# Insider Threats and Employee Monitoring: Balancing Security, Privacy, and Evidence


Speakers:

- **Daniel B. Garrie**, Esq., Founder, Law & Forensics; Neutral, JAMS; Adjunct Faculty, Harvard
- **Willie C. Session,** Ph.D., CISO, Booking Holdings Financial Services
- **Ed Stroz**, Consultant
- **Lawrence M. Hadley**, Esq., Partner, Glaser Weil Fink Howard Jordan & Shapiro LLC

# Disclaimer



This is not legal advice, nor should it be considered legal advice.



This presentation and the comments contained therein represent only the personal views of the participants, as spoken and do not reflect those of their employers or clients.



This presentation is offered for educational and informational uses only.

(c) 2026 Lexeprint Inc. All Rights Reserved.

# Speakers



**Daniel B. Garrie, Esq.**
Founder, Law & Forensics
Neutral, JAMS
Adjunct Faculty, Harvard



**Willie C. Session, Ph.D.**
CISO, Booking Holdings
Financial Services



**Ed Stroz**
Consultant



**Lawrence M. Hadley, Esq.**
Partner, Glaser Weil

(c) 2026 Lexeprint Inc. All Rights Reserved.

# Agenda

1. **Threat Model**
2. **Legal Boundaries**
3. **Evidence Discipline**
4. **Operational Playbook**

(c) 2026 Lexeprint Inc. All Rights Reserved.

# Threat Model



# Why This Topic Is Hard Now

**Security need**

**Privacy duty**

**Evidence burden**

**Defensible insider-threat monitoring = targeted collection + notice + minimization + chain of custody**




## Failure modes

- Over-collection that creates privacy and privilege problems
- Under-collection that leaves counsel without admissible evidence
- Poor documentation that makes valid evidence look unreliable
- Opaque AI scoring that creates employment and discrimination risk

(c) 2026 Lexeprint Inc. All Rights Reserved.

# Insider Threat Taxonomy

A defensible program starts by distinguishing intent, access, and evidence sources.

## Malicious insider

Data theft, sabotage, fraud, extortion, competitive misuse

## Negligent insider

Misdelivery, shadow IT, credential reuse, accidental disclosure

## Compromised insider

Phished account, stolen token, session hijack, malware-assisted access

## High-risk insider

Privileged admin, departing employee, contractor, M&A integration user

**Legal significance: motive is not enough. Tie each claim to policy authorization, system rights, evidence artifacts, and proportional collection.**

(c) 2026 Lexeprint Inc. All Rights Reserved.

# What Employers Actually Monitor

Employee monitoring is no longer just email review. It is a telemetry ecosystem.

### Endpoint

- EDR, file activity, USB, screenshots

### Identity

- SSO, MFA, privileged access, impossible travel

### Network

- DLP, proxy, CASB, firewall, VPN logs

### Collaboration

- Email, chat, shared drives, repositories

### Physical/IoT

- Badges, cameras, GPS, wearables

### AI/Analytics

- Risk scores, anomaly detection, productivity metrics

(c) 2026 Lexeprint Inc. All Rights Reserved.

# Legal Boundaries



# The Balancing Framework

Before collection begins, counsel should pressure-test the monitoring plan against six questions.

1. Purpose: security, compliance, misconduct, litigation, or HR?
2. Authority: policy, notice, consent, contract, law, or court order?
3. Scope: whose data, which systems, which time window?
4. Sensitivity: personal content, privileged material, biometrics, health, union activity?
5. Reliability: logs retained, time synced, tool validated, custodian documented?
6. Use: remediation only, discipline, regulator response, litigation, or prosecution?

(c) 2026 Lexeprint Inc. All Rights Reserved.

# Notice, Consent, and Transparency Are Not Boilerplate

The strongest evidence program starts before the employee exists in the investigation file.

### Policy layer

- Acceptable use and no/limited expectation of privacy
- Bring-your-own-device and personal-account rules
- Security monitoring disclosures at onboarding and annually
- Privileged / personal data escalation route

### Regulatory layer

- NY requires prior written notice for covered electronic monitoring
- California worker data rights now matter under CCPA/CPRA
- EU/GDPR and AI Act require transparency and lawful bases
- California AI framework restricts employers' use of AI workplace surveillance tools
- Colorado AI rules affect high-risk automated decisions

(c) 2026 Lexeprint Inc. All Rights Reserved.

# Reasonable Expectations of Privacy: The Quon Lesson

Workplace searches turn on purpose, scope, policy, and implementation facts.

## Case principle

- Public-employer electronic searches can be reasonable when motivated by a legitimate work-related purpose and not excessive in scope.
- Do not over-read Quon: the Court avoided sweeping rules for emerging communications technology.

## Practice translation

- Write policies that match real practice; informal manager assurances can muddy expectations.
- Collect the least intrusive data that can answer the work-related question.
- Separate business systems from employee personal accounts and devices.
- Ensure AI powered tools have undergone a legal review to identify data collected, inferences made, and tool capabilities.

(c) 2026 Lexeprint Inc. All Rights Reserved.

# Labor and Employment Risk: Surveillance Can Become the Claim

Monitoring may interfere with protected activity, wage-hour rights, or anti-discrimination laws.

### Section 7 / concerted activity

Monitoring that chills organizing or workplace-condition discussions may trigger NLRA issues.

### Wage-hour and scheduling

AI timekeeping, break tracking, scheduling, and productivity tools can create FLSA risk.

### Discrimination / retaliation

Risk scoring, productivity metrics, and automated flags can become adverse-action evidence.

### Disability and accommodation

AI tools assessing attention, response speed, or video presence may implicate accommodation obligations.

**Counsel should review both the collection practice and the downstream decision the data supports.**

(c) 2026 Lexeprint Inc. All Rights Reserved.

# AI-Driven Monitoring Raises a Different Evidentiary Problem

The question is not only “what did the employee do?” but “how did the system decide it mattered?”



## Legal asks

- What data trained or tuned the model?
- What features drove the score or alert?
- Who reviewed and overrode the result?
- Was the tool validated for the workforce and use case?

## Discovery asks

- Decision logs and model outputs
- Version history and threshold changes
- Vendor documentation and audit reports
- Adverse-action human review record

(c) 2026 Lexeprint Inc. All Rights Reserved.



# Evidence Discipline

# Digital Evidence Lifecycle for Insider Matters

Every step should be repeatable, logged, and explainable.




## Counsel controls the questions

- Define allegations and relevant period
- Identify data sources and custodians
- Preserve volatile data before imaging delays matter
- Document exclusions: personal, privileged, irrelevant, duplicative

## Forensics controls the proof

- Hash, time-zone normalize, and preserve originals
- Maintain chain-of-custody and tool/version notes
- Correlate logs across systems before drawing intent conclusions
- Separate artifacts from interpretations

(c) 2026 Lexeprint Inc. All Rights Reserved.

# Preservation Priorities: What Disappears First?

Legal hold language should track technical volatility.

| | |
|---|---|
| **Minutes to hours** | EDR alerts, active sessions, volatile cloud logs, ephemeral chat settings |
| **Days** | SSO/VPN logs, proxy events, DLP alerts, mobile telemetry |
| **Weeks to months** | Email, chat exports, shared-drive activity, HRIS, code repository events |
| **Longer-term** | Forensic images, retained backups, matter workspace, archived tickets |

(c) 2026 Lexeprint Inc. All Rights Reserved.

# Chain of Custody Is a Narrative, Not a Form

The record must show who touched the data, when, how, and why.



## Minimum record

- Custodian, system owner, data source, retention setting
- Collection method, tool, version, operator, date/time zone
- Hashes or integrity checks for exports/images
- Access controls for review workspace and evidence storage

## Common weaknesses

- Screenshots without source logs
- Exports altered by viewing or forwarding
- Unexplained time-zone conversions
- Missing exception logs and failed collection notes

(c) 2026 Lexeprint Inc. All Rights Reserved.

# The BYOD / Personal Account Trap

A company-owned device does not automatically make every open account a company evidence source.

### Personal email / messaging

- Stored Communications Act and state privacy risks; require legal review before access.

### BYOD / mixed-use device

- Ownership, consent, containerization, MDM scope, and family/member data matter.

### Cloud sync and browser profiles

- Local artifacts may point to external accounts the employer cannot lawfully enter.

### Privilege and counsel communications

- Screen for attorney-client and work-product material before wider review.

**Rule of thumb: preserve first, review lawfully second, and segregate sensitive material before HR or business review.**

(c) 2026 Lexeprint Inc. All Rights Reserved.

# Counsel-Directed Investigations and Privilege Discipline

Privilege is preserved by role clarity, purpose clarity, and circulation discipline.

## Structure

- Engagement letter defines forensic consultant’s role and counsel direction
- Investigation purpose documents legal advice and litigation-risk assessment
- Need-to-know distribution list for interim findings
- Separate business remediation from legal analysis where possible

## Watchouts

- Dual-purpose reports can invite privilege disputes
- Business-facing slide decks should avoid legal mental impressions
- Do not over-copy executives into tactical forensic workpapers
- Document non-testifying versus testifying expert transitions

(c) 2026 Lexeprint Inc. All Rights Reserved.



# Operational Playbook

# Insider Investigation Playbook: First 72 Hours

The first three days determine whether the matter stays controlled or becomes chaotic.

| | |
|---|---|
| 0–6 hours | Intake allegation; freeze destructive controls; preserve volatile logs; involve counsel; stop ad hoc review. |
| 6–24 hours | Define scope; issue targeted hold; collect critical logs; determine employee status and access risk. |
| 24–48 hours | Correlate identity, endpoint, network, and cloud artifacts; interview strategy; privilege screen. |
| 48–72 hours | Decide containment, discipline, regulatory notice, civil action, law enforcement, and litigation hold expansion. |

(c) 2026 Lexeprint Inc. All Rights Reserved.

# Policy Language That Survives an Incident

The goal is not maximal surveillance; it is defensible, documented authority.

### Notice

- Disclose categories of systems, purposes, timing, locations, and lawful means.

### Access control

- Define permitted use, prohibited exfiltration, personal account limits, and admin duties.

### Monitoring scope

- Explain security, compliance, operational, and investigative monitoring without promising constant review.

### Evidence use

- Reserve ability to preserve, collect, analyze, and disclose data for legal/compliance purposes.

### BYOD / personal data

- State what company can and cannot access; separate managed container from personal space.

### AI tools

- Disclose use of automated alerts and human review for significant employment decisions.

(c) 2026 Lexeprint Inc. All Rights Reserved.

# When Insider Monitoring Becomes Litigation ESI

Do not wait for discovery requests to decide how monitoring data will be searched and produced.

### Protocol topics

- Systems of record and log retention windows
- Custodians, shared accounts, admins, service accounts
- Time-zone normalization and deduplication rules
- Privilege and privacy redaction workflow
- Export format, metadata fields, and authentication method

### Negotiation leverage

- Explain proportionality with concrete data volumes
- Use sampling before broad forensic imaging
- Reserve phased discovery and clawback procedures
- Tie each source to claims/defenses and damages theory

(c) 2026 Lexeprint Inc. All Rights Reserved.

# Applied Hypothetical: Departing Engineer + DLP Alert

Use the framework to turn a messy fact pattern into a defensible plan.

## Facts

- DLP flags large download from source-code repository
- Employee gave notice 10 days earlier
- Files later appear in personal cloud-sync artifacts
- HR wants immediate termination
- Business wants counsel to “check the laptop and Gmail”

## Defensible response

- Preserve repo, SSO, VPN, endpoint, DLP, cloud logs
- Disable risky access; avoid content review beyond scope
- Review policy, notices, BYOD, and personal-account rules
- Forensically image work device if proportional
- Conduct privilege/personal-data screen before HR review

(c) 2026 Lexeprint Inc. All Rights Reserved.

# Governance Model: Who Owns What?

Legal needs clear lanes with Security, HR, Privacy, and IT.

| Legal | Security | HR | Privacy | IT |
| --- | --- | --- | --- | --- |
| Scope, privilege, hold, proportionality, use of evidence | Detection, containment, log preservation, tool validation | Policy enforcement, employee relations, discipline, accommodation | Notice, data minimization, cross-border, DSARs, sensitive data | System access, retention, export mechanics, MDM controls |

**No one function should be able to expand surveillance scope without a documented legal/business basis.**

(c) 2026 Lexeprint Inc. All Rights Reserved.

# Final Practitioner Checklist

The recurring theme: collect enough to prove the case, not so much that the collection becomes the case.

- ✓ Map monitoring tools and retention windows before incidents
- ✓ Update employee notices, acceptable-use policies, and BYOD terms
- ✓ Create a counsel-approved insider-threat evidence protocol
- ✓ Document purpose, scope, and minimization before content review
- ✓ Validate AI/analytics tools before using outputs for adverse action
- ✓ Preserve volatile logs and maintain chain of custody
- ✓ Use staged review with privilege/personal-data screens
- ✓ Translate technical findings into admissible evidence and human testimony

(c) 2026 Lexeprint Inc. All Rights Reserved.


Questions



**Daniel B. Garrie, Esq.**
Law & Forensics – Founder
JAMS – Neutral | Harvard – Faculty

**Contact:**
E: daniel@lawandforensics.com
W: https://www.linkedin.com/in/danielgarrie/

B.A., Computer Science, Brandeis Uni.
M.A., Computer Science Brandies Uni.
J.D., Rutgers School of Law

Daniel Garrie is the Co-Founder of Law & Forensics LLC, Head of Computer Forensics and Cyber Security Practice Groups and has been a dominant voice in the computer forensic and cybersecurity space for over 20 years. Prior to Daniel's legal career, he successfully built and sold several technology start-up companies. Since co-founding Law & Forensics LLC in 2008, Daniel has built it into one of the leading boutique cybersecurity forensic engineering firms in the industry. Daniel has both a Bachelor's and a Master's Degree in computer science from Brandeis University, as well as a J.D. degree from Rutgers Law School. Daniel has led forensic teams in some of the most visible and sensitive cyber incidents in the United States.

Daniel regularly testifies as an e-discovery, cybersecurity and computer forensic expert witness, authoring forensic expert reports on multi-million-dollar disputes. His ability to perform complex investigations and effectively communicate the results to a jury has made him one of the most sought-after experts in the country. His testimony has been pivotal in a number of cases. Since 2008, Daniel has served as a Neutral and Special Master and in 2016, he joined JAMS as one of the organization's youngest Neutrals. At JAMS, Daniel serves as an Arbitrator, Forensic Neutral, and technical Special Master with a focus on cybersecurity, cyrptocurrency, and complex software and technology related disputes.

Daniel is well-published in the cybersecurity space, Editor-in-Chief of the Journal of Law & Cyberwarfare, author of more than 200 articles and books including, "Understanding Software, the Internet, Mobile Computing, and the Cloud. A guide for Judges", published by the Federal Judicial Center. He has been recognized by several United States Supreme Court Justices for his legal scholarship and is a trusted source and a thought leader for cybersecurity articles and opinions, being cited over 500 times to date.



**Willie Session, PhD**
Chief Information Security Officer – Booking Holdings Financial Services

**Contact:**
E: willie.session@bookingholdingsfs.com
URL: https://www.linkedin.com/in/willie-session-phd-77358a6a/

Willie Session is a strategic cybersecurity executive and operational risk leader with a track record of aligning security programs with overarching business objectives. Holding a Ph.D. in Cybersecurity Leadership, Mr. Session partners with executive leadership and boards of directors to navigate complex regulatory landscapes, mitigate multifaceted enterprise risks, and build resilient security organizations.

Core Competencies:
Enterprise Risk Governance: Architecting and executing holistic strategies across cybersecurity, insider threat, fraud mitigation, third-party vendor risk, data loss prevention, and compliance.
Operational Leadership: Directing multidisciplinary teams spanning cyber & physical security operations, security engineering, threat monitoring, business continuity, and executive protection.
Financial & Cost Optimization: Conducting rigorous cost-benefit analyses to justify tech investments; notably drove a sustained reduction in annual security operating costs from $16.5M to $5.5M without compromising security control efficacy.
Regulatory Compliance & Assurance: Successfully leading organizations through high-stakes regulatory examinations, internal audits, and industry security assessments.
Continuous Modernization: Assessing enterprise-wide gaps to integrate emerging technologies, maintain alignment with regulatory shifts, and establish industry-leading security benchmarks.

Whether building scalable security foundations or scaling global operations, Mr. Session focuses on empowering high-performing teams, protecting critical enterprise assets, and enabling sustainable business growth.



**Ed Stroz**
Consultant

**Contact:**
E: nedstroz@gmail.com
URL: https://www.linkedin.com/in/edstroz/

Ed was the founder of the digital forensics firm, Stroz Friedberg, global leader in investigations, intelligence and risk management. He held the position of Co-President there from its start in 2000 to 2021. He sold the firm to Aon plc in 2016.
Ed oversaw the firm's growth and client development, while ensuring the maintenance of its distinctive culture. He also provided hands on strategic consulting in investigations, intelligence and due diligence, plus cyber and physical security. Before starting the firm, Ed was a Special Agent with the FBI where he formed their computer crime squad in New York.

Trained as a Certified Public Accountant, Ed has extensive experience in investigations of white-collar crime including bank fraud and securities fraud, and has testified in court numerous times as an expert witness.

Ed is a trustee of Fordham University, his alma mater, and serves as an advisor to the Center on Law and Information Policy (CLIP) at Fordham Law School. Ed sits on the Board of Directors of the Crime Commission of New York City, an independent non-profit organization focused on criminal justice and public safety policies and practices, and is a member of the Association of Former Intelligence Officers (AFIO). He served on the New York State Courts System E-Discovery Working Group, established to provide ongoing support and expertise to the New York State Judiciary in the area of e-discovery.

As a member of the National Association of Corporate Directors (NACD), in 2017 he earned the CERT Certificate in Cybersecurity Oversight from Carnegie Mellon University.



**Lawrence M. Hadley**
Partner—Glaser Weil Fink Howard Jordan & Shapiro LLC

**Contact:**
E: lhadley@glaserweil.com
W: www.glaserweil.com

Glaser Weil

Mr. Hadley is a Partner at Glaser Weil Partner and the Intellectual Property Chair. He is a highly skilled patent and trade secret first chair trial and appellate attorney who represents a wide range of technology-industry clients. In addition to patents and trade secrets, Larry has extensive experience in trademark and copyright law. He is well respected for vigorously and successfully representing clients going up against tech giants and is consistently sought after as a creative problem solver whose deep and broad knowledge of intellectual property law allows him to decisively counsel his clients through complex litigation and achieve precedent-setting results.

Larry has handled intellectual property and complex litigation cases involving computer hardware and software design, networking and wireless communications, medical devices, telecommunications and transportation. His proficiency in technology has led him to appear in trial and appellate courts across the country and before the United States International Trade Commission (USITC).