Seyfarth

The Modern Insider Threat: Shadow IT, BYOD, and Trade Secrets

February 19, 2026

Legal Disclaimer

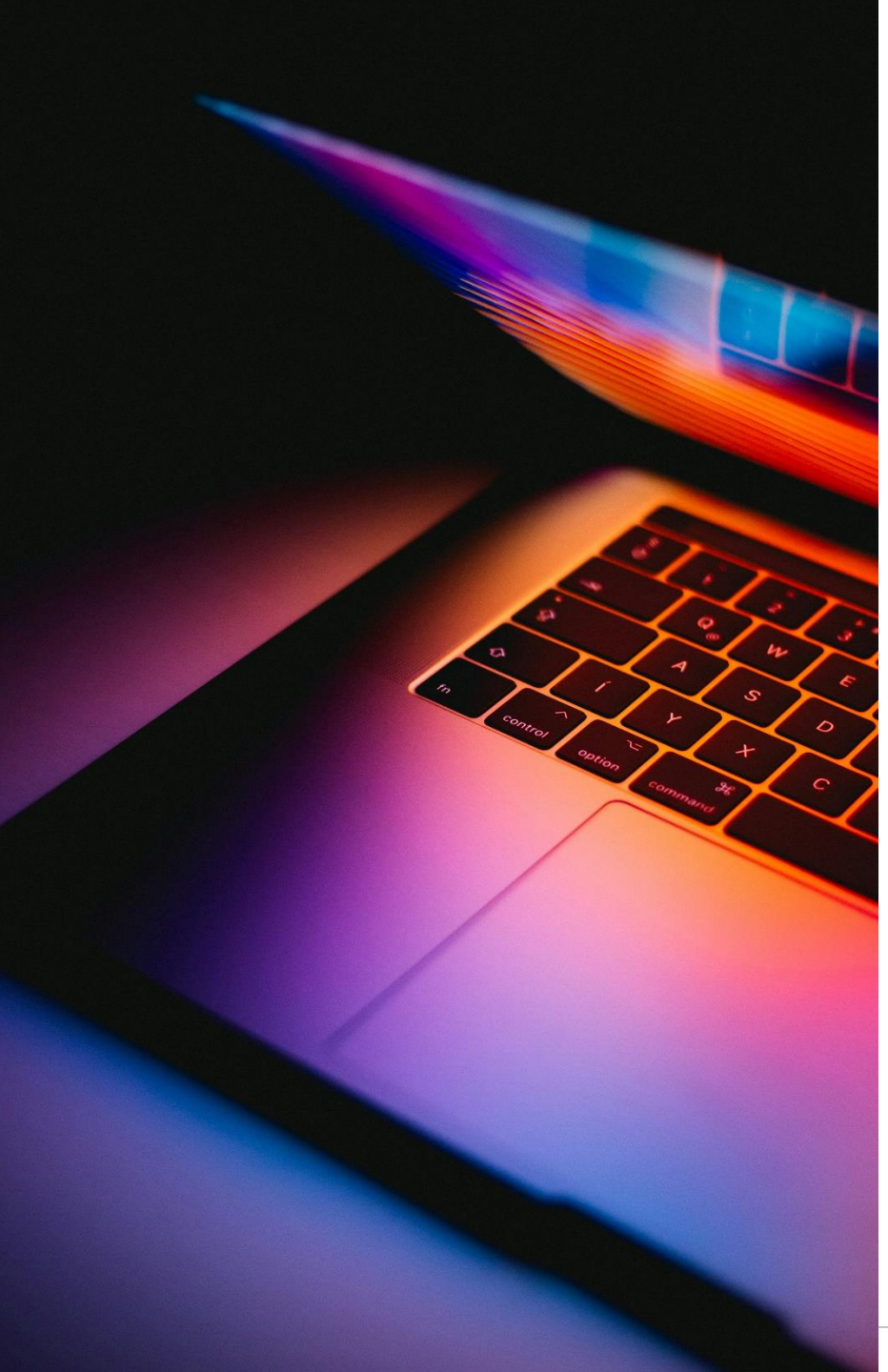
This presentation has been prepared by Seyfarth Shaw LLP for informational purposes only. The material discussed during this webinar should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The content is intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have.

Speakers

Matthew Catalano
Partner
New York Office

Peter Tsai
Counsel
New York Office

Danny Riley
Associate
Chicago Office



Agenda

1 | What Are We Really Talking About?

2 | Shadow IT and BYOD as Enterprise Trade Secret Risks

3 | The Modern Discovery Landscape

4 | Privacy, Security, and Information Governance

5 | Technical Controls and Organizational Strategy

6 | Key Takeaways

7 | Questions


What Are We Really Talking About?

Defining the Landscape

Shadow IT

- Use of applications, platforms, or tools outside formal IT approval
- Includes SaaS tools, messaging apps, AI tools, cloud storage, and personal devices
- Employees solving business problems faster than policy can keep up
- Often invisible to IT, Legal, and Security teams

BYOD

- Employees using personal phones, laptops, and tablets for work purposes
- Often intertwined with shadow IT rather than a separate issue
- Personal devices exist outside corporate-owned environments
- Reduced visibility, control, and enforceability over business data

Why This Matters Now

- **Remote and hybrid work normalization**
  - Work data now lives across personal devices, home networks, and unsanctioned cloud services
- **Explosion of collaboration tools and generative AI**
  - ChatGPT, Copilot, Slack, Teams, WhatsApp, Signal — employees adopt faster than policy can respond
- **Accelerated employee mobility**
  - Departing employees carry institutional knowledge on personal devices and accounts
- **Trade secret exposure, discovery blind spots, privacy and compliance conflicts**


Why Shadow IT
and BYOD
Are Now Trade
Secret Risks

Key Trade Secret Pressure Points

01

Blurred Boundaries

- No clear line between personal and business data on shared devices
- Personal cloud accounts commingled with work product
- Photo libraries containing screenshots of confidential documents

02

Inconsistent Enforcement

- Policies exist on paper but are not enforced in practice
- Executives exempt themselves from rules employees must follow
- Informal workflows become the real system of record

03

AI-Generated Work Product

- Source code created with AI tools raises IP ownership questions
- AI notetaking apps capturing meetings with confidential content
- Prompts containing trade secrets submitted to third-party LLMs

Real-World Shadow IT Incidents

AI TOOLS

Source Code Leaked to Generative AI

- Engineer uploaded proprietary source code to a publicly available generative AI chatbot
- Data stored on third-party servers with no retrieval or deletion path
- Company subsequently banned all generative AI tools at the workplace

MESSAGING

Unauthorized Messaging App Fines

- Financial services firms fined $1.1B in aggregate by regulators
- Employees used unauthorized messaging apps for official business
- Violated record-keeping and retention obligations

CLOUD STORAGE

Trade Secret Theft via Personal Cloud Accounts

- Engineer used personal cloud storage account to exfiltrate trade secrets
- Unvetted cloud platform created an invisible data pipeline outside corporate controls
- Highlights risk of shadow IT as a vehicle for IP theft

Shadow IT as Enterprise Risk

- **Shadow IT is the overarching problem**
  - Employees consistently find workarounds faster than corporate policy can adapt
- **BYOD as a major facet of shadow IT**
  - Personal devices are outside corporate-owned environments
  - Cost-benefit analysis: MDM, remote wipe, containerization, off-platform messaging policies
- **The effect of AI**
  - GenAI tools used for drafting, coding, and analysis create risk of trade secret ingestion, storage, or reuse by third-party platforms
  - *Company banned ChatGPT after an engineer accidentally uploaded proprietary source code; data stored on third-party servers with no way to retrieve or delete it*

Shadow IT, BYOD, and the Modern Discovery Landscape

BYOD By the Numbers

82%

of organizations report using BYOD

67%

of employees use personal devices for work

~70%

of BYOD devices in the workplace are unmanaged

$132B

global BYOD market size (2025 est.)

64%

of cybersecurity professionals cite data loss as top BYOD risk

62%

of companies rethinking or moving away from BYOD

Sources vary; figures compiled from industry surveys and market research.

Possession, Custody, and Control

- **What courts expect companies to preserve and produce**
  - Control without ownership: courts have found obligation to preserve data on employee personal devices
  - BYOD policies may expand or limit the scope of discoverable information
- **In re Pork Antitrust Litigation (D. Minn. 2022)**
  - Major food processing Company's BYOD policy limited ownership to company-synced data; court found employer did not control personal, un-synced data on employee devices
  - Remote wipe capability alone did not establish control over personal data
  - *But: court enforced subpoenas directed to individual employees for text message data except for the one employee who maintained a clear boundary against personal device use for work*
- **Westin v. DocuSign, Inc. (N.D. Cal. 2024)**
  - Court held that BYOD terms gave employer control to obtain employees' text messages concerning company information
  - Employees' BYOD agreements required them to search personal devices for company information when such devices were used for work purposes

Common Discovery Issues

- **Messaging platforms outside corporate control**
  - Text messages, WhatsApp, GroupMe, Signal, Telegram, Facebook Messenger, LinkedIn
- **Cloud drives and personal email**
  - Google Drive, Dropbox, iCloud — employees routinely sync work files to personal accounts
- **AI-generated work product**
  - AI copilot data, prompt history, AI-generated documents may be discoverable
  - Emerging case law around preservation obligations for enterprise AI tools

Privacy, Security, and Information Governance

Privacy and Governance Implications

Privacy Constraints

- Employee privacy expectations vary by jurisdiction
- Regional restrictions: EU (GDPR), UK, Asia-Pacific privacy regimes
- Monitoring employee personal devices raises significant legal questions
- GDPR fines up to €20M or 4% of global revenue for non-compliance

Governance Breakdowns

- No retention rules for unsanctioned tools
- Distinction between Records vs. Non-Records in retention policies
- “Shadow contracts”: employees accept click-wrap ToS, creating binding un-negotiated agreements without legal review
- Informal systems are hardest to defend in court

Security Gaps and Real-World Lessons

- **Data exfiltration without intent**
  - Employees inadvertently expose trade secrets through personal device syncing, AI tool usage, and unsanctioned cloud storage
  - *1 in 3 data breaches now involve shadow IT; average breach cost: $4.88M (2024)*
- **Lack of logging, monitoring, or audit trails**
  - Shadow IT tools operate entirely outside corporate visibility — no DLP, no SIEM, no forensic trail
- **SEC Fines (2022): Wall Street firms fined $1.1B in aggregate**
  - Employees used unauthorized messaging apps for official business, violating record-keeping and retention rules — a textbook shadow IT enforcement failure
- *Key theme: The more informal the system, the harder it is to defend in court and the more trade secret exposure it creates*


Technical Controls and Organizational Strategy

Technology Alone Is Not Enough

- **Policies without enforcement fail**
  - Executive text message spoliation examples demonstrate that even documented policies are insufficient without consistent application
- **Tools without governance create false confidence**
  - Deploying MDM or DLP without clear policies, training, and enforcement is insufficient
- **Organizational alignment is essential**
  - Legal, HR, IT, and Security must work from the same playbook
  - Clear escalation paths when shadow IT or BYOD issues arise

Examples of Effective Controls

DEVICE

Mobile Device Management

- MDM for corporate and BYOD devices
- Conditional access and identity controls
- Remote wipe capabilities
- Containerization of business data

PLATFORM

Approved Tools & AI

- Approved messaging and collaboration platforms
- AI governance framework with sanctioned tools
- DLP monitoring across approved channels
- Clear prohibition of unsanctioned tools for business use

PROCESS

Organizational Playbook

- Cross-functional coordination: Legal, HR, IT, Security
- Incident response procedures for data exposure
- Regular policy reviews and employee training
- Exit protocols for departing employees

A Practical Roadmap for Organizations

Identify High-Risk Roles

- Sales, engineering, executives, and data-heavy roles are highest risk
- Map which roles have access to trade secrets and sensitive data
- Assess current shadow IT and BYOD exposure
- Evaluate which unapproved tools are already in use

Establish Approved Frameworks

- Approved frameworks for messaging, collaboration, AI, and recording tools
- Account for regional realities (WhatsApp in Europe, local labor and privacy laws)
- Define governance tiers: corporate-owned, BYOD with MDM, prohibited use cases
- Balance cost, usability, and data protection

Measuring What Matters

- **Auditability**
  - Can your organization demonstrate what tools employees are using and where business data resides?
- **Preservation readiness**
  - If litigation arises tomorrow, can you preserve data across all platforms where business is actually conducted?
- **Compliance posture**
  - Are your policies consistent with your practices? Courts scrutinize the gap between written policy and actual enforcement.

Key Takeaways

1. Shadow IT and BYOD are not just IT problems — they are trade secret and litigation risks
2. The AI revolution has dramatically accelerated the speed and scale of potential exposure
3. Discovery obligations extend to data on personal devices and unsanctioned platforms
4. Privacy laws add complexity but do not excuse inaction on governance
5. Effective protection requires cross-functional alignment: Legal, HR, IT, and Security
6. Measure what matters: auditability, preservation readiness, and compliance posture


Questions?

thank you

Matthew Catalano
Email: mcatalano@seyfarth.com

Peter Tsai
Email: ptsai@seyfarth.com

Danny Riley
Email: driley@seyfarth.com

SCAN ME

CLE ATTENDANCE VERIFICATION FORM

Please scan the QR code to complete the digital attendance verification form to receive CLE credit for this program.

QR code directs you to our electronic form which can also be found in the calendar invite that was sent to you for this program.

You will need:

1. **Title:** The Modern Insider Threat: Shadow IT, BYOD, and Trade Secrets
2. **Date Viewed:** 02/19/26
3. **Attendance Verification Code:** SS3200

State-specific CLE credit information can be found in the form.