devices

Percentage of employees who would/wouldn't object to using wearable technology



Source: "Workplace Privacy & Protection: Is Your Employer Watching Your Every Move?" 20th HR Metrics & Analytics Summit, 2018, chart 8, https://tinyurl.com/y7ojwnm

Half of all employees surveyed would object to wearing technology that tracks their physical movements in the workplace, according to a 2018 global survey.

Employers have long monitored work-related phone calls and email, but today's software can scan them to determine an employee's mood and report findings to the boss. [10] Everything, from an employee's Fitbit readings to the tone of voice used in a conversation with a co-worker to the way a worker gazes at an object on screen, can be monitored.

"The technology is exploding every day and is transforming data and the HR role," says Baskaran Ambalavanan, a human resources tech specialist and vice president of Hila Solutions, a technology consulting company.

A 2018 survey of IT professionals in the United States and United Kingdom by software firm Alfresco found 98 percent of companies with more than 500 employees were monitoring employees' digital activity. [11] In 2001, according to data from the American Management Association, 80 percent of U.S. companies were monitoring email, computer and/or phone use. [12]

"It's at the point where virtually every major employer in America has some form of electronic surveillance in place," says Maltby, the lawyer for the National Workrights Institute, which is based in Princeton, N.J.

Recent Advances

A wide variety of monitoring tools are in use today, while others are still in the planning stages.

Online retail giant Amazon has patented – but not yet deployed – smart wristbands to track employees; the bands will sense warehouse workers' hand movements and buzz if an employee is moving to the wrong item. [13] Walmart has patented, though it has not yet deployed, a tool that listens in on customer-employee conversations at cash registers to help gauge employee performance and customer satisfaction. [14]

Currently in workplaces:

- Body heat and motion sensors that can determine when employees are sitting at their desks – or not. "Tens of thousands" of OccupEye devices have been placed in hundreds of offices worldwide to reveal how employees are using their workplace, which can help employers design and use office space more efficiently – or, critics might allege, check up on employee movements. [15]

- GPS tracking, which today is shifting from vehicles to employee smartphone apps. A 2012 study by the Aberdeen Group, a tech research firm, found 62 percent of companies with field employees such as delivery drivers or sales staff used GPS tracking, more than double the 30 percent reported in 2008. [16]
- Drones to monitor remote workers, such as railroad employees. [17]
- Sociometric wristbands or badges equipped with microphones to process the tone, volume and speed of workers' conversations, as well as employee movements. Hitachi, the Japanese conglomerate, has developed a badge-like "happiness meter" and a "Happiness Planet" phone app to suss out an employee's mood. [18]
- Fitness trackers, which in some cases are mandatory. A PricewaterhouseCoopers survey in 2016 estimated more than 75 million wearables were expected in the workplace by 2020; Gartner, a Connecticut-based global research firm, predicted two years ago that by 2018, some 2 million workers would be required to wear health trackers on the job. [19]
- Eye tracking using smart eyeglasses with multiple sets of cameras that can see not only what an employee sees, but how he or she sees it, whether focused or distracted. [20]
- Brain-wave tracking via sensors in headgear. Chinese companies are using this technology to monitor employee performance, such as whether a worker is tired and needs a break. [21]
- Biometrics such as fingerprints, facial recognition and iris scans, which are used by 62 percent of organizations surveyed to regulate employee access to buildings and data centers, according to Spiceworks, an Austin, Texas-based IT networking firm; another 24 percent plan to add biometrics by 2020. [22]
- In addition, companies are monitoring digital activity done on work devices or using the company's Web server, including email and Web browsing. At least 66 percent of companies track internet use, 45 percent log keystrokes and 43 percent monitor email. [23]

Companies also monitor employees' use of social media. Only 26 states have laws forbidding employers from requiring employees or applicants to turn over social media passwords. [24]

Ben Waber of Humanyze

New "people analytics" software is available that can pull much of this data together, harnessing the power of artificial intelligence and machine learning to make sense of monitoring results and other HR data about an employee. As a result, businesses can better identify who might be a candidate for promotion, might need additional help – or be a candidate for firing. [25]

Sixty-nine percent of 11,000 global companies surveyed worldwide in a Global Human Capital Trends survey by the consulting firm Deloitte are creating people analytics capabilities, up from 10 to 15 percent in prior years of the report; 17 percent already are using these tools. [26]

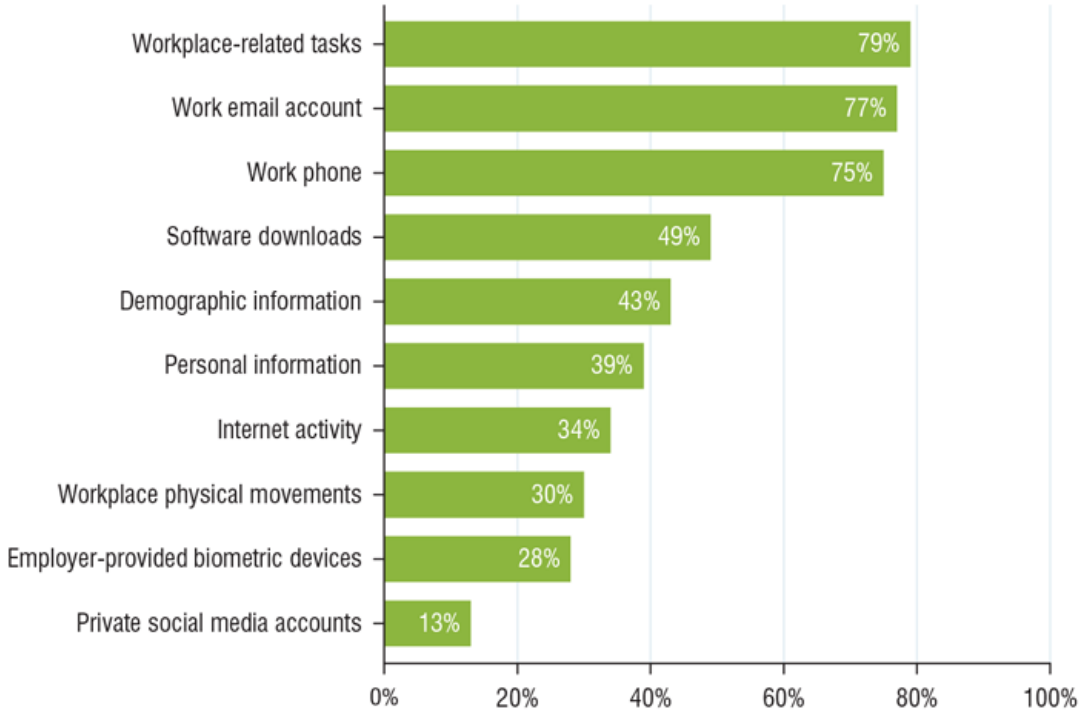
Besides learning more about an individual employee's performance, companies can use data gleaned from observing employee activity to make improvements in security, productivity and efficiency, advocates argue. [27]

"Every aspect of business is becoming more data-driven. There's no reason the people side of business shouldn't be the same," said Ben Waber, founder and CEO of Humanyze, which produces sociometric badges and people analytics software. [28]

Humanyze tools helped Bank of America call centers discover that when teams took breaks together, productivity improved and staff turnover dropped. Three months after Bank of America instituted shared breaks, employees were handling calls 23 percent faster, stress dropped by 19 percent and turnover fell by 28 percent, potentially saving the company billions of dollars over time, according to Humanyze research. [29] Similarly, Hitachi says its happiness meter helped a client company adjust employee break times to let people of similar ages relax together; the change tripled productivity. [30]

Employees Have Mixed Views on Surveillance

Percentage who call monitoring of various activities acceptable



Source: "Workplace Privacy & Protection: Is Your Employer Watching Your Every Move?" 20th HR Metrics & Analytics Summit, 2018, chart 5, https://tinyurl.com/y7ojwnm

Only a small minority of employees think it is acceptable for their employer to monitor their private social media accounts, while three-quarters accept monitoring of work email or phone use, according to a 2018 global survey.

Other examples:

- By tracking the movements of health care workers at Florida Hospital Celebration Health through smart badges, managers discovered some stations did not have enough medicines stocked, causing nurses to waste time tracking down extra supplies. [31]
- In 2009, UPS put about 200 sensors in each of its delivery trucks to track driving speed and other variables. Managers used the information to figure out how drivers could deliver more during their shifts. Four years later, UPS had upped its daily deliveries by 1.4 million additional packages, using 1,000 fewer drivers. [32]
- Point-of-sale video surveillance systems at chain restaurants resulted in a 22 percent average drop in theft and a 7 percent hike in revenue, according to a 2013 study. [33]
- Among the Chinese companies monitoring workers' brainwaves, a power plant claimed the practice had boosted profits by $315 million by allowing for more efficient use of the employees' time. The company said it used brainwave data to determine when employees were stressed or tired, then arranged break times accordingly so that they were working at peak efficiency. [34]

But beyond potential benefits lie possible downsides. Chief among these: the specter of Big Brother, which casts a shadow on many of the technologies, but perhaps most especially on the use of sociometric badges that track an employee's every movement and utterance. The data, along with other monitored metrics, such as time spent online, is then fed into a behind-the-scenes analysis program to judge workplace performance.

"Especially with these new universal monitoring devices, your boss is virtually following you around every minute of the day," says Maltby, the National Workrights Institute lawyer. "Every word you say to a friend at the lunch table or to your spouse on the phone is recorded."

Humanyze says the data from its badges that is given to bosses is aggregated, not identified by person, and that the actual content of conversations is not recorded, only the tone, length and so on. Maltby is skeptical.

"It's so new that no one really knows what's going on," he says. "Are they really keeping the data anonymous? Employers generally want to know everything. If there's a device that each employee is wearing that's collecting every place that each individual employee goes through the day, I have a hard time imagining the employers not wanting to see it."

If the data is not stored anonymously, says Maltby, “privacy will be virtually extinct in the workplace.”

Lewis Maltby

Too little privacy can lead to the opposite of employers’ goal of better job performance, Kenneth Goh, a professor of organizational behavior at the University of Western Ontario’s Ivey Business School, told the CBC.

Goh said studies have shown that workers “thrive when they have some degree of privacy. They do more trial-and-error learning, they’re more willing to make mistakes in private.” He said that tracking on and off the job, such as with Fitbits, is “too Orwellian” and that employees are at risk of losing “the privacy of our actions, our movements, our physiological and emotional states.” [35]

Maltby says it should not be surprising that being surveilled can hurt employee morale, especially if workers find out it has been done secretly. “You don’t need to have an MBA from Wharton to figure out if someone finds out that their boss has been reading their personal emails to their husband, it’s not going to be a motivator,” he says.

Employees who resent monitoring are more likely to become stressed, alienated and less satisfied with their jobs, according to researchers. [36] Ethan Bernstein, an assistant professor of leadership and organizational behavior at Harvard Business School, found in his research that privacy was as essential as transparency for employees; he said those without it felt “exposed and vulnerable,” causing them to become so secretive that some even hid achievements. [37]

Researchers from George Washington University found that electronic performance monitoring led to decreased job satisfaction and increased counterproductive work behaviors, such as theft, absenteeism and cyberloafing. [38] Upset employees also may take their concerns public, resulting in negative publicity and possible brand damage. Amazon, for example, has been hit hard by employee accounts of “constant surveillance,” among other complaints. [39]

Another concern: data hacking, which can expose not only an employee’s financial and health information, but also biometric data, such as fingerprints or iris scans, which increasingly are being collected by employers. A 2015 data breach at the federal government’s Office of Personnel Management, for example, resulted in the theft of 5.6 million fingerprints. [40] A 2018 survey by the HR Metrics & Analytics Summit found 48 percent of employees did not trust their company to protect their data. [41]

Ethical monitoring?

How should companies approach monitoring? Are there ethical ways to surveil employees? The first step is open communication, says Kate Bischoff, a Minneapolis employment attorney.

“Companies are already looked at as the Goliath in any situation and the employee is always the David,” she says. “Well, now we have the Goliath as Big Brother, too – and that puts a lot of fear into employees. We have to make sure employees understand that this is something to help the business – and to help them as well.”

Bischoff cites the London Daily Telegraph newspaper’s 2016 decision to put OccupEye sensors under staffers’ desks without prior notification. Workers complained, the news went viral and the Telegraph pulled the sensors. [42] However, says Bischoff, the company did not install the devices to spy on workers, but rather to help save money – and jobs – by determining a more efficient use of space. “Had they told them, ‘We’re trying to figure out if we can reduce our real estate so that we don’t have to fire you,’ people wouldn’t have freaked out or contacted BuzzFeed,” she says.

Watch video with University of North Carolina communications professor Steve May on technology and surveillance:

Ambalavanan, the Hila Solutions HR tech specialist, agrees that businesses gain “a better buy-in” through communication with employees. He recommends companies have clear policies covering when and how employees might be monitored; have employees read and sign off on them; and have a forum or some other way to address employee concerns “before they become news.”

Another issue for employers is compliance with employee privacy laws.

The law, unfortunately, "doesn't do a very good job" of addressing surveillance and monitoring, says Bischoff. Some federal regulations cover aspects of the myriad issues raised, while some states have adopted laws to try, in piecemeal fashion, to deal with concerns.

Alaska, Connecticut, Illinois, Massachusetts, New Hampshire and Washington are among states that have passed regulations governing how employers handle workers' biometric data. [43] (Illinois' law, which was the first, is particularly tough, and has resulted in more than 60 class-action lawsuits against employers. [44]) Connecticut and Delaware prohibit employers from monitoring employee email or internet access without prior written notice. [45] California, meanwhile, has led the nation in consumer privacy regulations, including requirements for notification regarding GPS monitoring. This law helped a California salesperson, Myrna Arias, win a settlement with her employer, Intermex Wire Transfer, after the company fired her for deleting a GPS tracking app from her company-issued smartphone. [46]

"Between employers and hackers, privacy is disappearing fast."

In general, though, the law has not kept up with the rapid pace of technology, Bischoff says.

The federal regulation most on point is the Electronic Communications Privacy Act of 1986, which regulates the monitoring of employees' personal communications. "The only problem is, it applies to telephones because that's all there was in 1986," says Maltby. "You would think sometime in the last 34 years, Congress might have gotten around to saying, 'Let's apply the same concept to other forms of electronic communication.' But despite a great deal of urging by lots of people, it never happened."

Bischoff says privacy is "a difficult concept for Congress to tackle" because of the complexity of the issues. There isn't necessarily a partisan angle at play either, she adds, saying that while Republicans are currently in power, "it's not clear that Democrats would put this on the top of their agenda, either."

In Europe, on the other hand, a far-reaching electronic privacy law, the General Data Protection Regulation (GDPR), went into effect on May 25. This law regulates what companies can do with peoples' data and how long it can be kept, with penalties for violators of up to 20 million euros (about $23 million). Though it is a European Union regulation, it covers any company, including U.S.-based ones, with employees in Europe. [47]

"This kind of privacy legislation does affect what we do here in the U.S.," says Bischoff, since many companies have European-based workers.

Another factor for employers to consider: whether a labor union is present. Where that is the case, surveillance practices must be part of collective bargaining and employers cannot surveil employees who are organizing, says Felicia Davis, partner in the employment division at Paul Hastings LLP, a Los Angeles-based law firm.

Paula Brantner, a senior adviser to Workplace Fairness, an employee-rights advocacy group in Silver Spring, Md., says that unions have been able to "create some boundaries and limitations for the employer." Employers with unionized workforces can still monitor their workers, but it must be done with employees' consent and knowledge, she says.

In general, says Davis, employers need to "make sure that employees know that they are being monitored or may be monitored. The actual law on it will vary from state to state in terms of whether [businesses] have to do it," she says, but notification is a good defense against any potential invasion-of-privacy claims.

Employers also need to make sure that they are not so enticed by the latest, shiny new technology that they institute something unnecessary, says Maltby. "Employers – maybe Americans in general – we love technology," he says. But sometimes technology solutions "are not nearly as good as some of the old-fashioned ones."

Brantner agrees. "Some of the technology is very far-reaching," she says, "but that doesn't mean you have to institute everything that's available."

About the Author

Lorna Collier is a business and health writer whose reporting has appeared in the Chicago Tribune, AARP Bulletin, U.S. News & World Report, CNN.com, Workforce Management, Crain's Chicago Business, Monitor on Psychology and many other publications. She can be reached on Twitter at @lornacollier or via email (lorna@lornacollier.com). Previously, she reported for Business Researcher on workplace violence.

Chronology

1888-1992	**Early efforts to use technology for workplace surveillance**
1888	The first time clock is invented by Willard Le Grand Bundy to track workers' time on the job.
1911	Frederick Winslow Taylor, a mechanical engineer and efficiency expert, publishes Principles of Scientific Management, touting time and motion studies of workers to improve job performance.
1914	Auto pioneer Henry Ford starts the Ford Motor Co.'s Sociological Department; staffers monitor employees at work and at home.
1935	The National Labor Relations Act, protecting the rights of workers to bargain and preventing employers from surveilling union activity, is enacted.
1975-1978	Microcomputers (also known as PCs) are introduced into the workplace.
1986	The federal Electronic Communications Privacy Act passes, making the intercepting and monitoring of electronic communications unlawful; business communications generally are exempt, particularly if carried out on company-owned devices.
1991	The World Wide Web is created by Tim Berners-Lee.
1992	Mosaic – the first internet browser with a graphical user interface – is developed, driving internet growth in business among companies and consumers.
Late 1990s-Present	**Widespread adoption of surveillance in businesses.**
2001	An American Management Association survey of 435 employers finds nearly 80 percent surveil employees, with about 62 percent monitoring internet use.
2006	Wisconsin is the first state to ban mandatory radio frequency identification (RFID) microchipping of employees.
2008	Illinois passes the Biometric Information Privacy Act, making it the first state to restrict how business gather, use and store employee's fingerprints, DNA or other biometric data.… The federal Genetic Information Nondiscrimination Act (GINA), which restricts the way employers use employees' genetic information, is enacted.
2014	The software company Sociometric Solutions (later Humanyze) develops a sociometric ID badge for employees that can track movements and conversations.
2017	A California woman, Myrna Arias, settles a lawsuit against a former employer for firing her after she removed a GPS tracking app from her company-issued cellphone to prevent 24/7 surveillance.
2018	An amendment to Illinois' Biometric Information Privacy Act proposed to make employers exempt from restrictions governing the collection and maintenance of biometric data, which critics say would gut worker protections; the amendment is pending.

Resources for Further Study

Bibliography

Books

Bagley, Constance E., "Managers and the Legal Environment: Strategies for Business, 9th Edition," Cengage Learning, 2018. A Yale senior research fellow and former law professor looks at current legal issues facing business, including employers' right to restrict social media and international privacy laws such as Europe's General Data Protection Regulation.

Indiparambil, Jijo James, "Electronic Surveillance and Privacy in the Workplace: A Theological-Ethical Response," Lap Lambert Academic Publishing, 2017. A Belgian business ethics researcher examines whether spying on employees is counterproductive.

Waber, Ben, "People Analytics: How Social Sensing Technology Will Transform Business and What It Tells Us About the Future of Work," FT Press, 2013. The CEO and co-founder of the software company Humanyze explores how sensors and analytics can help companies improve performance and employee morale.

Articles

Dai, Hengchen, et al., "The Impact of Time at Work and Time Off From Work on Rule Compliance: The Case of Hand Hygiene in Health Care," Journal of Applied Psychology, May 2015, https://tinyurl.com/y8hdtxj5. Business researchers from the University of Pennsylvania and University of North Carolina studied whether monitoring health care workers' handwashing practices had beneficial results – and what happened when monitoring was ended.

Fusi, Federica, and Mary K. Feeney, "Electronic monitoring in public organizations: evidence from US local governments," Public Management Review, Nov. 10, 2017, https://tinyurl.com/yb7mwmp4. Arizona State University researchers reviewed the state of electronic monitoring in small- and medium-sized municipalities.

Miller, Andrea, "More companies are using technology to monitor employees, sparking privacy concerns," ABC News, March 10, 2018, https://tinyurl.com/ybnjousk. A reporter gives an overview of newer surveillance technologies and their legal implications.

Reports and Studies

"State Social Media Privacy Laws," National Conference of State Legislatures, Jan 2, 2018, https://tinyurl.com/jv9ha2f. A bipartisan organization examines and lists the states with laws regulating whether employers can require employees or applicants to submit social media usernames and passwords.

"Your Employer May Be Watching Your Every Move: Employees Find Workplace Monitoring Objectionable, Says New Survey," PRNewswire, June 7, 2018, https://tinyurl.com/ybmds359. A survey of 250 global human resources professionals found that most employees are concerned about data privacy but accept some type of monitoring as long as it is work-related.

Ella, V. John, "Employee Monitoring and Workplace Privacy Law," American Bar Association National Symposium on Technology in Labor and Employment Law, April 2016, https://tinyurl.com/yadlskov. The American Bar Association gives an overview of current law and recent cases covering different aspects of workplace surveillance/monitoring and worker privacy.

The Next Step

Devices

Campbell, Dakin, "HSBC is making a $130 million investment in its bank branches and the latest step is to arm its bankers with Samsung watches," Business Insider, Oct. 22, 2018, https://tinyurl.com/y7xsk5p6. To improve communication, the bank's branch managers will use Samsung watches to send and receive messages and speak to colleagues using a microphone.

Dundas, Suzie, "Kinetic Uses A.I. To Monitor Workplace Movement – But It Isn't Aiming To Be Big Brother," Forbes, Oct. 25, 2018, https://tinyurl.com/yag97hze. A new wearable device, which detects unsafe body positioning and movements and alerts the wearer, aims to help prevent workplace injuries and improve worker safety.

Ma, Alexandra, "Thousands of people in Sweden are embedding microchips under their skin to replace ID cards," Business Insider, May 14, 2018, https://tinyurl.com/ybch9sty. About 3,000 people in Sweden have accepted implanted microchips, which eliminate the need for office key cards and IDs. The chips even take the place of train tickets.

Legal Action

Cimpanu, Catalin, "Wendy's faces lawsuit for unlawfully collecting employee fingerprints," ZDNet, Sept. 23, 2018, https://tinyurl.com/y9mfqdly. A class-action lawsuit filed by former employees of the fast-food company alleges that Wendy's does not disclose what it does with employee fingerprints collected by biometric scanners.

Grimes, Steven, and Eric Shinabarger, "Biometric Privacy Litigation: The Next Class Action Battleground," Bloomberg Law, Jan. 17, 2018, https://tinyurl.com/y7c3tgg8. About 60 class-action lawsuits have been filed under Illinois' decade-old Biometric Information Privacy Act, which covers how employers use employees' biometric data.

Hong, Nicole, "At Stake in Lawsuit: What Can Bosses Access on Your Personal Devices?" The Wall Street Journal, Sept. 9, 2018, https://tinyurl.com/yak2n36r. A lawsuit alleges that a company accessed a former employee's home computer to read his email and steal data. Legal experts say the case raises questions about the boundaries between work and personal devices.

Organizations

American Management Association
1601 Broadway, New York, NY 10019
1-877-566-9441

www.amanet.org
customerservice@amanet.org
@amanet
Professional management organization that provides training, seminars, podcasts and other services, plus information about management topics, including workplace surveillance.

Electronic Frontier Foundation
815 Eddy St., San Francisco, CA 94109
1-415-436-9333
www.eff.org
info@eff.org
@EFF
Organization focused on civil liberties in a digital world; answers legal inquiries and provides advocacy, online privacy tools and other resources.

Electronic Privacy Information Center (EPIC)
1718 Connecticut Ave., N.W., Suite 200, Washington, DC 20009
1-202-483-1140
www.epic.org
info@epic.org
@EPICPrivacy
An independent research center aimed at focusing attention on privacy and human rights issues; maintains other sites such as privacy.org and privacycoalition.org.

National Workrights Institute
128 Stone Cliff Road, Princeton, NJ 08540
1-609-683-0313
www.workrights.org
info@workrights.org
@usworkrights
Founded in 2000 by former staff of the American Civil Liberties Union's National Taskforce on Civil Liberties in the Workplace, this advocacy organization provides legal databases and information about workplace privacy and human rights issues.

Privacy Rights Clearinghouse
3033 5th Ave., Suite 223, San Diego, CA 92103
1-619-298-3396
www.privacyrights.org
admin@privacyrights.org
@PrivacyToday
Privacy-rights organization that responds to consumer complaints and questions about privacy issues; maintains a database of articles, reports and other resources.

Society for Human Resource Management (SHRM)
1800 Duke St., Alexandria, VA 22314
1-800-283-SHRM (7476)
www.shrm.org
@SHRM
The world's largest HR professional organization, with 300,000 members in 165 countries; it has a large database of articles about workplace surveillance and monitoring.

Workplace Fairness
8121 Georgia Ave., Suite 600, Silver Spring, MD 20910
1-240-772-1205
www.workplacefairness.org
@work_fairness
Organization promoting employee rights; it maintains a database of employment lawyers and guides to workplace issues, including surveillance.

Notes

[1] Danielle Paquette, "Some feared hackers and the devil. Others got microchipped," The Washington Post, Aug. 1, 2017, https://tinyurl.com/ych9n83j; Chloe Aiello, "Wisconsin company known for microchipping employees plans GPS tracking chip for dementia patients," CNBC, Aug. 22, 2018, https://tinyurl.com/y83nt9s7.

[2] Aiello, ibid.

[3] Todd Lewan, “Microchips in humans spark privacy debate,” Associated Press, July 21, 2007, https://tinyurl.com/y9nl642q.

[4] Paquette, op. cit.

[5] Amy Delgado, “Employee privacy at stake as surveillance technology evolves,” CBS News, Aug. 14, 2018, https://tinyurl.com/y9ywazrq.

[6] Ifeoma Ajunwa, Kate Crawford and Jason Schultz, “Limitless Worker Surveillance,” California Law Review, June 1, 2017, https://tinyurl.com/ycca83fv.

[7] “There will be little privacy in the workplace of the future,” The Economist, March 28, 2018, https://tinyurl.com/ycodtl3l.

[8] Olivia Solon, “Big Brother isn’t just watching; workplace surveillance can track your every move,” The Guardian, Nov. 6, 2017, https://tinyurl.com/ycva5ccl.

[9] “Hidden Devices Scrutinize Employees,” University of Denver Daniels College of Business, Jan. 8, 2015, https://tinyurl.com/y7h44d59.

[10] Josh Bersin, “People Analytics: Here With a Vengeance,” Forbes, Dec. 16, 2017, https://tinyurl.com/y87qotr2.

[11] Tim Sandle, “Watch out, your employer may be watching you,” Digital Journal, June 24, 2018, https://tinyurl.com/yb7klx5r.

[12] “2001 AMA, US News, ePolicy Institute Survey: Electronic Policies and Practices | Summary of Key Findings,” ePolicy Institute, 2001, https://tinyurl.com/y7oa34ud.

[13] Thuy Ong, “Amazon patents wristbands that track warehouse employees’ hands in real time,” The Verge, Feb. 1, 2018, https://tinyurl.com/yb5ucajw.

[14] Delgado, op. cit.

[15] Claire Zillman, “Here’s Yet Another Way Your Boss Can Spy on You,” Fortune, Jan. 13, 2016, https://tinyurl.com/jjojcb7.

[16] Ibid.

[17] Marco Margaritoff, “Union Pacific is Using Drones to Monitor Railroad Employee Safety,” The Drive, March 14, 2018, https://tinyurl.com/ybgp4p55.

[18] Scott Wilson, “Hitachi invents ‘happiness meter’ which monitors your every move (and then tell your boss),” SoraNews24, Feb. 11, 2015, https://tinyurl.com/ydc97rvo; “Hitachi develops smartphone technology measuring happiness,” news release, Oct. 2, 2017, https://tinyurl.com/y8gdj36q.

[19] Teena Maddox, “The future of wearables and their role in the workplace,” TechRepublic, May 13, 2016, https://tinyurl.com/yad73o7r.

[20] James Watkins, “Soon, your boss will be watching your every eye movement – get ready,” Ozy, May 30, 2017, https://tinyurl.com/yaovcpz3.

[21] Tara Francis Chan, “China is monitoring employees’ brain waves and emotions – and the technology boosted one company’s profits by $315 million,” Business Insider India. April 30, 2018, https://tinyurl.com/y8kxyw2s.

[22] “Spiceworks Study Reveals Nearly 90 Percent of Businesses Will Use Biometric Authentication Technology by 2020,” Spiceworks, March 12, 2018, http://tinyurl.com/yczjsqaa..

[23] “The rise of workplace spying,” The Week. July 5, 2015, https://tinyurl.com/ycm2hz4g.

[24] “State Social Media Privacy Laws,” National Conference of State Legislatures, Jan. 2, 2018, https://tinyurl.com/jv9ha2f.

[25] Mark Swartz, “Five Trends in Monitoring and Tracking Employees,” Monster Worldwide, 2018, https://tinyurl.com/yarx86zm.

[26] Bersin, op. cit.

[27] Ryan Derousseau, “The tech that tracks your movements at work,” BBC, June 14, 2017, https://tinyurl.com/ya7r5kmw.

[28] “There will be little privacy in the workplace of the future,” op. cit.

[29] Ron Miller, “New Firm Combines Wearables and Data to Improve Decision Making, Feb. 24, 2015, https://tinyurl.com/y8zh6swe.

[30] Wilson, op. cit.

[31] Lee Michael Katz, “Monitoring Employee Productivity: Proceed with Caution,” Society for Human Resource Management, June 1, 2015, https://tinyurl.com/hdd3ay2.

[32] “The rise of workplace spying,” op. cit.

[33] Ibid.

[34] Stephen Chen, “ ‘Forget the Facebook leak’: China is mining data directly from workers’ brains on an industrial scale,” South China Morning Post, July 17, 2018, https://tinyurl.com/y7zkdcx5.

[35] “Too Orwellian? Companies monitoring personal time, for ‘self-improvement,’ ” CBC News, Sept. 15, 2015, https://tinyurl.com/yamwkfk4.

[36] Ellen Ruppel Shell, “The Employer-Surveillance State,” The Atlantic, Oct. 15, 2018, https://tinyurl.com/y7q6lvp7.

[37] Ethan Bernstein, “The Transparency Trap,” Harvard Business Review, October 2014, https://tinyurl.com/nw6w4un.

[38] David L. Tomczak, Lauren A. Lanzo and Herman Aguinis, “Evidence-based recommendations for employee performance monitoring,” Business Horizons, Volume 61, Issue 2, March-April 2018, pp. 251-259, https://tinyurl.com/yanct4qj.

[39] Shona Ghosh, “Peeing in trash cans, constant surveillance, and asthma attacks on the job: Amazon workers tell us their warehouse horror stories,” Business Insider, May 5, 2018, https://tinyurl.com/y7mr8yqw.

[40] Everett Rosenfeld, “Estimated 5.6M had fingerprints stolen in hack: OPM,” CNBC, Sept. 23, 2015, http://tinyurl.com/yakl36o7.

[41] Andie Burjek, “Monitor Responsibly: How Employers Are Using Workplace Surveillance Devices,” Workforce.com, Aug. 31, 2018, https://tinyurl.com/y9byrmba.

[42] Ben Quinn and Jasper Jackson, “Daily Telegraph to withdraw devices monitoring time at desk after criticism,” The Guardian, Jan. 11, 2016, https://tinyurl.com/ybq7uhs4.

[43] Lisa Nagele-Piazza, “How will workplace GPS tracking and biometric data collection trends affect HR?” Society for Human Resource Management, Jan. 8, 2018, https://tinyurl.com/yctfbe73.

[44] Steven Grimes and Eric Shinabarger, “Biometric Privacy Litigation: The Next Class Action Battleground,” Bloomberg Law, Jan. 17, 2018, https://tinyurl.com/y7c3tgg8.

[45] “State Laws Related to Internet Privacy,” National Conference of State Legislatures, July 25, 2018, https://tinyurl.com/lzm4sbs.

[46] Kaveh Waddell, “Why Bosses Can Track Their Employees 24/7,” The Atlantic, Jan. 6, 2017, https://tinyurl.com/y9bhot5s.

[47] Sara Jodka, “The GDPR Covers Employee/HR data and It’s Tricky, Tricky (Tricky) Tricky: What HR Needs to Know,” Dickinson Wright, April 2018, https://tinyurl.com/y8ze3otr.