MAY 29, 2025 | AI/TECHNOLOGY, PRIVACY & DATA SECURITY

Navigating Legal Risk in the Remote Work Era

The widespread adoption of remote work arrangements has reframed the employment landscape, offering organizations access to a broader talent pool and increased operational flexibility. However, this reorganization also presents complex legal challenges—many of which remain underappreciated.

As employees work from locations that may be hundreds or thousands of miles from their employers' offices, questions of applicable law, regulatory obligations, and legal exposure become increasingly difficult to resolve. In particular, employers must contend with a patchwork of state and federal employment laws, jurisdictional triggers based on employee location, and a rising set of cybersecurity and compliance risks; all of which may be activated by something as simple as an employee moving across state lines.

The Problem of Legal Geography: Where Your Employees Are Matters

Too often, employers operate on the assumption that compliance flows from where the company is headquartered. But in practice, most employment laws look to the employee's physical location, not the employer's. And in a remote-first world, that means companies are increasingly subject to laws in places they never intended to do business.

Sometimes, those laws have clearly defined geographic limits. Other times, they don't. In general, courts apply a presumption against extraterritoriality, declining to apply a state law outside its borders unless the statute expressly says otherwise. However, this is state-dependent: some states reject the presumption and instead rely on traditional statutory interpretation or conflict-of-laws principles. This creates real confusion—particularly when an employee lives in one state, reports to a supervisor in another, and accesses systems hosted in a third.

In Washington, D.C., for example, the law often looks to where the controlling authority or supervisor resides. That means a Virginia-based employee working remotely could potentially be protected by D.C.'s Human Rights Act simply because their boss sits in a D.C. office. In contrast, California's CFRA typically applies to employers with five or more employees nationwide, even if just one works remotely in California. New York's paid sick leave law triggers based on total employee headcount, regardless of where employees are located.

Not Just Leave Laws: Workers' Comp and Wage Claims

The same jurisdictional tangle applies to workers' compensation insurance, which is state-regulated and location-specific. If a remote employee moves to another state, even temporarily, and suffers a workplace injury

there, an employer might find itself out of compliance and uninsured, despite having coverage in the home state.

Similarly, wage-and-hour enforcement agencies may assert jurisdiction based on where the work is performed. A remote worker who moves to Massachusetts or California—two states with aggressive wage enforcement regimes—may trigger recordkeeping, overtime, or meal/rest break obligations even if the employer never intended to operate in those jurisdictions.

Disability Accommodations and Remote Work

Remote work raises important considerations under the Americans with Disabilities Act (ADA). In many cases, remote work may be considered a reasonable accommodation, particularly if the employee can perform essential job functions from home. Blanket refusals to allow remote work—especially when previously permitted—can lead to legal challenges.

More broadly, remote work itself has roots in disability accommodation. Many of the structures now widely used for hybrid and distributed workforces began as accessibility strategies. As such, employers should treat remote work policies not only as productivity tools, but also as frameworks for compliance and inclusion. Denying remote work without individualized assessment can increase risk under the ADA and parallel state laws.

Surveillance and Privacy Compliance

Employers using digital productivity tools or surveillance software must carefully navigate state privacy and consent laws—including notice and affirmative agreement requirements in jurisdictions like California, Connecticut, and New York. These rules vary widely and often require transparency about monitoring methods, data use, and access rights.

I-9 Verification and Remote Onboarding

On the compliance front, employers must ensure they follow DHS guidance for Form I-9 verification when onboarding remote employees. This includes adhering to evolving rules for document inspection, which now permit alternatives to in-person review under designated circumstances. Failure to comply can lead to fines and delays in workforce activation.

Insider Threats, Dual Jobs, and Cross-Border Data Exposure

Legal risk is only half the story. Employers must also contend with security vulnerabilities introduced by remote work—particularly the growing threat of insider access abuse. Remote onboarding makes it harder to verify identity, monitor behavior, or detect when someone is using multiple logins, multiple devices, or even subcontracting their job to someone else.

One of the most alarming examples involved a widespread infiltration scheme by North Korean IT operatives, who posed as remote contractors and embedded themselves into U.S. companies. These operatives used AI-generated resumes, spoofed identities, and third-party U.S. devices to obtain credentials and take advantage of proprietary access.

Compounding this risk is the dual employment problem: remote workers taking on multiple roles, sometimes with

competitors, while logged into proprietary systems. Without proper controls, this creates exposure to IP theft, trade secret misappropriation, and misuse of company infrastructure.

Cross-border concerns add another layer. The U.S. Department of Justice's recent rule on sensitive personal data prohibits unauthorized access to personal data by individuals or entities affiliated with foreign adversaries. The rule explicitly highlights employment and contracting relationships as vectors of risk, reinforcing the importance of knowing not just who your workers are—but where they are, and who else might be behind them.

Each of these elements underscores a larger truth: employment agreements and company policies must evolve to address the operational and legal complexities of a distributed workforce. To manage risk across jurisdictions, employers should establish core protocols that apply regardless of employee location. Use the checklist below as a starting point for legal and operational safeguards.

Checklist

To manage risk across jurisdictions, employers should establish core protocols that apply regardless of employee location. Use the checklist below as a starting point for legal and operational safeguards:

- Require employees to disclose current work location and notify of relocations.
- Track employee count by state to identify triggered laws (e.g., paid leave, discrimination, wage rules).
- Consider whether necessary to maintain workers' compensation coverage in every state where employees work.
- Update employment agreements with jurisdiction clauses, confidentiality, and dual employment provisions.
- Limit access to sensitive systems based on necessary access.
- Monitor for insider threat signals: location spoofing, multiple jobs, or foreign access.
- Revoke credentials and retrieve data promptly at offboarding.
- Ensure monitoring tools comply with state privacy and consent laws.

Conclusion

Remote work offers real advantages—but only when employers understand and manage the legal obligations that follow employees across jurisdictions. A single relocation can trigger new wage laws, leave entitlements, workers' compensation requirements, or even data security concerns. Organizations that take a proactive, jurisdiction-aware approach to remote work can stay compliant, protect sensitive information, and support flexibility without increasing exposure. Legal counsel can be instrumental in helping employers evaluate risk, update policies, and implement frameworks that reflect both operational needs and legal obligations—ideally before issues arise.