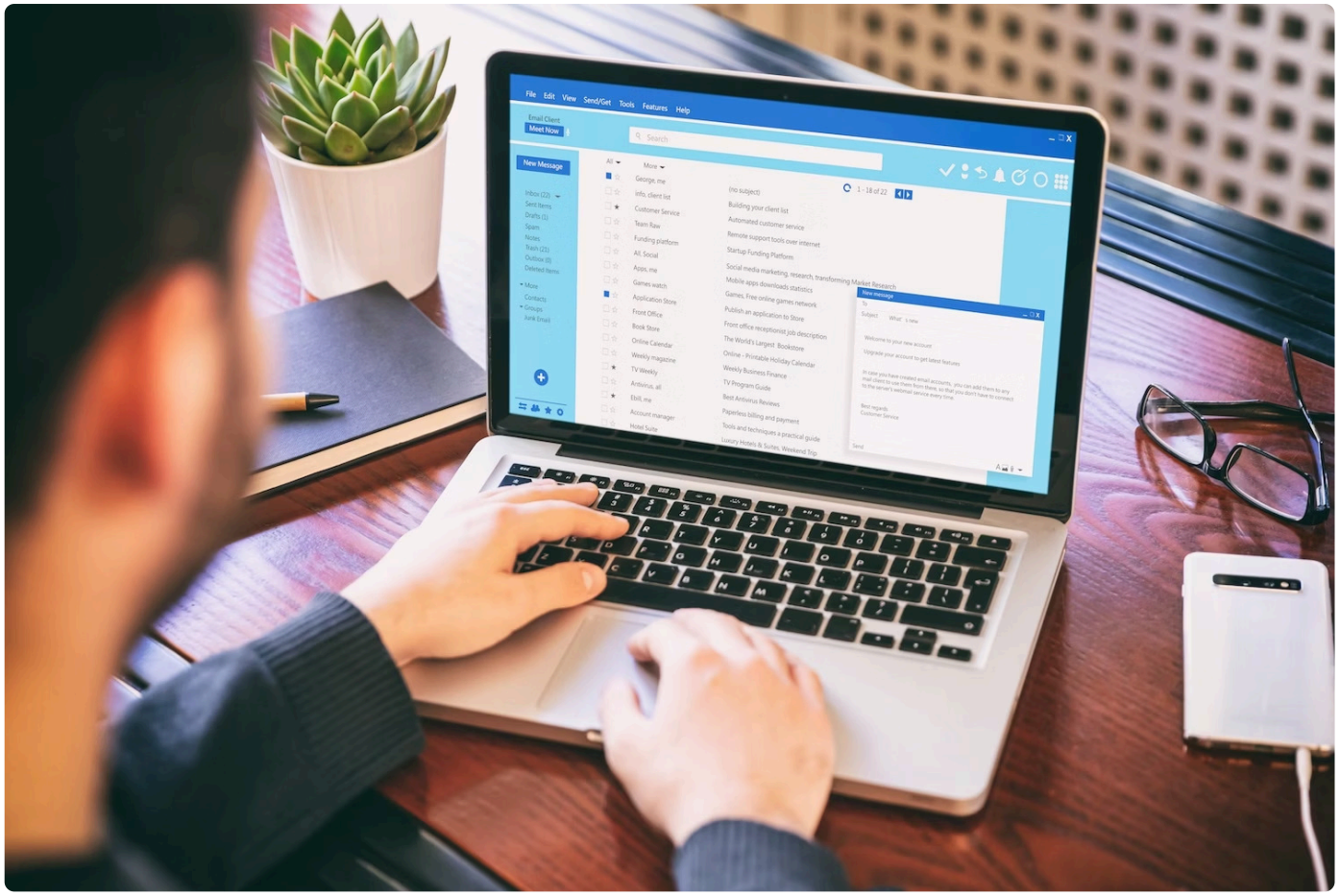
# Workplace Monitoring Laws: Email, Devices, Video, and Remote Work

**Scott Johnson** is a Partner at Dunlap Bennett & Ludwig PLLC, where he focuses on management-side employment law and litigation, corporate transactions, government contracting, and outside general counsel services. Scott regularly advises employers on worker classification, independent contractor agreements, restrictive covenants, and multi-state compliance, with particular experience helping growing companies design classification frameworks that hold up under IRS and state agency scrutiny.

**Scott Johnson, Partner**

DUNLAP BENNETT & LUDWIG



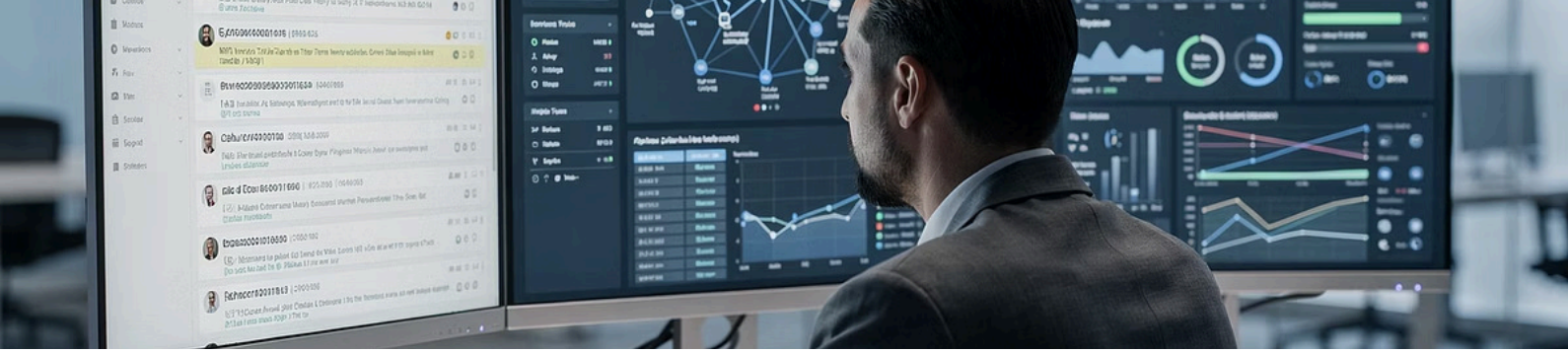
Employer monitoring of workplace communications and devices is lawful in most circumstances—but "lawful" is not the same as "unrestricted." The legal framework governing workplace monitoring is built on federal baseline rules that grant employers significant latitude, layered with state-specific notice, consent, and recording requirements that vary by jurisdiction, communication type, and whether the employee is working on-site or remotely.

*This article explains the federal framework that governs most employer monitoring, the state laws that impose additional obligations, and the practical distinctions between monitoring email, phone calls, video, internet usage, and personal devices.*

**Note:** Our previous article "Employee Privacy Rights in 2026: What Employers Need to Know," provides the foundational overview of the 2026 state privacy law landscape, the critical employee data exemption, and the federal statutory framework. This article builds on that foundation. If you have not read it yet, we recommend starting there.

# The Federal Baseline: ECPA and Its Exceptions

The Electronic Communications Privacy Act of 1986, as amended, is the primary federal statute governing employer monitoring of electronic communications. ECPA prohibits the intentional interception of wire, oral, and electronic communications—but it includes two exceptions that, in practice, permit most workplace monitoring.



## The Business-Use Exception

Under 18 U.S.C. §2511(2)(a)(i), an employer may intercept communications on telephone or electronic equipment provided by the employer in the ordinary course of business. Courts have interpreted this to permit monitoring of employee email, chat, and internet usage on company-owned systems when the monitoring serves a legitimate business purpose—security, compliance, productivity management, or investigation of misconduct. The exception does not authorize monitoring for personal curiosity or purposes unrelated to the employer's business.

The business-use exception has a practical limit: when an employer monitoring a phone call determines that the call is personal in nature, the employer is expected to stop listening. Courts have consistently held that continuing to monitor a call once it is identified as personal exceeds the scope of the business-use exception.

## The Consent Exception

Under 18 U.S.C. §2511(2)(d), interception is permitted where one party to the communication has given prior consent. In the employment context, this typically means the employer obtains employee acknowledgment—through an acceptable use policy, an employee handbook provision, or a standalone monitoring consent form—that communications on company systems may be monitored. A well-drafted policy that employees sign serves as both the legal basis for monitoring and the practical mechanism for managing expectations.

Together, these two exceptions mean that employers who maintain clear written monitoring policies, use them on company-owned systems, and obtain employee acknowledgment are operating within ECPA's framework for the vast majority of workplace monitoring activities.

## The Stored Communications Act

The Stored Communications Act (SCA), which is Title II of ECPA, prohibits unauthorized access to stored electronic communications. For employers, the SCA primarily restricts access to employees' personal email accounts, cloud storage, and social media accounts that are not hosted on company systems. Accessing an employee's personal Gmail account, even on a company device, without authorization would implicate the SCA. The SCA reinforces what good policy already dictates: company monitoring policies should be limited to company systems and company-provided accounts.

# State Electronic Monitoring Notice Requirements

Several states impose notice or consent requirements that exceed the federal baseline. The most significant are Connecticut, New York, and Delaware, each of which requires affirmative employer action before monitoring begins.

1

### Connecticut

Prior written notice to all employees who may be subject to electronic monitoring; conspicuous posting in workplace

**Consent required:** Notice only

**Statute:** Conn. Gen. Stat. §31-48d

2

### New York

Written notice to employees upon hiring that electronic activity may be monitored; conspicuous posting

**Consent required:** Notice only

**Statute:** N.Y. Civ. Rights Law §52-c

3

### Delaware

Written notice to employees before monitoring electronic communications, including email, internet, and telephone

**Consent required:** Notice only

**Statute:** Not specified

4

### California

Notice at collection of personal information; all-party consent for audio recording of calls

**Consent required:** Notice + audio consent

**Statute:** CPRA; Cal. Penal Code §632

5

### Texas

Consent before capturing biometric identifiers

**Consent required:** Biometric consent

**Statute:** Tex. Bus. & Com. Code §503.001

6

### Colorado

Written consent before biometric data collection (effective July 2025)

**Consent required:** Biometric consent

**Statute:** Colo. Privacy Act (amended)

**Practice Note:** An important distinction runs through this table. Connecticut, New York, and Delaware require notice—not consent—for electronic monitoring. The employer must inform employees that monitoring occurs, but does not need the employee's affirmative agreement to proceed. California requires notice for data collection generally and consent specifically for audio recording. Colorado and Texas require consent, but only for biometric data collection, not general electronic monitoring. Conflating notice with consent—or applying one state's standard across the board—is a common and avoidable compliance error.

Employer review of email and chat communications on company systems is the most well-established form of workplace monitoring. Under ECPA's business-use and consent exceptions, employers may review company email, Slack and Teams messages, and internal chat platforms when they have a legitimate business reason and employees have been notified that monitoring may occur.

Best practice is a written electronic communications policy that states clearly: employees should have no expectation of privacy in communications sent, received, or stored on company systems. The policy should specify what may be monitored (email, chat, file transfers, internet history), who has access to monitoring data, how long it is retained, and the business purposes it serves. Employees should sign an acknowledgment.

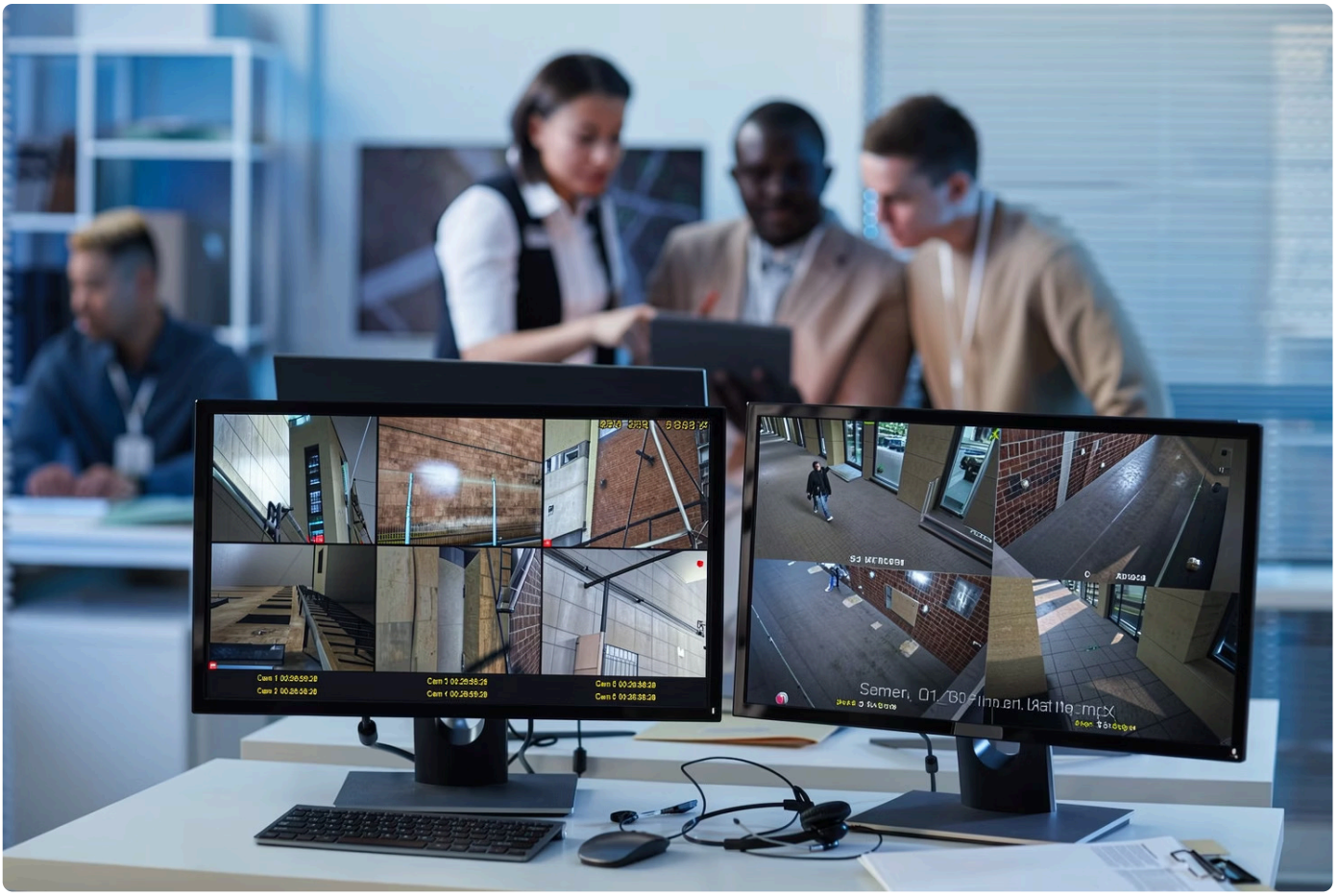
Text messages on company-issued phones present a closer question. Courts have generally permitted employer review of text messages on company devices under the same framework—business use, company ownership, policy notice—but employer access to text messages on an employee's personal phone requires either consent or a lawful basis such as litigation hold or investigation subpoena.

# Phone Monitoring and Audio Recording

Phone monitoring involves a layered analysis. At the federal level, ECPA's business-use exception permits employers to monitor business calls on company phone systems, subject to the personal-call limitation described above. But audio recording—whether of phone calls or in-person conversations—implicates state wiretapping and eavesdropping laws that vary significantly.

The majority of states follow a one-party consent rule: recording is permitted if one party to the conversation consents. In the employer context, the employer (or an agent monitoring the call) typically serves as the consenting party. But eleven states—California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, New Hampshire, Pennsylvania, and Washington—require all-party consent for audio recording. In these jurisdictions, an employer who records a phone call without the other party's knowledge faces potential criminal liability, not just civil exposure.

The practical takeaway: for organizations with employees or callers in all-party consent states, phone monitoring policies must either obtain consent from all parties (through a recorded disclosure at the beginning of the call) or limit monitoring to silent observation without recording.



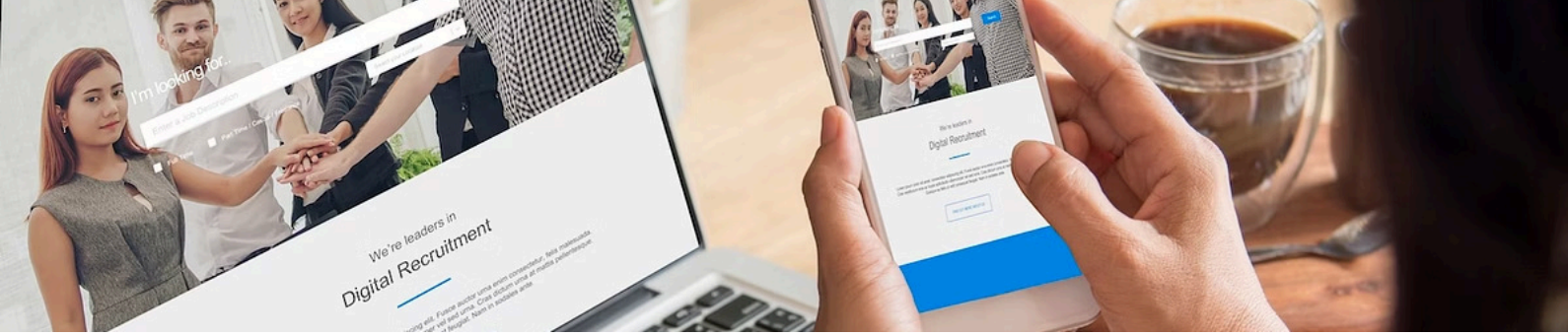
# Video Surveillance in the Workplace

Silent video surveillance in the workplace is generally permitted for legitimate business purposes—security, theft prevention, safety—provided employees receive notice. Courts have drawn a consistent bright line at private areas: video recording in bathrooms, locker rooms, changing areas, and lactation rooms is prohibited in virtually all jurisdictions and will generate liability.

The addition of audio to video surveillance transforms the legal analysis. Because audio recording implicates wiretapping statutes, a security camera with a microphone in an all-party consent state may violate state law even if the video component is permissible. Employers should default to silent video unless they have specifically analyzed the audio recording laws in each jurisdiction where cameras are deployed.

Break rooms present a gray area. While not "private" in the same sense as a restroom, employees may have a reasonable expectation that conversations in a break room are not being recorded. The safest approach is conspicuous signage and a policy that identifies all areas under video surveillance.

Employers routinely monitor internet usage on company networks and devices for security and productivity purposes. This includes web browsing history, application usage analytics, download logs, and time-on-site metrics. Under ECPA's business-use exception and with appropriate policy notice, this monitoring is generally lawful.




# Internet Usage and Web Browsing Monitoring

Keystroke logging and screen capture tools represent a more invasive form of monitoring that can inadvertently capture personal information—passwords to personal accounts, medical portal interactions, or private communications. The legal permissibility of these tools depends on the same framework (business purpose, company system, employee notice), but the intrusiveness increases litigation risk and may implicate state privacy protections, particularly in California, where the constitutional right to privacy applies even in the workplace.

# BYOD Policies and Personal Device Monitoring

Bring-your-own-device arrangements create the most challenging monitoring questions because the employer's interest in securing corporate data sits in tension with the employee's ownership of the device and expectation of privacy over personal content.

A well-drafted BYOD policy addresses this tension directly. It should specify that the employer may access, monitor, and remotely wipe corporate data and applications on the personal device; that the employer will use mobile device management (MDM) or containerization technology to separate corporate data from personal content; that the employer will not access personal applications, photos, messages, or browsing history outside the corporate container; and that the employee consents to these terms as a condition of using a personal device for work.

Without this separation—both technological and contractual—an employer who performs a full device wipe or reviews personal content on an employee's phone during an investigation risks Stored Communications Act claims, state privacy claims, and practical litigation over the destruction of personal property.

# Remote Work Monitoring: The 2025 Frontier

The shift to hybrid and remote work has expanded workplace monitoring into employees' homes—and the legal framework has not fully caught up. Employers are deploying productivity tracking software, webcam-based activity verification, keystroke and mouse-movement monitoring, screenshot tools, and application-usage analytics on remote workers' company-issued devices.

The legal analysis for remote monitoring on company devices largely tracks the same framework as in-office monitoring: ECPA's exceptions apply, state notice requirements apply, and the employer's legitimate business interests support proportionate monitoring. But two additional considerations arise in the remote context.

First, webcam and audio monitoring in an employee's home raises heightened privacy expectations. A webcam that captures household members, personal conversations, or the interior of the home goes beyond what a security camera in an office lobby captures. Employers should limit webcam use to scheduled meetings and avoid always-on video monitoring absent extraordinary justification.

Second, the NLRB's attention to surveillance that chills Section 7 activity—the right to organize and engage in concerted activity—extends to remote monitoring tools. Keystroke logging and always-on screen monitoring that could capture employees discussing workplace conditions, wages, or unionization on company devices may draw NLRB scrutiny, particularly in the current enforcement climate.

## GPS and Location Tracking

GPS tracking of company-owned fleet vehicles is well-established and generally permissible when justified by safety, logistics, or regulatory compliance. The employer owns the vehicle, the tracking serves a business purpose, and employees are notified.

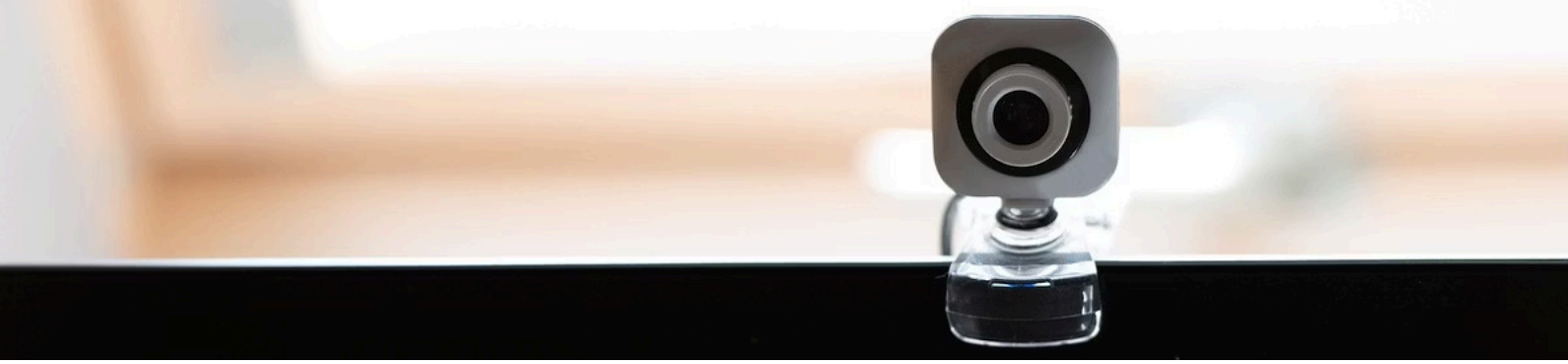
Tracking becomes problematic when it extends to employees' personal vehicles, to location tracking via personal cell phones, or to monitoring that continues during off-duty hours. Several states protect lawful off-duty conduct, and location tracking that reveals an employee's after-hours movements—visits to a doctor, a house of worship, a political rally, or a union hall—creates exposure under both state privacy laws and anti-discrimination statutes. The safest practice is to limit GPS tracking to company assets during working hours and to disable tracking functionality when employees are off duty.

## Building a Defensible Monitoring Program

The legal framework rewards transparency and proportionality. A defensible monitoring program includes the following components.

Written policy. A clear, comprehensive monitoring policy that identifies every form of monitoring the employer uses, explains its business purpose, describes the scope and timing of monitoring, identifies who has access to monitoring data, specifies retention periods, and states that employees should have no expectation of privacy on company systems.

Employee acknowledgment. Signed acknowledgment from every employee, obtained at hire and upon material policy updates. This satisfies ECPA's consent exception and state notice requirements simultaneously.



Jurisdiction-specific compliance. A matrix identifying each state where employees work and the specific monitoring, notice, consent, and recording requirements that apply in that jurisdiction. National employers cannot rely on a single policy drafted to federal minimums.

Proportionality. Monitoring should be calibrated to its stated purpose. Keystroke logging for a customer service team handling financial data is easier to justify than keystroke logging for a marketing team. Always-on webcam monitoring is almost never proportionate to any legitimate business need.

Separation of personal and business. Clear technological and policy boundaries between company systems (where monitoring is expected) and personal devices, accounts, and communications (where it is not). BYOD policies and MDM tools should enforce this boundary.

Documented business justification. For each monitoring tool deployed, a documented explanation of the business need it serves. This record supports the employer's position in any subsequent challenge and demonstrates the proportionality regulators and courts expect.

# About the Author

**Scott Johnson** is a Partner at Dunlap Bennett & Ludwig PLLC, where he focuses on management-side employment law and litigation, corporate transactions, government contracting, and outside general counsel services. Scott regularly advises employers on worker classification, independent contractor agreements, restrictive covenants, and multi-state compliance, with particular experience helping growing companies design classification frameworks that hold up under IRS and state agency scrutiny.

- **Please note:** *This article is for informational purposes only and does not constitute legal advice. The legal process is complex and highly dependent on the specific facts of your case. For guidance on your unique situation, we invite you to schedule a confidential consultation with our experienced legal team.*

## Strategic Counsel for Workforce Privacy Compliance

If you are aligning workforce data collection, biometric consent flows, monitoring policies, or vendor contracts with the most recent wave of state updates, our employment attorneys can help you design compliance programs that are defensible, practical, and built for the jurisdictions where your people actually work.

*Dunlap Bennett & Ludwig is a veteran-owned law firm with offices across multiple states. Our privacy and business attorneys combine legal expertise with practical operational experience to help companies navigate workplace monitoring compliance while maintaining focus on their core business objectives.*

To learn more about Dunlap Bennett & Ludwig, call **888-306-4030** or email **clientservices@dbllawyers.com**.