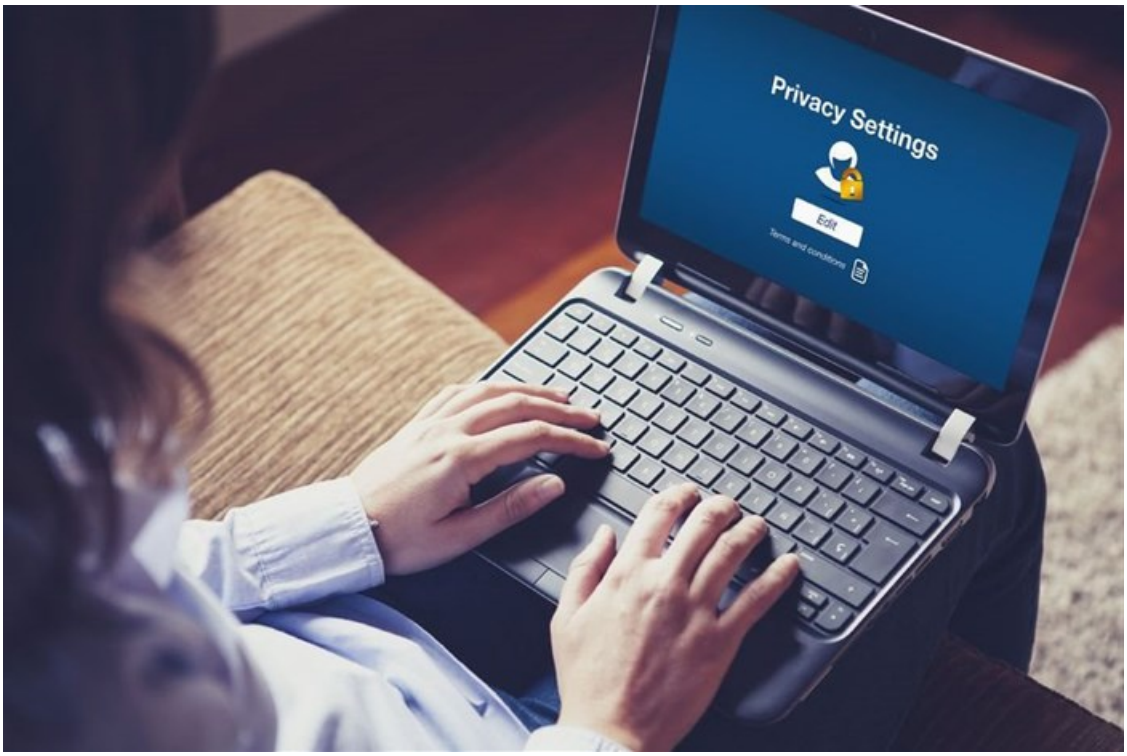
BIZCOMMUNITY

Employee privacy is as important as consumer privacy

By Andrew Bourne

4 Jun 2021

Of late, there have been a lot of headlines around major technology players putting customer privacy first and making data privacy one of their core values. The business landscape is hurriedly re-orienting itself to provide the digital consumer a safe space where their data is protected round the clock. Meanwhile, there's another important stakeholder whose privacy equally matters. Employees have just as much right to privacy in the workplace.



Recent trends like remote working and hybrid models have heightened the importance of employee privacy

Forced to switch overnight to remote work, organisations turned to digital collaboration and productivity tools to enable their workforce to continue their day-to-day operations. With little to no time to vet third-party vendors, organisations had to purchase and implement technology quickly or use free applications without weighing vulnerabilities. But this hasty transition was not without its risks, especially for employees. For instance, the steep rise in user base for video conferencing tools caught the hackers' attention and live meetings were invaded in some cases. Moreover, audio/video calls while working from home means that varied details of employees' personal lives are archived in vendors' data records, at risk of being compromised unless the vendor has a stringent data protection programme.

Many companies introducing remote monitoring software when their employees began working from home also raised a lot of privacy concerns. According to Gartner, more than one out of four companies purchased technology during the pandemic to passively track and monitor their employees. Another area where the delicate balance between privacy and necessity worried employees was the interim health data collection (like vaccination proof, medical records, household surveys, status updates, etc.) carried out to ensure a safe return to office.

Workers want their employers to be transparent and upfront with their data practices

Employee data collection is not new. Employers have been long studying workplace patterns, engagement survey

responses, and team dynamics to foster a productive work environment. Employees are usually willing to work together with their employer on this, provided the data gathered directly serves an internal business goal as well as the latter informs beforehand about what the data will be used for, how it will be stored, and who will have access to it. The same goes with employee monitoring. A 2018 Gartner study reported that more than 50% of the respondents were comfortable with monitoring on grounds of valid reasons from the employer.

To put things in perspective, employees willingly trust employers to keep their data safe and use it responsibly. But this trust is broken when employers keep employees in the dark about what purpose their data serves or cross a line with tracking by going to lengths like uninformed surveillance or camera monitoring. The moment employees feel their employer is invading their privacy, it will reflect in the organisation's attrition rate.

Shaky legal ground

Businesses may also be placing themselves on shaky legal ground when it comes to employee privacy. In terms of the Protection of Personal Information Act (PoPIA), employers have to make employees aware that their productivity and performance is being monitored and should provide reasons for doing so. The Regulation of Interception of Communications and Provision of Communication-Related Information Act (Rica), meanwhile, restricts the interception of communication except under very specific circumstances.

Rather than trying to evade these legal minefields, employers should look to build trust between themselves and employees, and build a safe and compliant environment where privacy is assured.

Commitment from the top

Ultimately, employee privacy is as much a leadership prerogative as anything else. It requires organisational commitment on an ongoing basis. Employee data, like customer data, is of critical importance and warrants the same level of protective measures like robust encryption both at rest and in transit, clear data handling statements, and informed consent. In the case of third-party services, the safe choice for businesses is to work with vendors who espouse an ethical approach to data privacy protection, are compliant with local regulations, and would never monetize data.

When privacy is assured, the trust relationship grows stronger. You build more loyal employees who are willing to go the extra mile for customers, ultimately resulting in a positive impact on your bottom line. As such, employee privacy shouldn’t be treated as a feature but as a non-negotiable given.

ABOUT THE AUTHOR

Andrew Bourne, Regional Manager - MEA, Zoho Corporation