

FEATURE

Workplace Privacy Expectations Shift for Younger Employees

July 16, 2025 | Nancy Mann Jackson



In 2022, after a Florida-based software company fired a remote employee based in the Netherlands for refusing to keep his webcam turned on, a Dutch court ruled in favor of the worker. The company had to pay the employee 75,000 euros, according to the [BBC](https://www.bbc.com/news/technology-63203945) - (<https://www.bbc.com/news/technology-63203945>).

In another case the following year, the Illinois Supreme Court found fast food chain White Castle was guilty of sharing employees' biometric data with a vendor without employee consent, according to the [American Bar Association](https://www.americanbar.org/groups/business_law/resources/business-law-today/2023-may/illinois-supreme-court-finds-white-castle-could-face-up-to-17b-in-damages/) - (https://www.americanbar.org/groups/business_law/resources/business-law-today/2023-may/illinois-supreme-court-finds-white-castle-could-face-up-to-17b-in-damages/). The Ohio-based restaurant chain required employees to scan their fingerprints to access their paystubs and provided the fingerprint data to an outside vendor to manage payment processing, which ran counter to the Illinois Biometric Information Protection Act.

New technologies have made it possible for employers to have greater access to employees and their data, but cases such as these show that going too far can have negative consequences. And younger generations of workers have different ideas about digital privacy than their older co-workers, making digital privacy an important component of the employee experience.

"If Gen Xers [born between 1965 and 1980] and Baby Boomers [born between 1946 and 1964] simply accept certain privacy regulations, younger employees are asking why," said Peter Miscovich, executive managing director and global future of work leader at global real estate and investment services company JLL. "They want to know, 'How is this being done and why is it being done?' and they're interested in being involved in designing privacy policies."

About two-thirds of global IT and business leaders (68%) said they believe failing to meet the digital experience demands of younger workers will lead employees to consider leaving the company, according to a [survey](https://www.riverbed.com/riverbed-wp-content/uploads/2023/09/global-dex-survey-2023-report.pdf) - (<https://www.riverbed.com/riverbed-wp-content/uploads/2023/09/global-dex-survey-2023-report.pdf>) by telemetry data firm Riverbed. As digital natives enter the workforce with new expectations, employers must evolve or risk losing employees' trust.

Whether you're new to HR or looking to sharpen your skills, build a strong foundation of HR knowledge and skills and elevate your professional impact.



The Generational Shift

There are a number of reasons why people in Gen Z (born between 1997 and 2012) and Gen Alpha (born after 2012) view privacy differently from previous generations. First, they are digital natives who may have a deeper inherent understanding of all the data available through online systems and the ability for organizations to access and use it.

A 2024 [Cisco survey](https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf) - (https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf) shows that younger consumers are more aware of privacy laws and more active in taking steps to protect their privacy. For example, 49% of survey respondents between the ages of 25 and 34 were classified as Privacy Actives — people who are concerned about digital privacy and willing to take action to protect it — compared to just 33% of both those ages 45 to 54 and those ages 55 to 64.

Also, Gen Z came of age when data privacy was in the spotlight. During the 2010s, British consulting firm [Cambridge Analytica accessed personal data](https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html) - (<https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>) belonging to millions of Facebook users for political advertising without consent. Facebook's parent company, Meta, eventually paid millions to settle the resulting lawsuit, and the controversy altered the public's view of technology companies and their access and handling of personal data.

As they populate the workplace, members of Gen Z and Gen Alpha expect their privacy concerns to be taken seriously. "A big mistake some organizations make is taking a top-down approach, tracking employees' time in the office or overseeing social media usage," Miscovich said. "Baby Boomers and Gen X were much more compliant, but younger workers want to know the how and the why, and the outcomes you're looking to achieve."

Preventive Health, Food as Medicine, and What's Next for Workforce Wellness | Tomorrowist

SHRM



Watch on

The Surveillance Backlash

Workplace [surveillance technology](https://www.shrm.org/topics-tools/research/clock-home-post-covid-19-employee-monitoring-workplace) - (<https://www.shrm.org/topics-tools/research/clock-home-post-covid-19-employee-monitoring-workplace>), including the use of AI to monitor workers, became increasingly common during and after the onset of the pandemic. Over the past several years, as new technologies have made surveillance easier, employers have monitored employees' emails and files, installed webcams on work computers, tracked when and how much a worker is typing, and monitored workers' calls and movements with trackable devices and other technologies.

Not surprisingly, employer surveillance is unpopular across the board, but especially among younger workers. In a [2024 survey](https://checkr.com/resources/articles/state-of-digital-privacy-and-safety-2024) - (<https://checkr.com/resources/articles/state-of-digital-privacy-and-safety-2024>) by background check company Checkr, when employees of all ages were asked if they felt employers' monitoring of their online activity during work hours was an invasion of privacy, 65% of respondents agreed or were on the fence. Agreement was inversely related to age: 72% of Gen Z respondents, 67% of Millennials, 63% of Gen Xers, and 60% of Baby Boomers agreed that their privacy was being invaded or that they were undecided about this issue. This discomfort with surveillance is so strong among younger employers that many are willing to make trade-offs: 54% of Gen Zers said they would consider taking a pay cut for enhanced privacy at work.

As younger workers have greater privacy expectations, traditional employer surveillance programs may alienate them. These workers want to be evaluated based on their outcomes rather than the minutes they spend on a task, said Danita Torres, executive vice president of operations and client services at Congruity HR.

"When it comes to building an employee experience that simultaneously delivers business results and keeps the best employees engaged, trust is everything," said Ethan McCarty, founder and CEO of employee experience agency Integral. "Using monitoring tools in ways that employees perceive as sneaky or malicious can quickly erode that trust, especially for younger workers who already view privacy differently and expect more transparency. If people feel like they're constantly being watched, they're less likely to feel valued and more likely to disengage. Essentially, you're pushing a transaction rather than a relationship. The dynamism of today's workplace calls for intentional, well-designed approaches that balance accountability with respect for individual boundaries."

Cases such as the Dutch webcam and White Castle rulings underscore that missteps around employee privacy don't just erode trust — they can have serious financial and legal consequences. As individuals have become increasingly concerned about digital privacy, new government regulations such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) are taking shape to support those concerns. “The laws are just catching up with what Gen Z and Millennials already expect: consent, access, and control over their data,” Torres said. “Things like GDPR and the California [Consumer] Privacy Act support those values. When companies comply with these laws, it signals to employees that their privacy matters, and that builds trust, especially with younger workers, by mirroring what they have come to expect: data transparency, control, and accountability.”

More regulations such as these are expected, and HR leaders will need to assist with compliance and enforcement efforts, Miscovich said. He expects that compliance and enforcement with privacy regulations will eventually be AI-enabled.

Ensure Compliance and Protect Privacy: Master Global Data Privacy with GDPR 

With this tension between managing risk and protecting employee trust, employers must endeavor to develop solutions that work for everyone. It's possible to strike a balance between risk and trust, fulfilling employer obligations without jeopardizing employee relationships.

Lead Organizational Change with Efficiency and Confidence: Practical Strategies for HR Professionals. Master SHRM's six step change framework to drive organizational success.

Even after the policy is developed, continue to allow for regular employee input. “Make sure employees know how to raise concerns, and that you’ll listen,” Torres said. “They want to know their voice is heard. One thing that’s worked well for us is creating a ‘Just Ask’ forum where our employees can ask questions privately or in a group setting. These questions are addressed monthly in our town hall meetings. It ensures that our team feels that our leaders are more transparent and less like Big Brother.”

Be transparent about how you track or monitor employees and their data.

"If you're collecting data such as productivity data or system usage, just explain what you're doing and why," Torres said. "In my experience, employees are usually fine with it if they understand the benefit and feel like they have a say. Offering opt-in choices or creating simple explainer sessions can go a long way in building that trust."

Miscovich recommended using digital dashboards that provide transparent visibility of what's being tracked, why it's needed, and how it's protected.

"Frame tracking as a tool for support and optimization, not punishment," McCarty said. "When people feel informed and included, they're more likely to act in good faith."

Revisit privacy policies regularly.

As technology and privacy regulations evolve, employers must be prepared to refresh their policies regularly. "Be sure your policy is continuing to meet enterprise objectives, workforce objectives, and employee expectations," Miscovich said.

The future of workforce strategy lies in privacy policies that reflect cultural values, not just legal requirements. Landing on the right balance of privacy and data security will depend on successful partnerships among CHROs and technology leaders, Miscovich added. "It's a new world in 2025, and the topic of privacy needs lots of attention," he said. "The responsibility for success on this topic lies with HR, IT, and the enterprise."

It's widely understood that high-quality, intentionally designed employee experiences have a direct impact on strong business outcomes. However, in a dynamic marketplace with rapid technology shifts and a diverse workforce, "a one-size-fits-all approach to privacy won't work," McCarty said. "Stay curious, keep listening, and design flexible privacy practices that respect different comfort levels while still protecting the business."

Nancy Mann Jackson is a freelance journalist and content writer who writes regularly about finance, insurance, HR, health care, and education. Her work has appeared in Entrepreneur, Forbes, Fortune, CNBC, and many other outlets.

The **SHRM CP/SCP Certification** - (<https://www.shrm.org/credentials/certification/organizations/certify-my-team>) is the gold standard for HR practitioners. The skills & knowledge learned during certification preparation are considered the most essential for an impactful and strategic HR professional.

Was this resource helpful?

[Leave Feedback](#) ➤

Advertisement