Monitoring employees is one way to ensure a productive and secure workflow within an organization. However, not all employees like being watched. Some even challenge the ethics and legality of workplace surveillance.

In this article, we explore the nature of workplace surveillance and consider the laws US employers should know and follow if they want to monitor their employees. We also look closely at an important part of workplace surveillance — employee monitoring — and provide you with six employee monitoring recommendations.
WORKPLACE SURVEILLANCE: DEFINITION, RISKS, LAWS, AND REGULATIONS

Workplace surveillance is a set of methods and practices for monitoring employees and workplaces. Employers apply them to:

- secure office assets
- protect sensitive and corporate information
- track employee productivity
- ensure a secure and safe workplace
- comply with industry regulations

Employee monitoring is broadly legal within the US but can be regulated differently within each state. Employers have the right to monitor employees’ digital activity, as the majority of companies provide employees with corporate devices and computer systems. In some states, however, employers have similar rights to monitoring even if employees use their own devices.

Apart from monitoring employees’ work-related communication, in some cases, employers can monitor their personal messages as well. This may be the case when messages are written during working hours and from a device that is the property of the organization.

These are the primary documents you should be familiar with that regulate workplace surveillance and digital privacy for US companies:

- Electronic Communications Privacy Act (ECPA)
- Stored Communications Act (SCA)
- Section 7 of the National Labor Relations Act
- General Data Protection Regulation, or GDPR (applies to US companies with employees and/or customers in the European Union)
Knowing the **legislation of the state your company operates in** is as crucial as knowing US federal laws. For instance, when talking about email or internet monitoring, you’re not obliged to notify your employees about it unless you operate in **Connecticut** or **Delaware**. At the same time, current laws in **Colorado** and **Tennessee** require employers to set written email monitoring policies.

Legal restrictions on workplace monitoring in several states like **Virginia** and **California** prohibit the use of electronic devices for recording or monitoring the activities of employees in areas designed for health or personal comfort.

**DISCLAIMER:** This White Paper should not substitute actual legal advice. Consult a lawyer to check whether laws to which you are subject permit employee monitoring. Learn what the applicable conditions and restrictions are before implementing employee monitoring practices into your workflow.

Apart from getting familiar with federal and state laws, you can find helpful information from trusted sources like the **Federal Bar Association**, the **American Bar Association**, and the **Workplace Fairness** non-profit organization.

**Risks of workplace surveillance** vary depending on the situation and may include:

- Fines and charges for legal violations
- Lawsuits from employees
- Reputational losses

**The legal consequences of improper workplace monitoring** depend on the type of violation and state legislation. For example, if an employer in West Virginia ignores the requirements of **521-3-20** of the West Virginia Code on the use of video and other electronic surveillance devices for the first time, the fine is $500. The penalty rises to $1,000 and $2,000 respectively for the second and third violations.
A violation of ECPA compliance can result in a $100 fine for each day of illegal monitoring or statutory damages of $10,000. The fines mentioned above were applicable as of
the date of publication. Make sure to do your own research and base your business decisions on the latest information.

MONITORING EMPLOYEES’ DIGITAL ACTIVITIES

There are many ways an organization can implement workplace surveillance. Employers often use video and audio surveillance within the office, record employees’ phone calls, track their GPS locations, and monitor their digital activity. In this article, we focus on digital employee monitoring as an essential part of modern workplace surveillance.

Types of workplace surveillance

Detailed tracking of employee performance requires more than just knowing how much time an employee spends sitting at the computer. Therefore, organizations deploy dedicated software to measure staff productivity and limit or restrict access to distractions, including entertaining websites and social media.

Another crucial reason for paying extra attention to electronic employee monitoring is data security. Employees may cause data breaches due to malicious intent or as victims of hackers. Digital monitoring aims to record user session activity, set response mechanisms to detect data misuse as fast as possible, and gather valuable information for investigating cybersecurity incidents.

When it comes to user monitoring, many employers want to know what their employees are doing during working hours and make sure they don't abuse their access to corporate data and systems. To see the full picture, it's usually enough to focus on the following categories of data:
What do employers need data about?

- **Data access.** It's essential to know who accessed sensitive resources and when in order to identify a threat in case of data leaks and make sure no one is overstepping their powers.
- **Keystrokes.** Recording keystrokes allows you to check that employees use work computers for business purposes only and make sure they don't share confidential information in messengers.
- **Idle time.** Monitoring time when an employee is away from a computer gives employers more insights on their actual performance and efficiency.
- **External devices and drivers.** Knowing which removable devices, such as flash drives, were connected to a computer can help with mitigating the risk of data leaks.
- **Visited URLs.** The history of employees' web browsers shows what websites and web applications they visit and what they're surfing for. Also, employers can check whether employees access suspicious resources.
- **Screen contents.** By gathering screenshots, video, and audio records of user sessions, it's possible to see everything the way it was on the screen. Such close monitoring significantly boosts employee efficiency, while the gathered information is priceless when investigating a cybersecurity incident.

Now let's move to the major legal recommendations you should follow to keep employee monitoring legal.
RECOMMENDATIONS TO KEEP EMPLOYEE MONITORING LEGAL

When adopting employee monitoring practices, businesses usually focus on metrics to track, security issues to mitigate, and tools to analyze workflow performance. However, the legal side of employee monitoring should also be taken seriously. Otherwise, you can end up paying fines for violating laws or insecurely storing private data.

Below, we provide six simple but essential tips that can help you keep your employee monitoring practices legal.

6 recommendations to keep employee monitoring legal

1. Know what to monitor

Be careful when choosing what types of digital employee activities to monitor and setting rules for your staff. For example, in some states, it's prohibited to request that employees verify their personal online accounts or to demand login information to personal accounts. Also, if your employees use personal devices for work purposes, consider ways to monitor without crossing the line into their private lives. For instance, you can make sure these devices aren't monitored during non-working hours.

2. Define who to keep an eye on

Employee monitoring can be selective. Regular users with no access to sensitive information can be monitored with minimum effort. On the other hand, all actions of privileged users have to be closely monitored and recorded to ensure the security of
critical data and comply with data security standards. You can also set incident response software to detect information compromise as soon as possible.

3. **Set clear written policies**

The best way to ensure an efficient workflow, legal compliance, and employees' understanding is to set clear policies and explain their importance to your staff. Make sure the following policies meet relevant security standards: [Electronic Communication Policy](#), [Bring Your Own Device Policy](#), and [Confidentiality and Non-Disclosure Policy](#). All employees should get familiar with your organization's policies on their first day at work and give their written consent to follow them.

4. **Notify your employees about monitoring**

Employee monitoring should be implemented legally and ethically. Although most state laws don't require you to notify your staff about digital monitoring, such a gesture will reduce stress among employees, as they'll know for sure what's monitored and what isn't. You can also explain the business reasons behind such monitoring so employees know your true motives.

5. **Use dedicated software**

Dedicated tools and solutions offer great help in organizing and executing user activity monitoring both legally and effectively. However, as the range of user monitoring solutions is rather broad, it's crucial to choose carefully.

When choosing a monitoring tool, learn about its functionality in detail to see if it covers your specific needs. Pay special attention to solutions that can track employees' performance, secure your company’s critical assets, and help your company stay compliant with industry regulations and local legislation.

6. **Deploy next-generation technologies**

Consider implementing tools that leverage innovative technologies such as artificial intelligence (AI) and machine learning. Advanced monitoring solutions apply AI-based user and entity behavior analytics (UEBA) to detect abnormal activity and respond to it in real time. If a malicious actor gains access to employee credentials and tries to
compromise critical data, UEBA software will immediately detect suspicious activity and block this user or send a warning message to the security officer or admin.

In any case, you have to constantly monitor updates to federal and local laws and revise your policies to keep your employee monitoring program legal. Also, it's always a good practice to **consult a lawyer** who can double-check your monitoring policies to make sure they comply with the law.

---

**LEGAL AND EFFICIENT EMPLOYEE MONITORING WITH EKRAN SYSTEM**

**Ekran System** is a universal user activity monitoring software platform that allows you to record actions of ordinary and privileged users as well as third parties.

**Monitor user activity** efficiently with a **helpful set of features** that include:

- **User session monitoring** to record employees’ sessions in video and audio formats, capture screenshots, and watch live users sessions. You can record user activity even if an employee is using multiple monitors

- **Web page and application monitoring** to provide you with more insights on which resources are accessed by employees during the day

- **Keystroke logging** to check whether employees are using corporate computers for personal purposes or sharing confidential information in messengers

- **Keyword-triggered monitoring** to start monitoring and taking screenshots only after detecting defined keywords entered by a user

- **USB monitoring and blocking functionality** to view information on mass storage devices connected to Windows systems and receive alert notifications

- **An AI-powered UEBA module** to create employee behavioral profiles, get early warnings about possible danger, and foresee insider threats

- **Offline monitoring** for continuous user monitoring in case the network connection goes down
You can use Ekran System to secure access to critical assets using multi-factor authentication, time-based user access restrictions, and secondary authentication to identify users of shared and built-in accounts.

Meanwhile, privileged access management from Ekran System helps you secure sensitive information and get full visibility of all privileged accounts. You can specify endpoints that can be accessed by certain privileged users, limit the time for which access is granted, and deliver temporary credentials.

Moreover, Ekran System functionality helps organizations meet various IT compliance requirements including those imposed by the GDPR, FISMA, NIST 800-53, SWIFT CSP, HIPAA, and PCI DSS.
CONCLUSION

Digital employee monitoring is a crucial part of modern workplace surveillance. Monitoring helps businesses track staff efficiency, secure sensitive information, and prevent cybersecurity incidents. However, when establishing practices for employee monitoring in the workplace, you must consider not only technical issues but also legal and ethical ones.

When implemented improperly, staff monitoring can cross boundaries into employees' personal lives and even lead to lawsuits and severe fines. This is why organizations should be familiar with federal and state legislation regarding workplace surveillance and keep them in mind when choosing dedicated user monitoring solutions.

With Ekran System, you can monitor and record user activity, get notified about suspicious events or processes, control access and privileges, respond to alerts in real time, and ensure compliance with legal and industry standards.