7 Best Privacy Practices for Employers When Using Geolocation Tools to Track Workers

Insights
1.08.25

Many employers have turned to geolocation tools like GPS devices to monitor employees' whereabouts and movements – especially those working remotely or in field-based roles. While these tools provide an effective way to boost operational efficiency, improve safety, and optimize resources, you must ensure you respect workers' privacy rights when deploying them. This Insight will explore the privacy obligations that come with monitoring your employees via geolocation tools and provide the seven best practices to guide your actions. You can also read about general employment guidance related to the use of wearable tech by clicking here.

1 OFFER INFORMED CONSENT

A cornerstone of privacy law is the requirement for informed consent. You must make your employees fully aware of the geolocation monitoring system and how it will be used.

2 LIMIT YOUR PURPOSE

Ensure that geolocation tracking is conducted for legitimate business purposes.

3 CONSIDER PROPORTIONALITY AND MINIMIZATION

Geolocation monitoring must be proportionate to the goals it seeks to achieve – and ideally should minimize data collection.

4 PROTECT DATA AND PROVIDE NECESSARY SECURITY

You have a legal obligation to protect any personal data collected through geolocation tools.

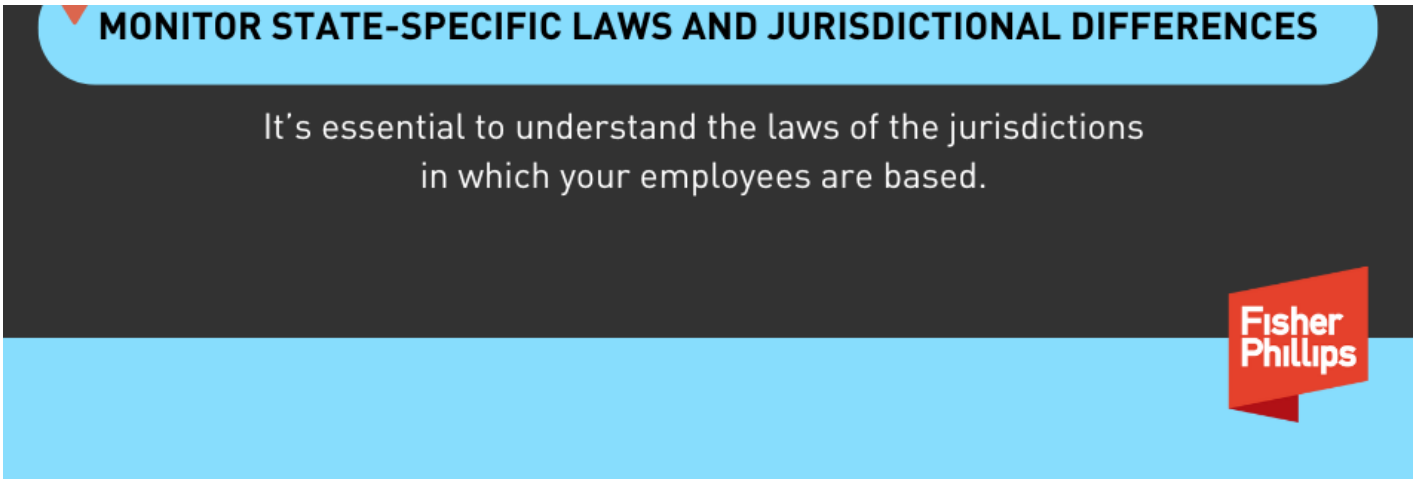
5 PROVIDE TRANSPARENCY AND DOCUMENTATION

Make sure to maintain transparency about your geolocation monitoring practices.

6 PRESERVE EMPLOYEE RIGHTS AND PROTECTIONS

In addition to data protection laws, employees have specific rights when it comes to monitoring.

7



1. Offer Informed Consent

A cornerstone of privacy law is the requirement for informed consent. You must make your employees fully aware of the geolocation monitoring system and how it will be used. This includes:

- **Clear Communication**: Explicitly inform your employees that they will be monitored using geolocation tools, specifying the scope, purpose, and duration of the monitoring. This communication should ideally occur at the beginning of the employment relationship or before implementing geolocation tracking.
- **Voluntary Consent**: While employees may be required to consent to geolocation tracking as a condition of their employment, it must be done in a transparent and voluntary manner. Coercion or the failure to fully disclose the nature of the tracking could mean there was no informed consent.

2. Limit Your Purpose

Ensure that geolocation tracking is conducted for legitimate business purposes. In many cases, this involves monitoring employees in roles that require travel, delivery, or site visits. Don't use geolocation tracking for personal reasons or to monitor employees' non-work activities. Legitimate business purposes can include, for example, protecting company property or customer property, ensuring there is no timecard fraud, checking whether employees are actually taking required meal or rest breaks (in some states), managing employee performance and efficiency, and optimizing travel or delivery routes.

Various states require consent if you monitor vehicles used for employment purposes. They vary from state to state and sometimes depend on such factors as whether the vehicle is company-owned or privately owned. Under many state laws, for example, employee tracking must be limited to specific and transparent purposes, such as ensuring productivity, protecting safety, or ensuring that business resources are being used efficiently. That said, while limiting the purposes for which geolocation data is used, your disclosure should comprehensively identify all the purposes for which you may use this day. Using geolocation data for purposes beyond the scope of the initial consent

may violate anti-stalking laws.

3. Consider Proportionality and Minimization

Geolocation monitoring must be proportionate to the goals it seeks to achieve – and ideally should minimize data collection.

- This means that you should only collect data that is necessary for the intended purpose, and the tracking should not be overly invasive. For example, monitoring an employee's movement outside of working hours may be viewed as excessive and a violation of their right to privacy.
- The Federal Trade Commission (FTC) has made it clear through various enforcement actions that it considers geolocation data to be sensitive location data. The agency emphasizes that employers should use geolocation monitoring tools in a manner that minimizes data collection and is not unduly burdensome on employees' privacy. Similar data minimization requirements exist under the California Consumer Privacy Act (CCPA).

4. Protect Data and Provide Necessary Security

You have a legal obligation to protect any personal data collected through geolocation tools. This includes:

- **Data Security**: You must securely store geolocation data, like any other personal information. You must also protect it from unauthorized access, alteration, or loss. Make sure to implement robust cybersecurity measures to ensure the data's integrity. This includes proper due diligence over the security measures of vendors you engage to collect, process, or store this data.
- **Retention Period**: Define and adhere to clear data retention policies. Geolocation data should only be stored for as long as necessary to fulfill its purpose. You should securely delete or anonymize the data when no longer needed.

5. Provide Transparency and Documentation

Make sure to maintain transparency about your geolocation monitoring practices. You should provide employees with clear documentation that explains:

- How geolocation data is collected, through which devices and applications
- What data is being tracked and for what purposes
- How long the data will be stored
- How the data will be used
- Who will have access to the data

You should also make employees aware of their rights regarding access to their data. For example, California privacy law requires that covered businesses provide employees with a privacy notice that

explains, among other requirements, data collection practices and retention policies. This is a best practice even if not required by applicable laws.

6. Preserve Employee Rights and Protections

In addition to data protection laws, employees have specific rights when it comes to monitoring. These rights vary by jurisdiction but generally include a right to privacy, particularly during non-work hours. You should avoid monitoring during personal time or in areas where employees would reasonably expect privacy (e.g., restrooms).

In California, the CCPA grants employees the "right to access" and the "right to correct," allowing them to obtain copies of the data held about them and request any inaccuracies be corrected. The CCPA requires employers to provide information to employees about their rights in a privacy notice.

7. Monitor State-Specific Laws and Jurisdictional Differences

It's essential to understand the laws of the jurisdictions in which your employees are based. For example, several states, including California, require that employers inform employees if they are being monitored electronically. In some cases, states allow geolocation tracking of company owned vehicles, but for personally owned vehicles written consent is required.

You should also be mindful of international differences. For instance, European data protection laws, such as the GDPR have stringent privacy regulations that may differ from those in the U.S. or other parts of the world.

Conclusion

Fisher Phillips will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. You can also visit FP's U.S. Consumer Privacy Hub for additional resources to help you navigate this area. If you have questions, please contact your Fisher Phillips attorney, the author of this Insight, or any member of our Privacy and Cyber team.

Related People

Kate Dedenbach, CIPP/US
Of Counsel
248.901.0301
Email

Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Service Focus

Privacy and Cyber

Consumer Privacy Team

Data Protection and Cybersecurity