Private Eyes Are Watching You

U.S. and International Privacy Laws Relating to Employee Monitoring

Agenda

1. Overview
2. United States
3. Canada
4. Europe & UK
5. Latin America
6. Asia-Pacific
7. Employee Monitoring Scenarios
8. Global Principles and Best Practices

Overview

- Employee monitoring has become a core element of workplace management, particularly with the expansion of remote work. Employers track activities to ensure productivity, prevent data leaks, and maintain compliance.
- This session explores the intersection of privacy and monitoring laws across major jurisdictions.
- We will review U.S. federal and state laws, EU and UK frameworks, and international developments in Latin America, Canada, and the Asia-Pacific region.

Workplace Surveillance

- Monitoring tools include trackers, facial recognition, and AI-driven analytics that evaluate productivity or detect insider threats.
- Authorities worldwide are responding to concerns about data overreach, discrimination, and lack of transparency in monitoring technologies.
- Employers must align security and performance objectives with fairness, transparency, and proportionality standards.
- A well-designed monitoring program minimizes legal risk while maintaining employee confidence and compliance with evolving rules.

What Constitutes Employee Monitoring

- Electronic communications monitoring involves reviewing emails, chats, and calls to ensure policy compliance and mitigate risk, but may trigger wiretap or notice requirements.
- Video surveillance is used for safety, loss prevention, or productivity oversight, but raises questions of proportionality and necessity, especially in non-work areas.
- GPS and geolocation tracking enable oversight of vehicles or remote workers, though tracking outside work hours can raise privacy concerns.
- Biometric systems such as fingerprints or facial recognition support attendance and access control, triggering heightened privacy obligations such as explicit consent and strict retention rules.
- Activity tracking software captures screenshots and monitors application or browser usage to assess productivity and detect misuse, raising concerns about excessive or off-duty monitoring.

Emerging Technologies and Risks

- Artificial intelligence tools evaluate behavior patterns and performance, which can blur the line between legitimate oversight and intrusion.
- Behavioral analytics such as emotion recognition, typing rhythm, or facial expressions introduce new privacy and bias challenges.
- Remote and hybrid work extend monitoring into private spaces, raising employees' reasonable expectations of privacy at home.
- As the volume and sensitivity of collected data increase, multi-jurisdictional compliance and governance become significantly more complex.

United States

U.S. Federal Framework

- The United States lacks a single comprehensive privacy statute; employee monitoring is governed by a patchwork of federal and state laws that create complex compliance obligations.
- The Electronic Communications Privacy Act (ECPA) prohibits intercepting communications in transit (real-time monitoring) without a legitimate business purpose or employee consent.
- The Stored Communications Act restricts access to stored emails or messages after transmission, even when data resides on company-owned systems.
- For unionized workplaces, implementing new monitoring (e.g., video surveillance) may trigger a duty to bargain under the National Labor Relations Act.
- The Equal Employment Opportunity Commission (EEOC) requires that monitoring involving health or biometric data be job-related, consistent with business necessity, and not discriminatory
- **Practical tip:** Combine documented business justification with transparent employee notice to mitigate federal liability.

Electronic Communications Privacy Act (ECPA)

- Monitoring is generally permitted when a clear business justification exists, such as ensuring compliance, preventing data leakage, or investigating misconduct.
- Implied consent can be established through clear policy notices and handbooks that state employees have no expectation of privacy on company systems.
- There are limits: accessing personal communications or private devices without authorization can violate federal law and trigger liability.
- **Best practice:** pair written consent with transparent policies and narrow the scope of monitoring to specific legitimate purposes.

Federal Wiretap and Recording Laws

- Consent rules vary by state: some require all-party consent to record conversations while others permit one-party consent, necessitating adherence to the stricter standard for cross-state calls.
- Employers who access stored communications must confirm lawful authorization to avoid violations under federal and state law.
- Recording for compliance (for example, in regulated financial services) must still satisfy proportionality, security, and notice obligations.
- **Best practice:** provide upfront notice and obtain employee consent for recordings, especially in multi-jurisdictional operations.

State Laws Overview

- Beyond federal rules, states play an important role in defining the limits of workplace monitoring.
- Certain jurisdictions, including California, Connecticut, and New York, impose mandatory notice or consent obligations before implementing monitoring systems.
- Other states rely on general privacy and labor laws, allowing employers discretion provided they act transparently and proportionately.
- Companies operating across multiple states must reconcile inconsistent obligations, adopting the strictest applicable standard to minimize compliance risk.

California: Strong Employee Privacy Protections

- California Constitution explicitly recognizes a right to privacy, influencing workplace monitoring standards.
- The California Consumer Privacy Act (CCPA) and its amendment, the CPRA, grant employees rights to access, delete, and correct personal data collected by employers.
- Employers must provide notice before data collection, disclose categories of information gathered, and limit use to legitimate business purposes.
- Precise geolocation is considered sensitive personal information under the CPRA, requiring a notice at collection, limited use for business purposes, and compliance with employee privacy rights and retention rules.
- **Practical takeaway:** Implement clear data retention policies and avoid excessive or undercovered surveillance to prevent claims of constitutional violations.

New York and Connecticut: Notice and Consent Obligations

- New York's 2022 law requires private employers to provide written notice to employees before monitoring email, internet, or phone use.
- Employers must obtain acknowledgment from employees confirming awareness of such monitoring practices.
- Connecticut mandates prior written notice of electronic monitoring, with limited exceptions for investigations involving misconduct.
- **Compliance tip:** Centralize policy distribution and maintain acknowledgment records as evidence of informed consent.

Illinois: Biometric Information Privacy Act (BIPA)

- Illinois' BIPA imposes strict requirements for collecting or storing biometric data, such as fingerprints or facial scans.
- Employers must obtain written consent, disclose data retention schedules, and protect information using reasonable security measures.
- Violations can result in private lawsuits, with statutory damages per violation, leading to significant exposure for companies using biometric timekeeping systems.
    - Example: Facebook settled a BIPA class action for $650 million over its facial recognition photo-tagging feature, showing how quickly damages can multiply.
- **Practical guidance:** Conduct biometric privacy impact assessments before implementation and secure written releases from employees.

Other State Developments

- Delaware requires explicit notice when employers monitor communications or internet activity.
- Texas and Washington have introduced biometric privacy laws similar to BIPA but without private rights of action (i.e., only the state attorneys general are authorized to enforce these statutes).
- Florida Statute § 934.425 prohibits a person from installing or using a tracking device or application on another person's property without consent, but this prohibition does not apply to a person acting in good faith on behalf of a business entity for a legitimate business purpose.
- Employers should watch for new state-level bills addressing monitoring and workplace AI oversight.

U.S.: Key Takeaways

- Notice or consent may be required in several states, especially for electronic communications monitoring.
- Monitoring must be lawful and necessary: interception of communications requires a legitimate business purpose or prior consent; accessing stored messages also has limits.
- Biometric and health data are subject to stricter scrutiny: must be job-related, consistent with business necessity.
- Best practices: provide transparent notice, limit monitoring to legitimate purposes, secure data, define retention, and document business justification.

Canada

Canada: Legal Overview

- Canada's privacy framework blends federal oversight with provincial autonomy, requiring employers to align practices with both PIPEDA and applicable provincial laws.
- The federal Personal Information Protection and Electronic Documents Act (PIPEDA) covers federally regulated sectors such as telecommunications and banking.
- Alberta, British Columbia, and Quebec maintain private-sector privacy statutes that set out distinct obligations for employers operating in those provinces.
- Across jurisdictions, the guiding principles are transparency, proportionality, and necessity, demanding that employers justify and communicate monitoring activities.

Canada: Compliance in Practice

- Employers should provide clear notice describing the purpose, scope, and timing of each monitoring activity before it begins.
- Monitoring measures must be proportionate, demonstrating that the benefits outweigh the intrusion on employee privacy for the specific context.
- Employees have rights to access and challenge personal information collected through monitoring, requiring documented response procedures.
- **Practical tip:** conduct periodic privacy risk assessments and policy reviews to keep programs aligned with federal and provincial requirements.

Canada: Key Takeaways

- Necessity and proportionality are mandatory: monitoring must be reasonable, not overly intrusive, and clearly tied to a legitimate work-related purpose.
- Notice is essential: employees must be informed about what is being monitored, why, and how the information will be used.
- Employee rights apply: workers can access, challenge, or request correction of personal data collected through monitoring.
- Best practice: document business justification, conduct privacy risk assessments, and periodically review monitoring programs for compliance.

EUROPE & UNITED KINGDOM

GDPR Overview

- The General Data Protection Regulation (GDPR) sets strict conditions for monitoring and data processing, emphasizing transparency, proportionality, and necessity.
- Employee data is protected even when collected in professional contexts, requiring a lawful basis for each processing activity.
- Monitoring activities must undergo a legitimate interest assessment balancing business needs with employee rights.
- Fines for non-compliance can reach up to 4% of global annual turnover or €20 million, whichever is higher.

Lawful Bases for Monitoring Under GDPR

- Monitoring is generally justified under legitimate interest, provided that the employer's need outweighs the employee's right to privacy.
- Consent is often not a valid basis in employment contexts due to power imbalances between employer and employee.
- Employers should document the legitimate interest assessment (LIA) to demonstrate accountability and proportionality.
- Transparency obligations require employers to issue detailed privacy notices describing monitoring methods and retention periods.

EU Court and National Decisions

- The European Court of Human Rights (ECHR) in Bărbulescu v. Romania held that employers must inform employees in advance about monitoring and its scope.
- National data protection authorities have fined companies for failing to justify continuous video surveillance or tracking systems.
  - Example: In 2024, Amazon was fined in €32 million for overly intrusive warehouse tracking and video surveillance without sufficient justification in France.
- Employers must balance productivity and security objectives with workers' rights, ensuring the least intrusive means possible.
- **Practical advice:** Regularly audit monitoring practices and review proportionality assessments to align with evolving case law.

UK ICO Guidance on Workplace Monitoring

- The UK's Information Commissioner's Office (ICO) updated its Workplace Monitoring Guidance in 2023, aligning with GDPR principles while offering practical advice.
- Employers must conduct Data Protection Impact Assessments (DPIAs) for high-risk monitoring such as email interception or CCTV surveillance.
- Covert monitoring is permissible only in exceptional cases involving serious crime or misconduct and must be time-limited and narrowly targeted.
- The ICO emphasizes fairness, transparency, and employee awareness as core compliance principles.

EU & UK: Key Takeaways

- Lawful basis required: monitoring must rely on a lawful basis (usually legitimate interest or contract performance); employee consent is rarely valid due to power imbalance.
- Transparency is essential: employees must be clearly informed in advance about monitoring, its purpose, scope, and retention periods.
- Proportionality and necessity: employers must show monitoring is limited to what is necessary and not overly intrusive (e.g., avoid constant surveillance or monitoring in private areas).
- DPIAs are required for high-risk monitoring: Data Protection Impact Assessments are required when using tools like CCTV, or location tracking.
- Workers' rights: employees retain data rights (access, objection, erasure) and must be able to challenge excessive monitoring.
- Enforcement is active: national authorities have issued significant fines.

Latin America

Brazil: Legal Framework and Applicability

- **Comprehensive Regulation:** Brazil's General Data Protection Law (LGPD - Law No. 13,709/2018) establishes a national framework governing the collection, use, and storage of personal data, including in employment relationships.
- **Scope of Application:** The LGPD applies to both public and private entities that process personal data in Brazil or handle data concerning individuals located in Brazil, regardless of where the processing occurs.
- **Employment Relationships:** While the LGPD does not contain provisions exclusive to the workplace, it applies broadly to employer processing of employee, contractor, or candidate data, covering recruitment, monitoring, and termination activities.
- **Core Objective:** The law aims to safeguard fundamental rights of freedom, privacy, and the free development of personality, requiring lawful, transparent, and proportionate data practices.

Brazil: Lawful Bases and Core Principles

- **Legal Bases for Processing:** Under the LGPD, data processing in employment contexts typically relies on legal obligation, contract performance, or legitimate interest rather than consent, which is rarely valid due to the imbalance of power between employer and employee.
- **Purpose Limitation:** Employers must collect and process data only for specified, legitimate, and clearly communicated purposes directly related to the employment relationship.
- **Proportionality and Necessity:** Monitoring must be limited to data strictly necessary to achieve the stated purpose, avoiding excessive or continuous surveillance that could infringe employee rights.
- **Transparency Obligation:** Employers must provide employees with privacy notices describing data categories, processing purposes, retention periods, and the possibility of sharing with third parties or authorities.
- **Accountability Principle:** Employers must demonstrate compliance by implementing internal policies and maintaining documentation evidencing lawful data handling.

Brazil: Monitoring Practices in the Workplace

- **Electronic Communications and Email:** Employers may monitor company-provided email accounts to ensure compliance with internal policies and security requirements, provided employees are informed in advance and monitoring is limited to professional content.
- **CCTV and Video Surveillance:** Video monitoring is lawful when used for safety and security purposes and does not intrude into private or sensitive areas. Covert surveillance is generally discouraged unless justified by exceptional circumstances, such as suspected misconduct.
- **GPS Tracking:** Tracking devices may be used on company vehicles or equipment when the purpose is legitimate and the monitoring does not extend into personal or off-duty activities.
- **Biometric Systems:** Use of fingerprints or facial recognition for access control and timekeeping is permissible if proportionate and accompanied by clear notice and data protection safeguards.

Brazil: Compliance and Implementation Measures

- **Internal Governance:** Employers should develop and maintain privacy policies outlining monitoring practices, retention periods, and employee rights under the LGPD.
- **Data Minimization and Retention:** Personal data collected through monitoring should be limited to what is necessary and retained only as long as required for the stated purpose or legal compliance.
- **Employee Awareness:** Clear communication about monitoring policies during onboarding and periodic training reinforces transparency and reduces the likelihood of disputes.
- **Documentation and Risk Management:** Employers should document lawful bases for monitoring, ensure secure storage of collected data, and review monitoring tools periodically to confirm necessity and proportionality.
- **Practical Tip:** Embedding LGPD principles into company policy not only mitigates legal risk but strengthens organizational culture and employee trust.

Mexico: Legal Framework for Employee Monitoring

- **Regulatory Foundation:** The Federal Law on the Protection of Personal Data Held by Private Parties (FDPL) establishes rules for how employers can collect and process employee data, including that obtained through workplace monitoring.
- **Lawful Basis:** Monitoring must be justified by legitimate purposes tied to the employment relationship, such as compliance, security, or productivity oversight. Consent may not be required if the monitoring is proportionate and related to the employer's obligations.
- **Transparency Obligation:** Employers must notify employees before monitoring begins, clearly outlining the purpose, methods, data collected, and retention periods. Hidden or continuous monitoring without legitimate justification can be deemed unlawful.
- **Scope of Regulation:** The FDPL applies broadly to private-sector employers that process personal data in Mexico, regardless of storage medium or technology used.

Mexico: Monitoring Practices and Compliance Requirements

- **Electronic Communications:** Employers may review company-provided emails and systems for security and policy compliance if employees are informed and the monitoring remains proportionate to business needs.
- **CCTV and Surveillance:** Video monitoring is permitted for safety and security purposes but must avoid private spaces and continuous observation unrelated to legitimate business purposes.
- **Remote Work and Device Monitoring:** Tracking software or productivity tools must be disclosed to employees and limited to company-owned devices to avoid infringing privacy rights.
- **Practical Tip:** Employers should maintain written policies on monitoring, document their justification for each monitoring activity, and provide clear notice templates to ensure compliance and employee awareness.

Chile: Legal Framework for Employee Monitoring

- **Statutory Foundation:** Law No. 19.628 on the Protection of Private Life governs the processing of personal data in Chile, including that collected through employee monitoring.
- **Scope and Applicability:** The law covers both public and private employers and applies to all data that can identify an employee, regardless of the monitoring technology used.
- **Consent and Legitimate Purpose:** Monitoring is lawful when employees provide informed, written consent and when it serves a legitimate business purpose, such as ensuring compliance, workplace safety, or security.
- **Limitations on Monitoring:** Surveillance must remain proportionate to its intended purpose. Constant or covert monitoring without a clear and documented justification violates privacy expectations.

Chile: Transparency and Compliance Measures

- **Transparency Obligations:** Employers must inform workers about monitoring practices in advance, specifying the methods used, data collected, purposes, and duration of retention.
- **Internal Policies:** Incorporate monitoring rules into employment handbooks and onboarding materials to ensure awareness and consistent application.
- **Data Protection Practices:** Limit access to collected data, store it securely, and delete it once it is no longer necessary for the stated purpose.
- **Best Practice:** Conduct periodic internal reviews of monitoring systems and maintain documentation demonstrating compliance with Law No. 19.628's proportionality and transparency requirements.

Latin America: Key Takeaways

- Lawful basis required: monitoring must rely on a lawful basis under local privacy laws.
- Transparency and employee notice: employees should be informed about monitoring practices (methods, purposes, data collected, retention).
- Proportionality and necessity: employers must show monitoring is limited to what is necessary and not overly intrusive (e.g., avoid constant surveillance or monitoring in private areas).
- Limits and proportionality: continuous or intrusive surveillance (especially in private areas or outside work duties) is restricted. Monitoring must be necessary, proportionate, and limited to workplace-related purposes.
- Best practice across region: maintain written policies, document legal basis, train employees, and periodically review monitoring tools for necessity and compliance.

Asia-Pacific

Japan: Legal Framework for Employee Monitoring

- **Regulatory Basis:** Employee monitoring in Japan often involves handling personal information governed by the Act on the Protection of Personal Information (APPI).
- **Purpose Specification:** Employers must clearly define the purpose of monitoring and limit data collection and use to what is necessary for that purpose.
- **Legitimate Business Objective:** Monitoring must be justified by a legitimate need, such as ensuring security or preventing misconduct, and should never be excessive or unjustified.
- **Advance Notification:** As a general rule, employees should be informed in advance of any monitoring practices.
- **Risk of Violation:** Excessive or unnecessary surveillance may constitute a privacy infringement and expose employers to legal challenge under the APPI.

Japan: Governance and Workplace Application

- The Japanese Personal Information Protection Commission recommends that employers:
  - Define monitoring purposes in internal policies and communicate them clearly to employees.
  - Designate responsible personnel with specified authority for oversight.
  - Establish implementation rules in advance and explain them to all staff involved.
  - Conduct regular reviews to confirm monitoring remains appropriate and compliant.
- **Modern Workplace Implications:** Employers should ensure monitoring is lawful, proportionate, and transparent, with policies reviewed periodically for APPI alignment.
- **Employee Trust and Conduct:** Clear policies on monitoring and social media use help balance compliance and transparency, mitigating risks and reinforcing respect for employee privacy.

China: Legal Framework for Employee Monitoring

- **Regulatory Basis:** Employee monitoring in China falls under the Personal Information Protection Law (PIPL), which requires an identified lawful basis for collecting or processing personal data in the employment context.
- **Lawful Grounds:** In addition to consent, processing is lawful when it is necessary for:
  - The conclusion or performance of an employment contract;
  - Human-resources management in accordance with labor policies or collective agreements;
  - The performance of legal obligations or statutory duties;
  - The protection of life, health, or property in emergencies; or
  - The processing of publicly disclosed information within a reasonable scope.
- **Consent in Employment:** Consent is one lawful basis under the PIPL, but its validity in employment is debated due to the power imbalance. Therefore, employers often rely instead on other legal bases such as performance of the employment contract or HR management.
- Before implementing workplace surveillance, employers must identify and document the specific legal basis relied upon.

China: Practical Requirements and Transparency Obligations

- **Minimization Principle:** Monitoring must have a clear and reasonable purpose, be directly related to that purpose, and be conducted within the minimum necessary scope to avoid excessive data collection.
- **Proportionality:** Employers must ensure that surveillance measures are proportionate to the objective pursued and avoid intrusive methods where less invasive options can achieve the same purpose (e.g., if the goal is to prevent employees from accessing irrelevant websites, it is preferable to restrict access rather than monitor browsing activity).
- Employees must be informed before processing begins about:
  - The purpose and method of monitoring;
  - The types of personal information collected;
  - The duration of storage; and
  - Any potential consequences arising from surveillance.

Australia: Overview of Federal and State Regulations

- Australia's privacy and monitoring framework is shaped by both federal legislation and state-specific surveillance laws.
- The Privacy Act 1988 governs handling of personal data nationally, while the Telecommunications (Interception) Act 1979 prohibits unauthorized interception of communications.
- State laws, particularly in New South Wales (NSW) and the Australian Capital Territory (ACT), impose notice and purpose requirements for workplace surveillance.
- Employers must reconcile differences between federal and state frameworks to ensure lawful, transparent monitoring.

Australia: NSW and ACT Workplace Surveillance Acts

- NSW and ACT require written notice at least 14 days before implementing surveillance, including details on purpose, method, and location.
- In the ACT, employers must consult with employees before introducing surveillance technologies.
- Covert monitoring is allowed only with judicial authorization and for investigating serious misconduct.
- All surveillance records must be used solely for legitimate purposes, and employees should have access to policies outlining these obligations.

Australia: Victoria and Other States

- The Surveillance Devices Act 1999 (Victoria) forbids recording private activities without consent and prohibits surveillance in sensitive areas such as restrooms.
- GPS tracking of company vehicles requires employee awareness and consent under implied or express terms of employment.
- Other states, like Queensland and South Australia, rely on general privacy and interception laws rather than specific surveillance statutes.
- **Practical Tip:** Employers should adopt uniform policies and consent procedures nationwide to maintain consistent compliance.

Asia-Pacific: Key Takeaways

- Monitoring must be lawful, necessary, and purpose-specific: local laws require that employee monitoring has a clearly defined business purpose and is limited to what is necessary.
- Employee notice and transparency are central
- Practical compliance expectations: document lawful basis, define internal rules, assign responsible personnel, retain data only as needed, secure storage, and conduct periodic reviews or DPIA-style assessments when risks are high.

Employee Monitoring Scenarios

Scenario 1: Geolocation Monitoring

Scenario 1:

SnoopWorks International is a US-based company that employs a sales team that works remotely. They would like to track geolocation data on their company-issued cell phones to ensure their sales force is productive. They will only track data during work hours. SnoopWorks has sales team members in California, Florida, New York, Canada, and Brazil. Can SnoopWorks comply with all applicable privacy laws by notifying employees that they will be tracking their locations?

Scenario 1: Geolocation Monitoring

Scenario 1:

SnoopWorks International is a US-based company that employs a sales team that works remotely. They would like to track geolocation data on their company-issued cell phones to ensure their sales force is productive. They will only track data during work hours. SnoopWorks has sales team members in California, Florida, New York, Canada, and Brazil. Can SnoopWorks comply with all applicable privacy laws by notifying employees that they will be tracking their locations?

Which of the following are true:

A. This complies with FL law. Employers are permitted to use GPS tracking as long as it is during work hours and for business-related purposes.

B. This complies with the CCPA, as long as the employee is notified of the tracking.

C. This complies with New York's employee monitoring law because the employees are being provided with notice of the monitoring.

D. This complies with PIPEDA (Canada) as it serves a legitimate business purpose and employees are informed.

E. This complies with LGPD (Brazil) as long as the employee provides general written consent on being monitored by the employer.

Scenario 2: Wearables

Scenario 2:

SnoopWorks employs workers at manufacturing plants in Illinois, Pennsylvania, Brazil, China, and France. The plants contain hazardous chemicals, in addition to heavy equipment, both of which create safety concerns. SnoopWorks would like to require its manufacturing workers to wear smart watches that will monitor employees' heartrates, create ergonomic maps to monitor posture while carrying heavy equipment, and alert employees when they are in proximity to potential hazards. The data from such devices will be maintained in employees' personnel files for one year after collection and will be accessible to human resources managers during that time. SnoopWorks will provide employees with notice but does not intend to obtain consent: any employees who decline to use the smartwatches will be terminated.

Scenario 2: Wearables

Scenario 2:

SnoopWorks employs workers at manufacturing plants in Illinois, Pennsylvania, Brazil, China, and France. The plants contain hazardous chemicals, in addition to heavy equipment, both of which create safety concerns. SnoopWorks would like to require its manufacturing workers to wear smart watches that will monitor employees' heartrates, create ergonomic maps to monitor posture while carrying heavy equipment, and alert employees when they are in proximity to potential hazards. The data from such devices will be maintained in employees' personnel files for one year after collection and will be accessible to human resources managers during that time. SnoopWorks will provide employees with notice but does not intend to obtain consent: any employees who decline to use the smartwatches will be terminated.

Which of the following are true:

A. This complies with the EEOC's recent guidance regarding the use of wearables because the collection of information is job-related and consistent with business necessity.

B. This violates the Illinois Biometric Information Privacy Act (BIPA) because the employer is not obtaining consent to the collection of the data.

C. SnoopWorks can do it in France as long as it obtains written consent from the affected employees.

D. SnoopWorks must obtain separate explicit consent from its Chinese employees for this type of monitoring.

E. This complies with LGPD (Brazil) because the monitoring is for the protection of the employees.

Scenario 3: Screen Trackers/Video Recordings

Scenario 3:

SnoopWorks' corporate employees are provided with company-issued laptops. Many employees work remotely. They are based in Connecticut, Delaware, Pennsylvania, Germany, and Canada. SnoopWorks would like to implement software that will track the employees' screen activity in real time to ensure productivity. The software monitors keystrokes, browser usage, and the time spent on each application, and it also records audio/video from cameras installed on the laptops. SnoopWorks' HR department will have access to the data and may take disciplinary action based on the information collected. SnoopWorks' handbook states that SnoopWorks has the right to monitor employee activity on any company-issued devices, and that employees do not have a right to privacy in communications on any such devices. SnoopWorks does not intend to issue any additional/separate notices relating to the software.

Scenario 3: Screen Trackers/Video Recordings

Scenario 3:

SnoopWorks' corporate employees are provided with company-issued laptops. Many employees work remotely. They are based in Connecticut, Delaware, Pennsylvania, Germany, and Canada. SnoopWorks would like to implement software that will track the employees' screen activity in real time to ensure productivity. The software monitors keystrokes, browser usage, and the time spent on each application, and it also records audio/video from cameras installed on the laptops. SnoopWorks' HR department will have access to the data and may take disciplinary action based on the information collected. SnoopWorks' handbook states that SnoopWorks has the right to monitor employee activity on any company-issued devices, and that employees do not have a right to privacy in communications on any such devices. SnoopWorks does not intend to issue any additional/separate notices relating to the software.

Which of the following are true:

A. This violates Connecticut law because the employer has not posted a conspicuous notice about monitoring in the workplace and provided specific notice to employees regarding the monitoring. This also violates CT's wiretap law because it captures audio without the consent of both parties.

B. This does not violate Delaware law because Delaware does not require notice and consent to electronic monitoring.

C. This complies with Pennsylvania law.

D. SnoopWorks can do this in Germany as long as its employees there have been provided with and consented to the handbook.

E. This is not allowed in Canada because the monitoring is not reasonable and transparent

Scenario 4: Chair Sensors for Office Utilization

Scenario 4:

SnoopWorks has decided to implement a “hoteling” system to reduce office space and associated overhead, given its hybrid workforce. To track usage rates in the office, SnoopWorks installs sensors under office chairs in an open office with a "hoteling" system to track usage rates. The sensors monitor when chairs are occupied but do not collect identifiable data about individual employees. SnoopWorks does not provide notice to employees. The sensors are used in New Jersey, Texas, Brazil, Canada, and Scotland. Is SnoopWorks compliant with applicable privacy laws?

Scenario 4: Chair Sensors for Office Utilization

Scenario 4:

SnoopWorks has decided to implement a “hoteling” system to reduce office space and associated overhead, given its hybrid workforce. To track usage rates in the office, SnoopWorks installs sensors under office chairs in an open office with a "hoteling" system to track usage rates. The sensors monitor when chairs are occupied but do not collect identifiable data about individual employees. SnoopWorks does not provide notice to employees. The sensors are used in New Jersey, Texas, Brazil, Canada, and Scotland. Is SnoopWorks compliant with applicable privacy laws?

Which of the following are true:

A. This complies with New Jersey law, which does not require notice or consent in this context.

B. This violates the Texas Capture or Use of Biometric Identifiers Act (CUBI) because it does not provide notice or require consent from employees.

C. This complies with the laws in Brazil, Canada, and Scotland, but SnoopWorks should inform the employees of the monitoring and obtain their consent as a matter of good practice.

GLOBAL PRINCIPLES & BEST PRACTICES

Common Themes Across Jurisdictions

- Transparency remains the universal foundation: employees must know what monitoring occurs, why it occurs, and how data is used.
- Proportionality and necessity guide permissible monitoring: only data relevant to legitimate business purposes should be collected.
- Accountability and documentation are critical; maintain policies, assessments, and records of compliance activities.
- Data security measures such as encryption and restricted access must accompany monitoring programs to safeguard collected information.

Building a Global Compliance Framework

- Employers should conduct law mapping to identify applicable privacy regulations across jurisdictions before deploying monitoring systems.
- A unified global policy fosters consistency while allowing for regional adaptations in notice, consent, and recordkeeping requirements.
- Training and governance structures ensure HR, IT, and legal teams understand and consistently apply monitoring policies.
- Cross-department collaboration enhances oversight and minimizes risks of fragmented compliance efforts.

Conducting Impact Assessments and Audits

- Data Protection Impact Assessments (DPIAs) or Privacy Impact Assessments (PIAs) are essential before introducing monitoring tools with privacy risks. In many jurisdictions (e.g., Europe, China, Brazil), they are not only best practice but legally required when the monitoring presents high risk.
- Assessments should evaluate less intrusive alternatives and document justifications for chosen methods.
- Retention and deletion policies must ensure data is not stored longer than necessary for the stated purpose.
- Comprehensive documentation demonstrates accountability and supports defense in regulatory inquiries.

Compliance Checklist

- **Define purpose:**
  - Document the specific, legitimate aims for monitoring and the metrics you will use.
- **Select legal basis:**
  - Identify and record the lawful basis per jurisdiction (e.g., contract performance, HR management, legal obligation, legitimate interests, or consent) where applicable.
- **Assess risk (DPIA/PIA):**
  - Perform and record DPIAs/PIAs for high-risk monitoring where applicable.
- **Limit scope and intrusiveness:**
  - Choose the least intrusive tool; avoid sensitive areas; disable off-duty tracking; set sampling rather than continuous capture where possible.
- **Consult and notify:**
  - Provide clear advance notice; bargain/consult where required (unions, works councils); follow local notice rules.
- **Vendor and data safeguards:**
  - Put DPAs/SCCs in place; restrict access by role; log access; use encryption; test security.
- **Retention and deletion:**
  - Set short, purpose-based retention; auto-deletion; document schedules.
- **Employee rights handling:**
  - Provide channels for access, correction, objection; handle requests within statutory timelines.
- **Training and governance:**
  - Assign accountable owners; train staff operating the systems; keep policy and SOPs current.
- **Review and audit:**
  - Re-evaluate necessity, proportionality, accuracy, and bias; remediate issues; document reviews.

Practical Steps for In-House Counsel

- Develop and review comprehensive monitoring policies reflecting both global and local legal standards.
- Negotiate vendor contracts to ensure third-party monitoring tools comply with privacy, data transfer, and security obligations.
- Coordinate among HR, IT, and compliance departments to ensure consistency in applying policies and responding to employee inquiries.
- Maintain dialogue with regulators and monitor legislative developments to anticipate compliance changes.

Takeaways

- Prioritize transparency: always notify employees before implementing monitoring systems.
- Document consent, assessments, and justifications for each form of monitoring.
- Apply data minimization and security principles to reduce risk of overreach or breach.
- Regularly update policies and conduct audits to align with new laws and technological advances.

U.S. and International Privacy Laws Relating to Employee Monitoring

Thank you for joining us. We look forward to seeing you at future events.

Key Regulatory Bodies & Resources

- **United States**
  - Equal Employment Opportunity Commission (EEOC)
  - National Labor Relations Board (NLRB)
  - State privacy/enforcement bodies: e.g., California Privacy Protection Agency (CPPA), state Attorneys General
- **Canada**
  - Office of the Privacy Commissioner of Canada (OPC)
  - Provincial regulators: OIPC British Columbia, OIPC Alberta, Commission d'accès à l'information (Québec)
- **European Union**
  - European Data Protection Board (EDPB)
  - National DPAs: CNIL (France), BfDI (Germany), AEPD (Spain), Garante (Italy), DPC (Ireland), etc.
- **United Kingdom**
  - Information Commissioner's Office (ICO)

Key Regulatory Bodies & Resources

- **Brazil**
  - Autoridade Nacional de Proteção de Dados (ANPD)
- **Mexico**
  - Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)
- **Chile**
  - Law 21.719 creates the new Data Protection Agency (enters into force Dec 2026)
- **Japan**
  - Personal Information Protection Commission (PPC)
- **China**
  - Cyberspace Administration of China (CAC) and competent authorities under PIPL
- **Australia**
  - Office of the Australian Information Commissioner (OAIC)
  - State/Territory bodies for surveillance/privacy (e.g., NSW Information & Privacy Commission; Office of the Victorian Information Commissioner)