KEKER
VAN NEST
& PETERS

Preparing for Trade Secret Litigation in a New Age

March 26, 2025

Presenters

Rachael Meny
rmeny@keker.com

Ben Rothstein
brothstein@keker.com

Luke Apfeld
lapfeld@keker.com

Amy Philip
aphilip@keker.com

Agenda

- Trade Secret Overview
- Preventing Trade Secret Theft
- Identifying Trade Secret Theft
- What's New In Trade Secret Law

Trade Secrets Overview

Trade Secret Overview: What is a Trade Secret?

"Trade secrets are a peculiar kind of property. Their only value consists in their being kept private."

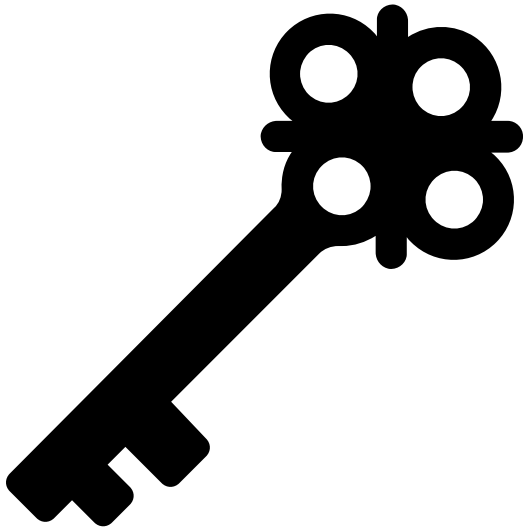
-- DVD Copy Control Ass'n v. Bunner, 31 Cal. 4th 864, 880 (2003) (citations omitted).

Statutorily Defined

Each statute is a little different, but generally, a trade secret is information that:

(1) Derives *independent economic value* from not being generally known,
(2) [cannot be *readily ascertained* by proper means], and
(3) is the subject of *reasonable efforts to maintain its secrecy*.

Trade Secret Overview: Common Trade Secrets



Software/Technology

- Source code and algorithms
- Internal-facing interfaces and workflows

Manufacturing / Biotech

- Recipes or materials information
- Manufacturing and quality control processes and steps

Finance

- Forecasts
- Non-public information re: investors, capital table

Sales/Marketing

- Customer lists and information
- Pricing strategies
- Product roadmaps for unreleased products

Trade Secret Overview: Negative Trade Secrets

"Negative" trade secrets:

- TS can be knowledge that a certain technology/procedure does not work

- But employees' **"general skill, knowledge, and experience" are not trade secrets** even if acquired due to employment. *Winston Research Corp. v. Minnesota Min. & Mfg. Co.*, 350 F.2d 134, 144 (9th Cir. 1965)

- Former **employees can be enjoined from using knowledge of the particular specifications** of former employer's machines – **but can't be expected to forget** "what not to do" and "how not to make the same mistakes" in developing similar machine at competitor's company *Winston Research Corp. v. Minnesota Min. & Mfg. Co.*, 350 F.2d 134, 144 (9th Cir. 1965)

Trade Secret Overview: Negative Trade Secrets

"Negative" trade secrets:

Waymo v. Uber – Judge Alsup allowed <u>one</u> alleged, negative trade secret to be tried

> The results of extended research, which proves that a certain process will *not* work, can qualify as an enforcible trade secret if all prerequisites for a trade secret are met. This type of information is sometimes called "negative know-how." By the same token, depending on the facts and circumstances, negative know-how might *not*, in a given case, qualify as an enforcible trade secret because, for example, it remains one of those practical on-the-job insights that augment the engineer's general skills and know-how, or can be found in the literature. It is for the jury, in each case, to determine whether negative know-how qualifies or not as a trade secret, applying the same test as for other know-how.

- *Nov 21, 2017 Revised Tentative Jury Instructions on Trade Secret Misappropriation*

Trade Secret Overview: Negative Trade Secrets

"Negative" trade secrets:

***Genentech v. JHL et al* – Judge Alsup argument re injunction**

Defense: [Plaintiffs] have the burden of putting in evidence that…JHL is using [a trade secret]…

Judge Alsup: No, see, that's an incorrect test. **"Is using it" is not the standard**. It could be that it's like negative knowhow … **They could use negative knowhow** in order **to save time** in order to come up with -- or they could look at what Genentech did, and said: Okay, they had a pretty good procedure, but…we're going to start with what they did and we're going to improve on it. So at the end of the day they're not using it. **They're using an improved version. But still, they used it to get there**. Listen. People go to prison for that.

February 2019 hearing

Preventing Trade Secret Theft

Preventing Trade Secret Theft

To win, Trade Secrets Must:

(1) Derive *independent economic value* from not being generally known,

(2) [not be *readily ascertained* by proper means], and

(3) **be the subject of *reasonable efforts*** *to maintain its secrecy*.

Preventing Trade Secret Theft

What is worth protecting as a Trade Secret?

- Define (or Know) Your Key Trade Secrets
- Identify Key Areas of Vulnerability *in advance*
- Treat as a Trade Secret
- Coca-Cola:
  - Kept in bank vault
  - BOD resolution to open vault
  - Only two people may know formula
  - They cannot fly on same plane
  - Identities protected

Coca Cola Bottling Co. of Shreveport, Inc. v. Coca Cola Co., 107 F.R.D. 288 (D. Del. 1985)

Preventing Trade Secret Theft

Take “Reasonable Efforts”

- Company Policies and Training
- Onboarding New Employees Properly
- Exiting Departing Employees Properly
- Other:
  - Confidentiality Agreements
  - IT/Digital Security
  - Physical Barriers
  - Labeling

Preventing Trade Secret Theft

Implement Policies & Procedures

- **Confidentiality Obligations**
  - Employment & separation agreements, handbooks, NDAs
- **Limit Work Activities to Company Devices & Applications**
  - Waive privacy as to employer-issued devices
- **Enforce Policies re: Company Devices/Applications**
  - Enforce no use of personal emails/applications
  - Prohibit deletion/destruction when leaving
  - Get them back or wipe them
- **Review & update regularly**
- **Involve Senior Management**

Preventing Trade Secret Theft

Train, Enforce, Train Some More

- **Regularly Repeat Confidentiality Obligations**
- **Remind of Limits on Work Activities via Company Devices/Applications**
- **Periodically Train & Track Compliance with Policies**
- **Consider What Should be Privileged (or not)**

Preventing Trade Secret Theft: “Reasonable Efforts”

Be careful of disclosures to:

- Regulatory Agencies (Home and Abroad)
- Manufacturing Partners
- Investors
- Business Partners
- Broader Industry Community
- Interview candidates

“Reasonable Efforts”: Onboarding Check List

- ✓ Standard system & forms
- ✓ Inquire re restrictive covenants from past position
- ✓ Careful job placement
- ✓ Admonish about use of past information
- ✓ Sign new agreements
- ✓ Train on your policies

Reasonable Efforts: Onboarding

Onboarding Practices

- **High-risk hires** – identify & act to prevent misappropriation risk *before* interview or start
- **Interviews** – use care when interviewing, especially with key competitors
- **Confirm no information** – ensure new hires confirm (in writing) they did not bring information & remind during onboarding
- **Employment Agreements** – clear provisions re confidential/trade secret information

Reasonable Efforts: High Risk Hires

When hiring out of state employees, pay close attention…

- What's allowed & required will differ state by state
- Some restrictions may be required for new job
- Former employer may sue outside of California
- CA courts may not interfere, even if CA case is filed first
  - *Medtronic, Inc. v. Sup. Ct.,* 29 Cal. 4th 697 (2002) ("[E]ven assuming a California court might reasonably conclude that the contractual provision at issue here is void in this state, this policy interest does not, under these facts, justify issuance of a TRO against the parties in the Minnesota court proceedings.")

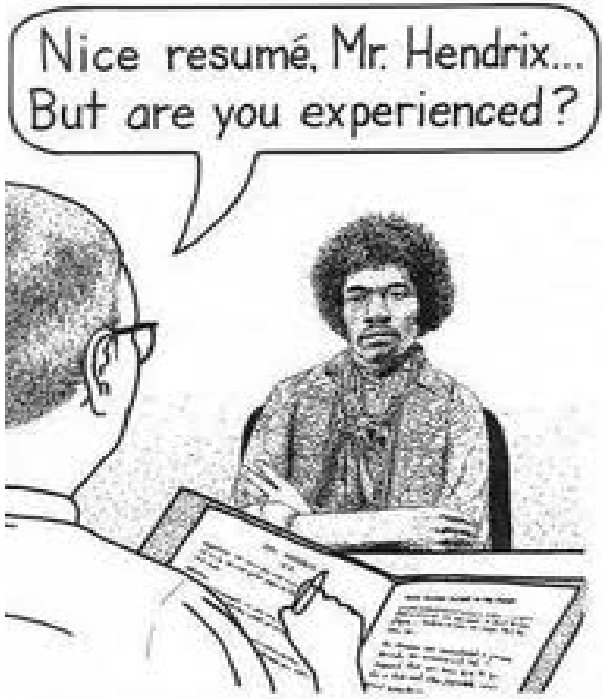
Reasonable Efforts: High Risk Hires

Pay attention to hidden non-CA law even when hiring employees from CA….

- Ask about:
  - Stock Agreement Provisions?
  - Acquisition Agreement Provisions?
  - Choice of Law Provisions?
  - Choice of Forum Provisions?
  - Where have they been working?

Reasonable Efforts: High Risk Hires

- Train interviewers on best practices because:
  - Interview comments / feedback aren't protected in litigation
  - Emails with or about candidate also unlikely to be protected



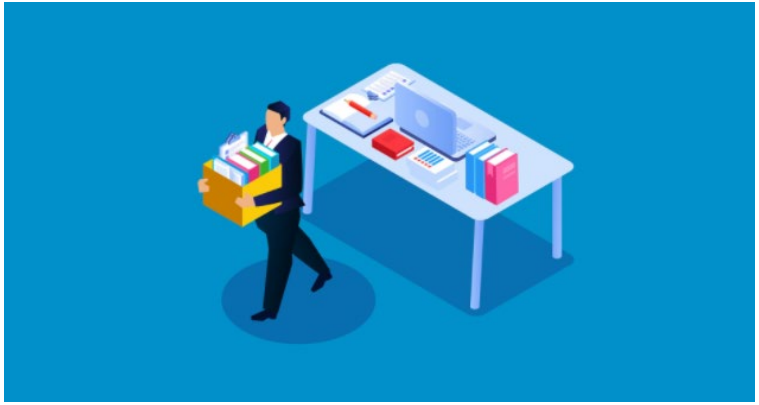
Reasonable Efforts: Confirm No Information

- Be extra vigilant about access to former employee documents on document platforms
  - Google Drive
  - iCloud Drive
  - Dropbox
- Documents may inadvertently be stored on local machines
- Personal and corporate drives get conflated/confused
- Personal drives can re-propagate on new devices

Preventing Trade Secret Theft: Offboarding

Offboarding Practices

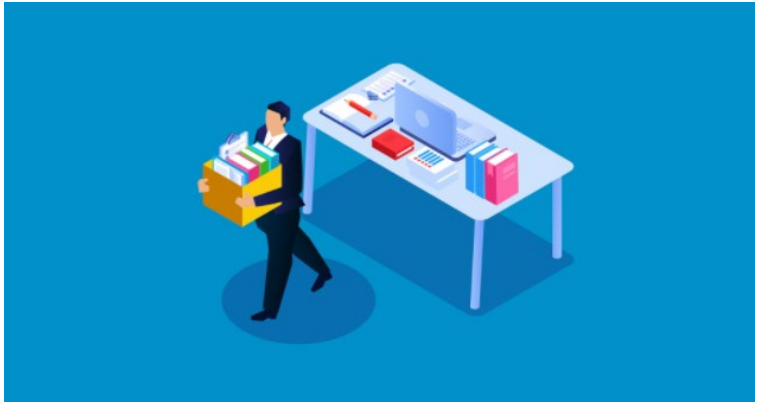
- Be Timely
- Have Exit Procedures
  - Checklist
  - Interviews
  - Signed Confirmations
- Remind of Obligations



Preventing Trade Secret Theft: Offboarding

Offboarding Practices

- Look for Misappropriation
- Follow up on Returned Documents/Equipment
- Preserve Returned Documents/Equipment if Questions

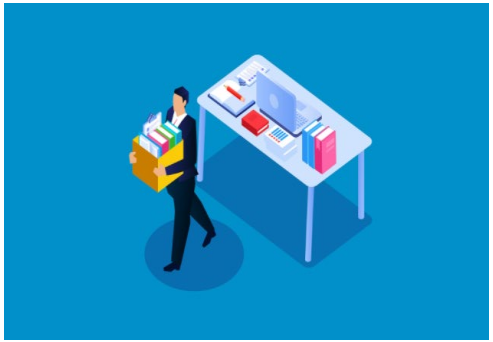


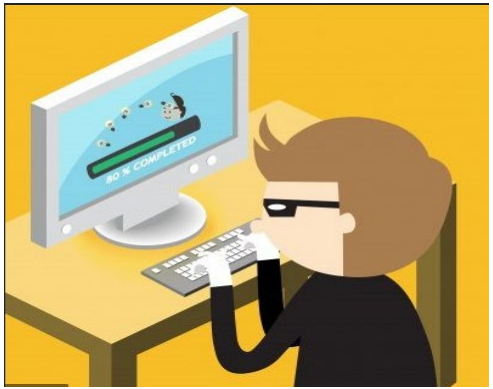
Identifying Trade Secret Theft

Identifying Trade Secret Theft

Confirm Suspicions

- Key Scenarios
  - Important employee(s) leave
  - Employee leaves on bad terms
  - Employee is hired by competitor
  - Layoffs/downsizing
  - Competitor develops a similar product

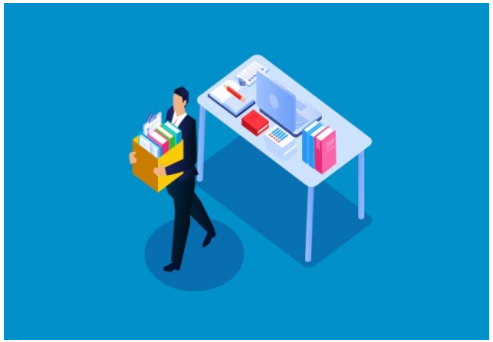


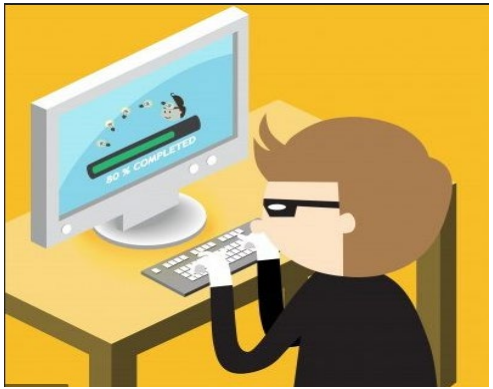


Identifying Trade Secret Theft

Confirm Suspicions

- **Investigation**
  - Physical access
  - Electronic access
  - Uploading/Downloading
  - Personal Accounts/Email
  - External drive use
  - Deletions before departure
  - Wiping software
  - Consider reach out(s)



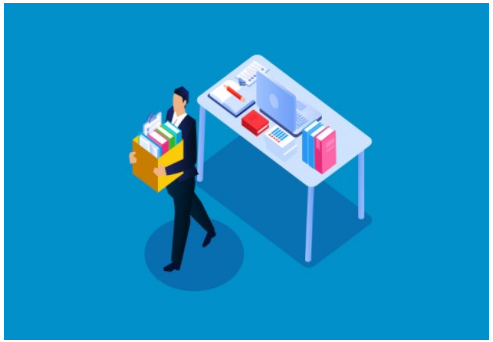


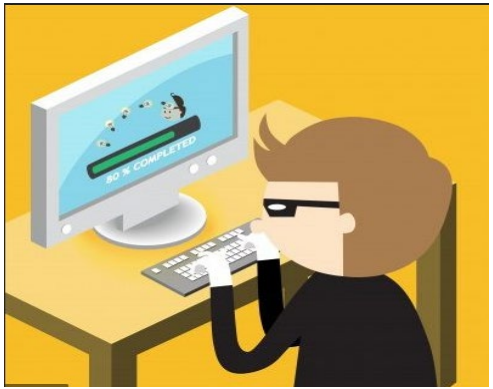
Identifying Trade Secret Theft

Confirm Suspicions

- **Plan for Potential Litigation**

  - Act promptly
  - Maintain privilege
  - Preserve what's needed
  - Interview witnesses
  - Send letters commensurate with findings



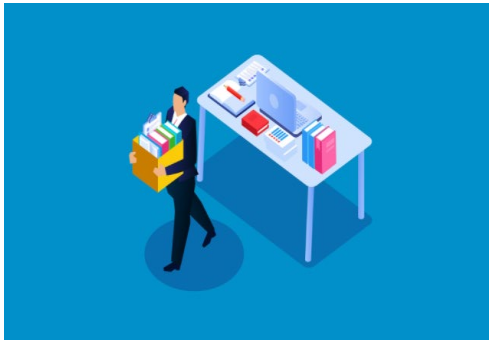


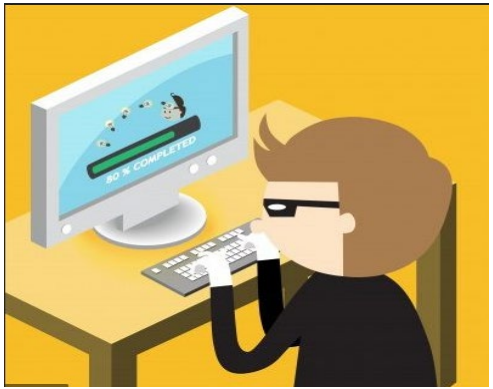
Identifying Trade Secret Theft

Confirm Suspicions

- **Plan for Potential Litigation**

  - Issue lit holds @ appropriate time
  - Consider who will testify
  - Consider who will give evidence of misappropriation





Identifying Trade Secret Theft

Referring matters to law enforcement

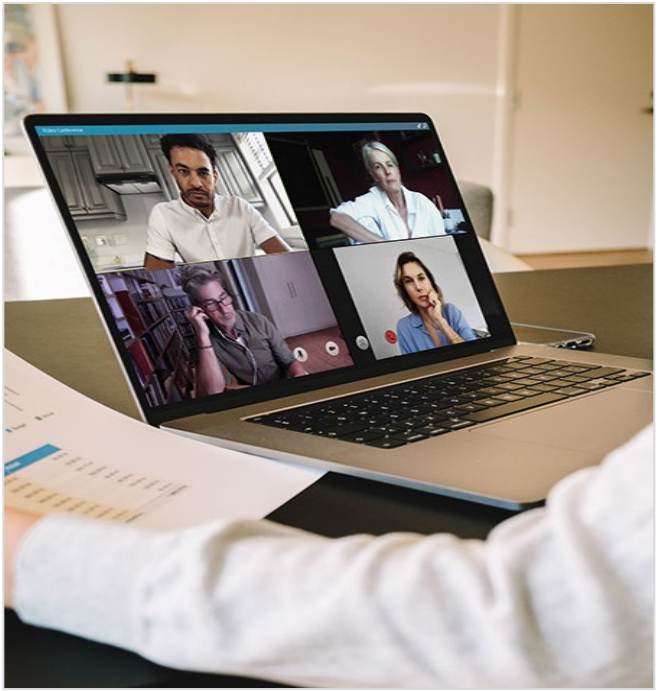
- Benefits
  - Powerful investigative tools
  - Important deterrent effect
- Disadvantages
  - Government timelines may be slower
  - Requires additional disclosure of trade secrets
  - Government investigation may require a lot of employee time

What’s New in Trade Secret Law

What's New In Trade Secret Law: 2024-25 Landscape

Workplace shifts and legal changes present new risks for companies.

- Exponential increase in ways to transfer data
- Massive increase in work-from-home and use of personal devices
- Increased use of AI
- Challenges to confidentiality provisions



What's New in Trade Secrets Law: The Cloud

Case Study 1: Former Google Software Engineer Indicted for Theft of AI Trade Secrets (N.D. Cal. 2025).

A former Google software engineer was indicted on seven counts of theft of trade secrets (and seven counts of economic espionage) by a federal grand jury in San Francisco on February 4, 2025.

The former Google employee, Linwei Ding, allegedly uploaded over 1,000 confidential files to his personal Google cloud account between May 2022 and May 2023, including trade secrets related to Google's AI technology.

What's New in Trade Secret Law: The Cloud

Cloud-based computing makes it harder for companies to protect trade secrets

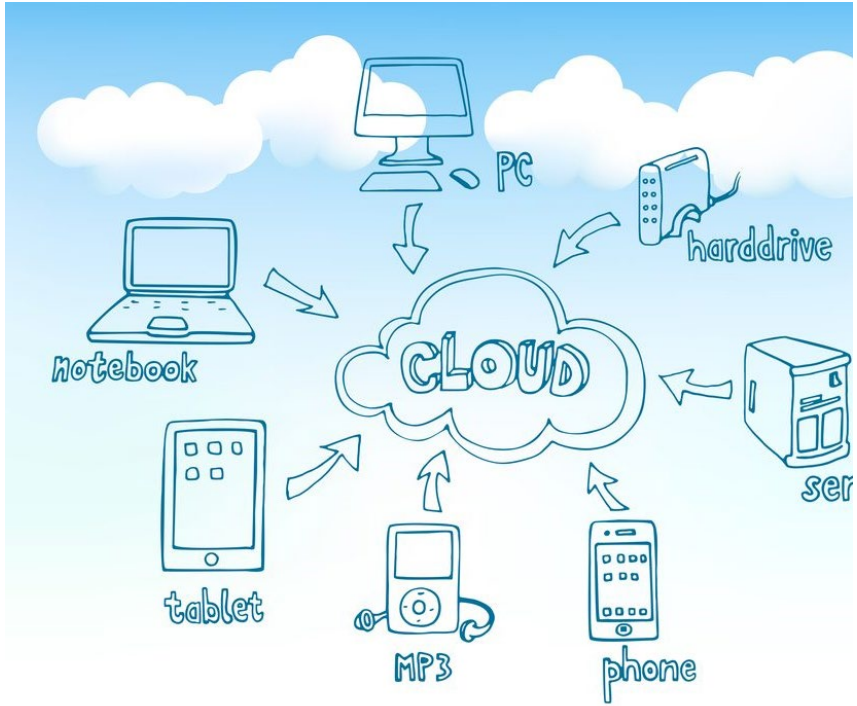
- Cloud computing makes it easy to share confidential documents and create local copies or downloads
- BYOD makes it harder to track potential misappropriation

What's New in Trade Secret Law: The Cloud

Implication of cloud-based computing on trade secret litigation

- Employees who inadvertently copy trade secret materials onto cloud accounts may still be liable for misappropriation if the information ends up on devices or systems of a new employer
  - *Apple v. Rivos,* WL 5183034, (N.D. Cal. 2003)
  - *CAE Integrated, L.L.C. v. Moov Techs., Inc.,* 44 F.4th 257, (5th Cir. 2022)

What's New in Trade Secret Law: The Cloud



Actions companies can take to minimize increased trade secret theft risk from cloud-based computing

- Require use of company-issued Apple or Google accounts
- Implement Data Loss Prevention (DLP) software
- Ask new employees to confirm existing cloud systems do not contain third party confidential information

What's New in Trade Secrets Law: Personal Devices

Courts may not deem allowing employees to use personal devices as "reasonable" trade secret protection

Patterson Dental Supply v. Daniele Pace et al., 2022 WL 18141871 (D. Minn. 2022)

What's New in Trade Secret Law: Personal Devices

- If allowing BYOD, create policies allowing company to examine BYOD devices used to access company resources

- Utilize exit interviews to ask employees about files existing on BYOD devices or personal cloud storage systems

What's New in Trade Secrets Law: Use of AI at Work

Case Study 2:

Two Nebraska-based technology companies sued a former salesman for trade secret misappropriation, alleging that the former employee (among other things) used an AI Meeting Assistant to record and transcribe confidential meetings, which was performed without consent of all participants.

West Technology Group LLC et al. v. Sundstrom, Case No. 3:24-cv-00178, U.S. District Court for the District of Connecticut.

What's New in Trade Secrets Law: Use of AI at Work

Case Study 3:

Samsung software engineering employees used ChatGPT to check and evaluate confidential company source code.

Even though this was used for purely internal purposes, ChatGPT does not know to distinguish between confidential and non-confidential information and uses any information inputted into the system to further optimize its algorithm.

These inputs are then available to be viewed by OpenAI or made accessible to other users.

What's New in Trade Secret Law: Use of AI at Work

Role and Impact of AI in Revealing Trade Secret Information

- AI's ability to identify patterns and make connections between unrelated data can assist in reverse engineering products or processes.
- AI's predictive capabilities, when combined with market data, research publications, and patent filings, can result in highly educated guesses about competitor trade secrets.

What's New in Trade Secrets Law: Use of AI at Work

Navigating Role and Impact of AI in Revealing Trade Secret Information

- Create limits around use of external AI programs or utilize in-house AI tools instead
- Invest in cybersecurity measures targeted towards AI
- Tighten NDAs and employee agreements
- Incorporate guidance on how to interact with AI in confidentiality agreements
- Train employees on the risks of trade secret exposure because of AI

KEKER
VAN NEST
& PETERS

Thank you!