REPLICON™ The Time Intelligence™ Company

Monitoring of Employees - A Global Regulatory Perspective

Written & Compiled by

Shreya Bhattacharya

REPLICON™ The Time Intelligence™ Company

Table of Content

Introduction

Employee monitoring is a growing practice in which organizations use digital tools to track work, employee performance, and work in progress. Workplaces use different monitoring methods to measure productivity, track attendance, assess behaviour, ensure security, and collect evidence pertaining to hours worked by the employees.

The standard monitoring technologies concentrate on monitoring computer, email, and telephone use, to help establish when employees are actively working and when they are not. Some employers use software that can examine the network, internet, and email usage of a sizable group of employee users, including recording the duration of time the users are idle, the rate of internet surfing, and the amount of incoming and outgoing emails and phone calls.

Types of Employee Monitoring

Employee monitoring is a method of using different types of surveillance devices to gather and analyse data about employee productivity, performance, web and app activity, etc. Below are the most common forms of employee monitoring used by employers -

1. **Video Surveillance** - Video Surveillance is used mostly by employers in order to prevent theft, violence or sabotage. There is a very small ratio of businesses which use video surveillance to monitor employees.
2. **Key Cards** - The software behind the key card chips gives the data regarding the whereabouts of employees in the workplaces and what time the employee came to work.
3. **Web & App Activity Monitoring** - Web and app activity monitoring programs are used to guarantee the safety and proper usage of company computers and mobile devices.
4. **Email Monitoring** - Emails sent or received through a corporation email account are usually not deemed private. Organizations use email hosting services like G Suite, and usually, they have admin access that allows emails to be monitored.
5. **Wiretapping** - Wiretapping can be used to record employees' phone call details and conversations. These can be recorded during monitoring.
6. **Geo-Tracking & Geofencing** - This is one of the most common methods of employee monitoring used by employers to track employees moving from one place to another during their work hours.

Geofencing and Geo-tracking

"Geofencing" and "Geo-tracking" are to some extent recent terms that have surfaced to illustrate various GPS monitoring methods. A geofence is a virtual border created by a software platform using GPS or other means to define a geographical area. When employers

use geofencing technology, they are notified when an employee enters or exits a particular geographical boundary set by the employer.

Geofencing lets an employer monitor more than just the clock-in/clock-out process. It gives the employer the ability to track and monitor their employees' location in real time, based on their GPS location and requires them to do a set of safety checks. Many employers use this technology in order to keep the labor cost low by tracking time worked by employees and the employee's attendance remotely. Companies that have employees in the field or on client appointments need a more effective way to keep track of their employee's time.

Benefits of Geo-Tracking Employees

1. Visibility to management regarding an employee's compliance with company policies
2. Capability to monitor illegal access to business property
3. Location tracing delivers real-time incident management
4. Employees are more motivated to conform with policies

Risks of Geo-Tracking Employees

1. Employees' loss of privacy
2. Employers can be subject to lawsuits if they fail to follow the privacy laws
3. Heightened risk for third parties to obtain sensitive personal information of employees and even companies.
4. Divulging private information of the company.

Geofencing and geo-tracking is utilized by employers in multiple ways. Basically, this technology can deliver businesses an efficient way to monitor their employees, improve time reporting and save money. The data recorded by the tracking system can be used to hold both employers and employees responsible for meeting their obligations. This allows the employer to prevent having to depend on self-reported hours and to avoid manually entering hours into the employer's timekeeping system.

A GPS (Global Positioning System) tracking system or geo-tracking system or simply a tracker is *a routing mechanism used in order to establish movement and geographic position for tracking location on a vehicle, property or person*. The use of GPS was started by the U.S. Department of Defence in 1973. GPS was installed in the first model spaceship released in 1978 and eventually added to the full collection of 24 functioning satellites in 1993. Employee monitoring is not a new phenomenon in private organizations. Henry Ford, the American industrialist did it way back in 1913, even though it was a little bit intrusive for today's standards.

GPS technologies can be especially helpful for employers in the construction industry. Many companies now offer services that allow employers to set geofencing limits, such as generating a geofence around construction and worksites. Using this type of technology, employers in the construction business have means to better handle their payroll and timekeeping, since the software system will log when an employee is on-site or off-site by electronic means.

Industries for courier and delivery services, logistics, constructions, public transportation, takeaway services use the mode of tracking employees via GPS technology. HVAC, cable, or electrical companies provide their employees with vehicles that they use to communicate to job locations. With the use of GPS on the vehicles, managers can track and monitor the vehicle's position, making sure that employees are staying on task and aren't using the vehicle for personal errands.

As the technology grew, employers across the globe began utilizing the tracking technology to monitor employees. With the upsurge in Global Positioning System (GPS) technology, employers have extraordinary access to their employees' location. For quite a few years, employers have been able to trace and track the movement of their field or mobile employees' locations through GPS devices in the vehicles. With newer technologies, employers can track locations through GPS apps in employees' smartphones and work devices. With the advancement of Satellite Navigation systems and therefore the increased utilization of smartphones, many businesses have adopted GPS tracking systems to also trace their employees to monitor work progress throughout the hours of service.

As discussed before, tracking employees' positions and movement through GPS can have many advantages for a company:

1. Monitoring overtime and compliance with labor laws.
2. Encouraging increased productivity through efficient travel for delivery.
3. Ensuring conformity with safety regulations by verifying that employees are not speeding or otherwise breaking traffic laws.
4. Validating the time stamp records and thereby verifying that company policies are observed & abided, and employees are engaging in safe conduct. Furthermore, if an employee is believed to have committed some unlawful activity, an employer can use GPS tracking as part of its internal inquiry.

Surely, there are noticeable benefits to using monitoring technology such as enhanced efficiency, ability to monitor hours and overtime, etc. But this also raises privacy and various legal concerns.

Employee Monitoring - Regulatory Landscape

As discussed above, in the past, time tracking has been used as the simplest way to measure work and calculate payments. At present, it is often used as a source of crucial data on how work is performed, what can be improved, and what trends of the work process require closer attention.

In many industries across the globe, time is tracked using a device that resembles a punch card system. This electronic device links to a computer program which processes and studies the data. Usually, the employee receives a card, chip, or wristband, through which the

employee registers with their name and ID number. Some systems need the employee to check in with the use of biometrics.

Many countries across the globe have specific regulations and requirements for employee monitoring. Below is a synopsis of certain regulatory practices for employee geo monitoring followed by individual countries.

Employee Monitoring in the United States

The United States monitoring laws give employers a vast array of rights to monitor their employees' movements on workplace devices. But this imposes certain restrictions on employers as any kind of monitoring must be corroborated by reasonable and valid justification. It is a very common business practice these days, among both public and private sector employers, to use software to track the employee location and activities.

Federal workplace privacy and employee monitoring laws for federal offices stem mainly from the Electronic Communications Privacy Act, 1986 [ECPA]. The ECPA permits federal employers to monitor all its employee verbal and written exchanges, provided that the employer can provide a reasonable and operational justification for it. It also allows for additional monitoring, if the employee gives consent.

Certain states in the United States regulate the use of GPS tracking devices among private sector employers, based on legislation and precedents.

California - The California Penal Code Section 637.7 restricts the installation of a GPS tracking device that decides the position or movement of an employee.

The California Penal Code states that no person or business in California shall use electronic tracking devices in order to track the location or movement of a person. However, this is not applicable to registered owners, lessors or lessees of a vehicle who have given their consent to use such tracking devices on their vehicle. Here, Electronic Tracking Device means any device connected to a vehicle or other portable thing that uncovers its location or movement and gives out electronic signals.

Employees should not have expectations of privacy when using company-owned vehicles or communication devices during business hours or for work reasons. However, whether GPS monitoring of such vehicles or other devices establishes an abuse of privacy requires considering various factors, including whether the employee uses that company-owned vehicle or other devices regularly, keeps it at his or her house during non-work hours, or uses it for personal reasons during non-work hours, among other things.

Recently, a new law **California Consumer Privacy Act ("CCPA")** was passed on January 1, 2020, which states that employers must take into consideration the disclosure requirements and potential liability that come with GPS tracking of employees moving forward. The CCPA gives California residents certain privileges and rights when it comes to privacy and monitoring. It does not differentiate between residents in their roles as consumers or employees and also gives substantial new data privacy access, disclosure, and deletion rights.

Thus, employees have the same rights as any consumer to request the concerned company (in this case, their employer) reveal how their personal information is being stored and used, and also to gain access to and/or deletion of that information.

As the GPS tracking data of employees which are collected, falls under the wide-ranging definition of "personal information" used in the CCPA, employers will be obliged to agreeably disclose such collection methods at or before the point of collection, provide employees with a copy of the data upon demand, and delete that data except for what is necessary to be maintained for a business purpose.

New York - In New York, there is a Senate Bill S4586A currently in the process of being passed which states that private employers who engage in monitoring which includes monitoring or otherwise intercepting telephone conversations or transmissions, electronic mail or transmission, or internet usage of or by the employee, by any electronic device or system, to give prior notice to employees in writing or via an electronic record or form.

Minnesota - Minnesota's statute forbids the use of a mobile tracking device without a court order.

Connecticut - Employers can use GPS tracking in company-owned vehicles without the employee's knowledge, but the employer must post a notice if they track employees on the company's premises.

Furthermore, in **Delaware**, employers are required to inform employees of monitoring emails. Additionally, **Colorado** and **Tennessee** have laws that require companies to set email monitoring policies.

Here are some of the US Court Rulings that have discussed and set guidelines for GPS tracking of employees -

Elgin v. Coca-Cola Bottling Co

The employer connected a GPS device to a company-owned vehicle to examine doubts of theft. The employee was exonerated of any misconduct but filed a state-law interference claim. A Missouri federal court overruled the claim, noting the employer owned the vehicle and the only information uncovered was the location of the vehicle.

Cunningham v. New York Department of Labor

The employer had a GPS device installed on the private vehicle of a state employee, who was allegedly committing misconduct, to collect information on his location. The employee was ultimately fired. The employee then filed a litigation case, alleging that the GPS device infringed his right to privacy. A New York court held that the connection of the GPS device to the employee's personal vehicle was an unwarranted search and contrary to statutory principles. The search was excessive in its scope, the court said, because the employee's personal vehicle was observed & monitored 24 hours a day, 7 days a week, and the GPS was not disconnected prior to the employee taking a holiday.

City of Ontario v. Quon

In 2010 the United States Supreme Court issued its opinion siding with the City and its officials in a workplace electronic monitoring case closely followed by employers and their counsel. The Court reversed the Ninth Circuit Court of Appeals' opinion, holding that the government employer's search of a police officer's personal and work-related text messages on an employer-issued pager was reasonable, and therefore the officer's Fourth Amendment rights were not violated.

The United States' legal system tries to balance out the necessity of workplace privacy and employee monitoring. That said, transparency and flexibility are always good practices.

Employee Monitoring in Canada

Canadian laws about privacy within the workplace clearly states that, employers should at all circumstances inform employees what is the type of personal data is going to be collected, used, and disclosed.

The Canada Privacy Act protects the privacy of individuals with respect to personal information about themselves held by a government institution (for example: banks). It also provides individuals with a right of access to that particular information. The Privacy Act has certain regulations which may apply to workplace monitoring, depending on the jurisdiction (federal or provincial/territorial), sector (public or private), the type of data being collected (health or other personal information), and whether the workplace is unionized or not.

In Canada, privacy and monitoring related regulations are governed mostly by the common & provincial civil law practices and by employment contracts and collective agreements.

The federal jurisdiction & several provinces including British Columbia, Alberta, and Quebec have provincial privacy legislation that regulates the safety of personal information in the context of employment.

In Ontario, there is no particular provincial privacy legislation governing the protection of employee personal information. The Ontario Court of Appeal in 2016, acknowledged a tort of privacy invasion called "intrusion upon seclusion." which may enforce requirements on employers similar to those found in other jurisdictions. With no specific legislation on the issue in Ontario, the driving principles emerging from the federal *Personal Information Protection and Electronic Documents Act,* are usually followed by employers in order to reduce risk and liability in this area.

Ontario is currently considering proposals that would implement a fundamental right to privacy for Ontarians, introduce more safeguards for artificial intelligence (AI) technologies, introduce dedicated protections for children, update consent rules to reflect the modern data economy, promote responsible innovation and correct the systemic power imbalances that have emerged between individuals and organizations that collect and use their data.

At present, Quebec is the only jurisdiction to enact a law that specifically addresses biometrics. Quebec's Act to establish a legal framework for information technology requires

organizations to notify the Commission d'accès à l'information before implementing a biometrics database. The regulator may then prohibit such a database from coming into service, order changes to the project, or order the destruction of the database.

The Saskatchewan Court of Appeal has also held that data 'tending to divulge personal details of the lifestyle and personal choices of the individual falls within the definition of intrusion of privacy (R. v. Trapp, 2011 SKCA 143). A work computer or mobile phone that an employee uses for minor personal use may well include such information.

Notably, however, the Supreme Court of Canada time and again, has in various cases observed that "*it is difficult to imagine a more intrusive invasion of privacy than the search of one's home and personal computer.*"

Thus, even if Canadian employers have some leeway in using technology to keep tabs on employees in certain circumstances, national and provincial privacy laws set limits and control mechanisms on how they may go about it.

Employee Monitoring in the EU

European Union does not have specific regulations related with employee monitoring, but the General Data Protection Regulation (GDPR) covers the various aspects relating to employee data protection and use of personal data for the purpose of employee monitoring.

GDPR (General Data Protection Regulation) laws came into effect in the EU on May 25, 2018. The GDPR seeks to make sure that organizations remain responsible and protect the personal information they collect and process for business purposes.

It highlights the following:

- Notifying the employees about the data collection procedures.
- Ensuring that employees have given their consent for personal data collection.
- Protecting all the data collected.

GDPR Article 88 allows EU member states to implement more detailed rules on employee data processing. GDPR gives the main reasoning for managing employee data for monitoring purposes. The law authorizes employers to collect, process, and use employee personal data for employment-related purposes where & when it is needed.

Any monitoring software will process personal data and depending on the software the employer is proposing to use, may pick up data beyond that required to monitor performance, such as medical information, personal emails, or bank details if the employee uses the computer to check their online banking during their lunch break, for example.

Hence, employers who introduce monitoring software are required to make sure whether it is necessary or justified, and where monitoring is introduced, ensure it is done so transparently and in accordance with data protection legislation.

GDPR needs data subjects (in this case - employees) to give their permission before the monitoring commences. However, employers are also able to track employees based on valid interest if they perform a legitimate interest assessment and have warranted reasons to process data without approval.

GDPR also expects employers to execute a Privacy Impact Assessment before executing the software, in order to ascertain needs and disputes that could occur once the corporate computer monitoring software is installed.

In France, the employer must abide by a three-step process in order to monitor its employees with devices. First, the employer must confer with the Health, Hygiene and Safety Committee, the staff representatives, and the Works Council prior to executing any sort of geo-localisation device. Then the employer should file a declaration to the data protection authority. Lastly, the employer must notify the employee about the installation of such devices, the data that will be collected and ask for his/her permission.

Employee Monitoring in Germany

Germany passed the new Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG) which substituted the previous BDSG on May 25, 2018. The new law correlates the German data protection regime with the GDPR. The new BDSG varies some of the GDPR's requirements. The requirements for managing employee personal data and employee monitoring are extensively covered under the new BDSG. According to the law, employers' monitoring activities must abide by the requirements of both the GDPR and the new BDSG, unless another law applies to the specific circumstances.

The BDSG does not expressly permit or prohibit employers from monitoring certain types of employee activities. However, employers should steer clear of monitoring locations where employees have a reasonable anticipation of privacy. Employers must assess and rationalize employee monitoring on a case-by-case basis to ensure compliance with the GDPR, the BDSG and other laws.

If the employer fails to adhere to the legal limitations on employee monitoring, the monitoring is a violation of the data protection law and employers may be prohibited from using material from the unlawful monitoring.

The Federal Labor Court in Germany (Decision 2 AZR 681/16) stated that information attained through usage of key logging to monitor an employee's usage of the company's internet access and IT systems could not be used to fire an employee for extreme use of the employer's systems during working time because use of the key logger was unfounded. In particular, based only on the key log monitoring, employers investigating an employee would be considered groundless surveillance.

Employee Monitoring in the UK

Even though employee monitoring is legal in the UK, employers should not make an attempt to look into employees' data without reasonable and proper justifications. In fact, there are

laws in the UK that steer the method of monitoring employees in the workplace. These consist of, but are not restricted to, the Data Protection Act (DPA) 2018 and the Employment Practices Data Protection Code (EPDPC) 2011.

Employers have the right to make sure that computers in the workplace are utilized properly and not inappropriately. However, prior to implementing the monitoring, employers must first discuss this with their employees and explain the monitoring. The reasons must be valid and in line with the business objectives. Employers are also expected to establish written guidelines on the usage of work on computers by employees, and employees should sign these policies accordingly.

In the UK, employers are permitted to monitor email content as long as it is on a company-given device, and there is a legitimate business reason behind it.

Employee Monitoring in Russia

Employee monitoring is permitted in Russia. *Art. 22 of the Labor Code* of the Russian Federation necessitates the employer to give all the instruments required for employees to perform their work duties, and the employer has the right to check work performance on these devices. All parties engaged in the monitoring activity must be sufficiently notified of the monitoring and justification in order to conduct employee monitoring.

Privacy laws in Russia are a rapidly developing branch in Russian legislation. The Federal Law in Russia on Personal Data (No. 152-FZ), executed on July 27, 2006, signifies the backbone of Russian privacy laws and requires data operators to take "all the necessary organizational and technical measures required for protecting personal data against unlawful or accidental access". Privacy law also requires that "personal data made publicly available" needs to receive consent from the data subject, i.e., the employee.

In the contemporary workplace, computers are labour instruments. Therefore, if the employer gives the computer to the employee, they have the right to control the use. However, the law entails an employer who monitors employees to build an ambiance of transparency. The monitoring procedure has to be incorporated in the employment contract and policies. One of the purposes of employee monitoring should be to track the period of working hours, and no personal data should be gathered to avoid legal disputes.

Employee Monitoring in Brazil

The Brazilian Congress has passed a comprehensive general data protection law (Law No. 13,709/2018 – the LGPD), which is meant to substantially alter the data protection system in Brazil. The LGPD is inspired by the European data protection framework, particularly the General Data Protection Regulation (GDPR).

The LGPD establishes comprehensive rules for the collection, use, processing and storage of personal data and which affects all sectors of the economy, including the relationship between customers and suppliers of products and services, employees and employers, transnational

and national commercial relations, as well as other relations in which personal data is collected in the digital environment or outside the digital environment.

With regards to monitoring and observation of individuals, labour precedents establish some rules on the monitoring of employees. Generally, Brazilian court decisions maintain that the monitoring of computer systems which are provided to employees by their employers is permitted. Therefore, IT resources made available for the exercise of the employees' functions may be subject to scrutiny. The surveillance of employees' personal devices may be probable (for example, in the event a professional email account is installed in the employee's cell phone or computer) to the extent that it concentrates only on the company's information. Employees' personal email shall not be monitored or accessed by the employer, and employees shall be informed in advance by their employer about all monitoring activities done.

Employee Monitoring in Australia

Under the *Australian Workplace Surveillance Act,* an employer can monitor employees in the office, if an official notice and monitoring policy is in place. There are also exemptions where employees can be monitored without being informed. To do so, employers are required to attain a "covert surveillance authority," which has clearly been issued by the Magistrate court. Employers have the permission to scrutinize screen activities and keystrokes on company-owned computers, but on the condition that employees get a notification before the monitoring and intent of the monitoring Additionally, employees must be informed they will be monitored in no less than 14 days prior to setting up monitoring/activation. Hence, employers in Australia are in most cases, allowed to set up computer software to monitor activity on the computers they give official purpose.

Employee Monitoring in India

Data protection in India is presently governed by the Information Technology (Reasonable security practices and procedures and confidential personal data or information) Rules, 2011 ("Data Protection Rules') notified under the Information Technology Act, 2000 ("IT Act"). The Data Protection Rules levy certain obligations and compliance requirements on establishments that collect, process, store and transfer personal data or information of individuals such as obtaining consent, publication of privacy policy, answering to requests from individuals, disclosure and transfer limitations.

Hence as per the the labour laws of India, the employer has the right to monitor employee activities, systems, premises, company emails, SIM cards, headsets, and computers. The core for the monitoring is protecting the company's classified and trademarked information. In order to notify employees, the organization can set up regulations which would explain such activities. If the monitoring goes outside company premises or is found to be a violation of employees' right to privacy, the corporation might have to justify monitoring.

Inspired by the GDPR, the PDP (Personal Data Protection) Bill was proposed in 2019 to get a meticulous & thorough makeover to India's current data protection system, which is currently regulated by the Information Technology Act, 2000 and the rules thereunder. The current draft

of the PDP Bill specifies compliance requirements for all forms of personal data, expands the rights given to individuals, establishes a central data protection regulator, as well as sets up data localization requirements for certain forms of sensitive data. Provisions in the PDP Bill apply specific focus to privacy and data transfer of foreign organizations operating in India. It also has provisions to enforce hefty financial penalties in case of non-compliance.

Employee Monitoring in China

In recent years, laws related to network security and data security have gradually increased, including the Cybersecurity Law of the People's Republic of China, 2017 which sets out the ideologies and procedures for the collection and use of personal information, the accountabilities of the operators of the network, etc. According to the Comprehensive Definition of personal information under the Cybersecurity Law, the scope of protection of employee's data includes employers collecting, storing, transmitting, processing and generating personal information from employees' social media, computers and mobile networks.

Effective November 1, 2021, China will enact a full finalized text of the Personal Information Protection Law (PIPL), the first such law ever to be passed in the country. The PIPL has taken some concepts from the GDPR laws in the EU with regards to privacy laws. Under the law, individuals shall have the right to inquire about what personal data is being collected and stored by the data processor. Employees require data processors to obtain consent before they can share the personal data with a third party. PIPL's auditing requirements allow companies to flexibly construct their self-monitoring systems to avoid leak of personal information.

In accordance with the labor contract law in China, employers must have a written policy which governs telephone monitoring. Employers usually monitor employees' mail, telephone, CCTV pointed at the computer monitor or other information systems. Since employees often store or transmit personal information in the enterprise system, it is advisable for the employers to establish rules and regulations on the monitoring system. Organizations must also expressly inform employees of the company's monitoring measures and forms of monitoring of the company's equipment, mail, systems, etc. Such rules and regulations or other documents must be confirmed in writing by employees explicitly stating that the company can obtain all the information.

Employee Monitoring in UAE

According to Articles 9 and 10 of the DIFC Data Protection Law 2007, if an employer wants to bring a monitoring policy in their business, they need to verify with the employees beforehand. Particularly when employees are utilizing their private devices for work, it may include personal data, which they do not want to disclose. Also, according to the Federal Laws, specifically the Cybercrimes Law, Telecommunications Law, and the Penal Code, it is not permissible to record phone conversations without the consent of the concerned parties.

The federal law of UAE has stringent rules to protect the privacy of employees' personal and confidential data. If an employer is monitoring their employees, the employer should make sure not to hinder or harm the privacy of employees in the workspace.

Pros and Cons of Monitoring

In order to monitor employees at work, the basic requirement is to keep in mind that there is a fine balance between employee privacy concerns and genuine business interests. Firstly, employers who have or are contemplating using a monitoring technology should be aware of employee privacy concerns and applicable regulations around it. Monitoring employees beyond the workplace can be especially invasive because it can encroach into an employee's private life. For example, GPS tracking of a company car may give information about the employee's location or activities after work hours.

Employee tracking systems can also present openings for misuse by other employees. Further, monitoring can potentially lead to hurting employee morale. Employee tracking may also be an issue in class or collective actions.

Having said this, there are many advantages of a meticulously created employee monitoring system. In the era of COVID-19, employee monitoring can be used to make sure that employees are following the company's instructions concerning social distancing. It could also be applied to establish who an infected employee met for in order to notify and to make decisions regarding a partial facility shutdown intended to stop the spread of the infection. GPS tracking of employees may help detect when a traveling employee has been in a mishap. Monitoring can help safeguard against or investigate charges of employee misconduct. Tracking also can be used to increase employee efficiency by emphasizing the need for training or making sure the proper use of employer resources. Employee monitoring may be used to ensure that unlawful individuals do not access secure areas. Workplace surveillance can also discourage employee theft, violence, and other prohibited behaviours.

Best Practices in Workplace Monitoring

Below are best practices for all employers seeking to implement monitoring in their workplace to avoid misuse of the monitoring technology:

1. **Establish reasonable grounds -** Privacy laws are built on a standard of practicality, with regard given to the nature of the monitoring and the anticipation of privacy in the situations. Before initiating any monitoring activity, employers should be concerned about what their justification is for participating in the monitoring and whether that rationale defends the type of monitoring that will take place.

   Using monitoring as a measure of performance and productivity of employees is typically harder to justify but may be considered reasonable in the conditions

depending on the nature of the monitoring being used. The more 'invasive' the monitoring, the greater the employer's rationale should be for using it.

2. **Disclose the monitoring activity** - It is a good exercise for employers to divulge monitoring activity to employees and others who may be concerned, even though that disclosure may not be strictly required in all situations. Employers should include a statement of the purposes for which the information is being collected or used.
3. **Create a policy** - Many employers prefer to execute clear procedures that define their practices concerning the collection, use, and disclosure of employee information. Even though the enforceability of such policies will depend on a number of aspects (comprising of the extent to which the policy is steadily applied, the employees' awareness of the policy, and the compliance of the policy with any relevant laws), it is a good practice for employers to set out expectations in advance, before a dispute or complaint arises.
4. **Obtain consent** - Employers looking to implement monitoring should be concerned about obtaining consent, if possible, in writing, for the collection of the information. Attaining consent will not ensure the workplace monitoring conforms with all privacy laws, but it can be a key element in establishing whether the collection of information was 'reasonable' or not.
5. **Use of Verified System** - Employers using verified and certified employee monitoring software which strictly adheres to all aspects of privacy concerns and applicable regulations in order to track attendance, hours of work, overtime, leaves etc., can be extremely beneficial to both employers and employees.

Teleworking and Employee Monitoring

With the start of the 2020 coronavirus (COVID-19) pandemic, the number of businesses switching their workforce to remote work has increased. Even though organisations around the world have started to reopen, teleworking will likely remain prevalent in the workforce.

After analysing the performance of remote working during this period, it was discovered by employers across various organisations that various employees were operating at peak productivity and efficiency levels at very different times of the day. Monitoring technology can help employers analyse and keep a track on various patterns and shift work done by employees.

Some organizations are using the data they gather from monitoring not only to keep track of remote employees but also to help plan for an eventual return to the workplace. Time tracking is very significant not only for big but small companies too. Time tracking behaves as a window for the company to know the quantity of work the teams are offering. Employers can also use the data to check whether the entire team or individuals are going beyond their capacity and working.

Employees working remotely have become empowered, are experiencing less stress and saving money. Employers are saving on operational costs, reducing physical retail space, have more productive employees with higher work quality, and everyone benefits from reduced green-house gas emissions from fewer employees commuting back and forth from work.

Conclusion

Regardless of being a somewhat new technology, GPS monitoring systems such as geo-fencing and geo-tracking are being applied rapidly across a broad range of industries. A massive amount of value can be realized through the management of labor costs and monitoring for misconduct or other security matters.

Employers need to respect their employees' right to privacy while tracking them. Employers need to have a defined process in place notifying their employees that their electronic device has a GPS tracking app fitted that will monitor their location. Employees should be mindful of and understand all the abilities of the tracking app, including time-clocking, mileage tracking, driving routes, etc.

Even though there are benefits of geo-monitoring for employers, these types of methods raise privacy concerns for employees. If an employer can track the location of its employees via their mobile devices, then the employer may ideally also have access to a wide array of information that is collected on the employees' mobile devices. In theory, the employer may have access to collections of information concerning its employees' whereabouts outside of working time, from the shops in which the employees buy stock, which doctors they visit and when, and even their sleep habits, social media usage, and other personal information.

Thus, there are always concerns about the privacy of the individual and regarding personal information which might end up in the hands of a third party.

Employees may be opposed to, and may even challenge, such monitoring due to privacy concerns. Even if the employer is able to defend these challenges effectively, the legal, and collective bargaining disputes can be expensive and drawn-out and can adversely affect not only employee confidence but also public affairs. Employers opting to execute a GPS monitoring policy should contemplate whether they can accomplish their objectives with less intrusive monitoring, such as geofencing, as opposed to more comprehensive GPS tracking. Irrespective of how employers opt to use this technology, interaction and transparency are vital to ensure privacy limits are respected and the technology is only being used in a purely work-related function.

While there are overlaps between monitoring and surveillance practices, the distinction between them suggests that greater ethical and privacy concerns arise from employee surveillance. It is important for an employer to keep the privacy of employees in check while monitoring an employee's location and whereabouts.

Majority of the countries across the globe, are now coming up with well-articulated, clear and stricter laws for monitoring employees, which will enable companies to flexibly construct their monitoring systems to avoid privacy issues and enhance work performance.