# AI and the Defend Trade Secrets Act (DTSA):

## Investigating and Litigating Stolen IP


Henry M. Sneath

Shareholder/ IP & Litigation Practice Chair

Houston Harbaugh, P.C.

Adjunct Professor – Trade Secret Law

Kline School of Law of Duquesne University

Corey A. Bauer

Shareholder

Houston Harbaugh, P.C.


# The Current State of AI – According to Claude.AI "AI in 2024: Key Insights"

- **Improved Reasoning Capabilities**
  - More sophisticated contextual understanding
  - Enhanced ability to break down complex problems
  - Increased nuance in language comprehension
- **Ethical and Regulatory Challenges**
  - Growing global discussions about AI governance
  - Emerging frameworks for responsible AI development
  - Heightened focus on potential societal impacts
- **Technological Advancements**
  - Continued improvements in model performance
  - Expansion of AI applications across industries
  - Increased computational efficiency
  - More sophisticated machine learning architectures
- **Critical Considerations**
  - Ongoing debates about AI safety
  - Transparency and explainability of AI systems
  - Potential economic and workforce transformations
  - Balancing innovation with responsible development

# Hey Claude - How will AI affect the legal profession?

- AI will augment, not replace, legal professionals by enabling more strategic, high-value work.
- AI is a powerful tool that amplifies human legal expertise, not a replacement for professional judgment, empathy, and complex reasoning.
- Lawyers who effectively integrate AI will gain significant competitive advantages in delivering more efficient, precise, and strategic legal services.*

**** Claude is bullish on the impact***

# Claude – what are critics of AI saying about the negative impact of AI on the legal profession?

- Ethical and Professional Risks
  - Potential bias in AI decision-making
  - Loss of human judgment and nuance
  - Reduced accountability for legal outcomes
  - Erosion of professional discretion
- Technical and Accuracy Concerns
  - Over-reliance on potentially flawed AI systems
  - Inability to fully comprehend complex legal contexts
  - Risk of perpetuating existing legal biases
- Confidentiality and Security Risks
  - Data privacy vulnerabilities
  - Potential breaches of attorney-client privilege
  - Cybersecurity threats
  - Unauthorized data mining

- **Fundamental Profession Transformation**
  - Diminished role of human interpretation
  - Over standardization of legal approaches
  - Potential reduction in creative legal strategies
  - Loss of empathetic client interaction
  - Potential failure to maintain competence in the tech (Rule 1.1)

# ABA Model Rule 1.1: Comment

- Maintaining Competence
  - [8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice**, including the benefits and risks associated with relevant technology,** engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject

# AI and The Practice of Law

- Using phone or Chrome;
- Using Westlaw or Lexis;
- AI generated evaluation of briefs;
- Forensic investigation;
- Document searching and production;
- Enhanced writing;
- Use of form documents;
- Hiring and job searching;
- Gathering evidence in tech and IP cases;
  - –Seizure of devices and data;
- Presentation of evidence;
  - –Who is the actual expert?
- Scene or accident recreations in civil and criminal case;
- Tech demonstration in IP patent cases;
- Certification of research;
- Court mandated rules on certification of human involvement.

# What is the DTSA?

- Amendment to the Economic Espionage Act (EEA) in 2016
  - EEA Carries criminal penalties for trade secret theft.
    - Can face forfeiture, fines and up to ten years imprisonment (much higher fines and 15 years if for a foreign entity)
  - DTSA provides a private civil action.
    - Also allows for *ex parte* seizure of private property.
    - Shares the definition of a "trade secret" with the EEA
- Until the DTSA, trade secret litigation was limited to state courts at common law or adopted version of the Uniform Trade Secrets Act (UTSA)
  - Every state other than NY and North Carolina has adopted some form of the UTSA

# When Will A Court Allow for an *Ex Parte Civil* Seizure?

The DTSA allows a court to issue an *ex parte* seizure of property "only in extraordinary circumstances."

To show "extraordinary circumstances," the DTSA requires the plaintiff to:

- Describe with reasonable particularity what is to be seized and where it is located;
- Not publicize the requested seizure; and
- Provide security for any damages the defendant or related third parties may suffer if the court later determines that the seizure was wrongfully granted.
- A plaintiff must also prove that the defendant would "evade, avoid, or otherwise not comply with" an order for other injunctive relief, like a temporary restraining order (TRO) under Rule 65 of the Federal Rules of Civil Procedure.
- Notably, a plaintiff is ***assumed*** to have specific knowledge about the defendant to describe with reasonable particularity the extraordinary circumstances that exist.

# Elements of DTSA Claim

There are four key elements to any civil claim brought under the DTSA:

- (1) the information **must be a trade secret**;
- (2) the **owner** of the trade secret must bring the claim;
- (3) the trade secret must involve goods or services used in interstate or foreign commerce; and
- (4) the information must have been misappropriated.

# Elements of EEA Trade Secret Theft

There are two subsections of the EEA criminalizing the theft of trade secrets:

- 18 U.S.C. § 1831, prohibits the theft of trade secrets for the benefit of a foreign government, instrumentality, or agent. A breach of § 1831 requires the government to prove four things:
- (1) the defendant stole, or without authorization of the owner, obtained, destroyed or conveyed information;
- (2) the defendant knew that this information was proprietary;
- (3) the information **was a trade secret**; and
- (4) the defendant knew that stealing the information would benefit, or was intended to benefit, a foreign government, instrumentality, or agent.

- The second provision, 18 U.S.C .§ 1832, criminalizes the theft of trade secrets for the benefit of someone other than the owner of the trade secrets. To establish a violation of § 1832, the government must prove:
- (1) the defendant stole, or without authorization of the owner, obtained, destroyed or conveyed information;
- (2) the defendant knew this information was proprietary;
- (3) the information **was in fact a trade secret**;
- (4) the defendant intended to convert the trade secret to the economic benefit of anyone other than the owner;
- (5) the defendant knew or intended that the owner of the trade secret would be injured; and
- (6) the trade secret was related to or was included in a product that was produced or placed in interstate or foreign commerce.

# What is a trade secret?

The most important point of proof (regardless of whether the DTSA or EEA is implicated) is that there exists an actual **Trade Secret**:

- EEA definition: "the term **'trade secret'** means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if. . ."

# What is a trade secret?

The most important point of proof (regardless of whether the DTSA or EEA is implicated) is that there exists an actual **Trade Secret**:

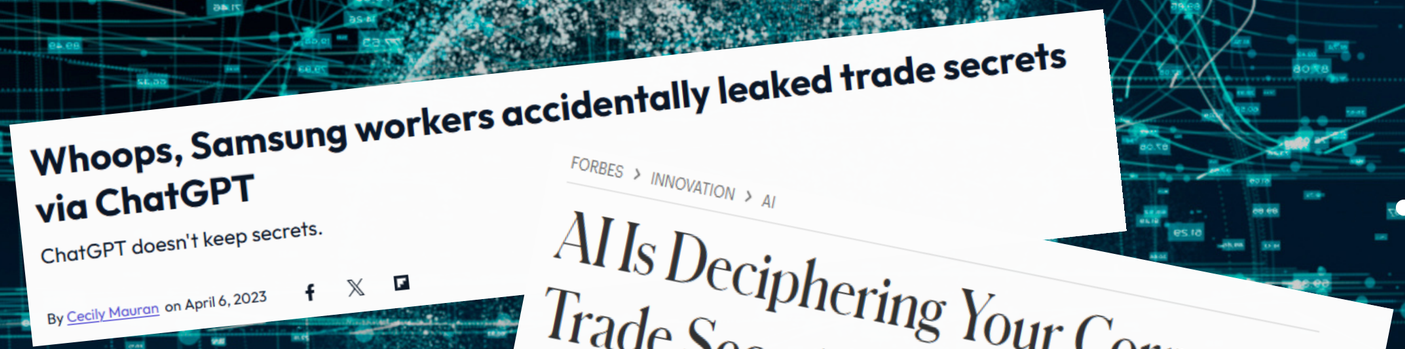
- Owner of the trade secret has taken **reasonable measures** to keep such information secret, and;
- And the protected information **"derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by another person** who can obtain economic value from the disclosure or use of the information"
- **In other words, it must actually be a SECRET.**

# Misappropriation per the DTSA

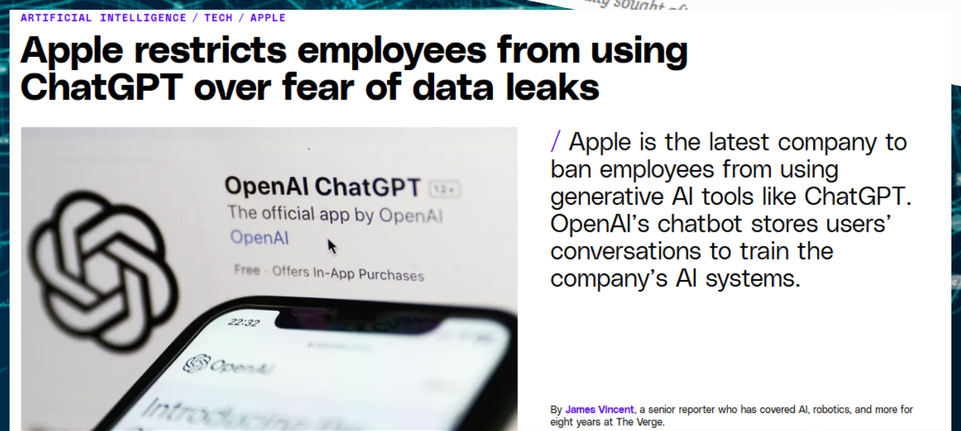
- the term “misappropriation” means—
  - (A) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or
  - (B) disclosure or use of a trade secret of another without express or implied consent by a person who—
    - (i) used improper means to acquire knowledge of the trade secret
- Does not include
  - Independent invention/reverse engineering;
  - License from the owner;
  - Observation from public display or use;
  - Obtaining from published literature.

# Questions about the DTSA or EEA?

# GenAI Has Caused Inadvertent Disclosure of Trade Secrets








- Companies are adopting GenAI for business purposes without consideration to use licenses .
- This can cause the inadvertent disclosure of trade secrets to the GenAI machine learning algorithm.
- Samsung reportedly leaked trade secret source code and meeting minutes to ChatGPT **three times.**

# What This Means for The Discovery Process

- Plaintiff's use of GenAI by employees should be investigated thoroughly:
  - Does the plaintiff or company asserting theft use GenAI as part of its business processes?
  - Does the company have a GenAI policy?
    - When was it introduced?
    - Did it have a policy against the use of GenAI at the time of the alleged theft?
    - Before the alleged theft?
  - Do they have an Enterprise License or End-User License Agreement restricting collection of their data for training?
  - Does the company monitor employee prompts and GenAI outputs? If so, get them.
  - Should you subpoena the GenAI provider they use? Microsoft, Google, OpenAI, etc.?

# AI and the Investigation of Trade Secret Cases

- Given the complex nature of trade secret cases, there are often many documents produced between the parties or disclosed by the Government.
- Parties also need to be aware of the need for digital forensics and preservation. Generally speaking, the following must be followed:

Step 1: Identify and analyze all hardware and software with potentially relevant data.

Step 2: Notify all potential parties of their duty to preserve documents and data in said hardware and software.

Step 3: Hire a third party digital forensic team (like BitxBit) to perform a collection and analysis of all relevant data.

What do you do with all of these newly collected documents?

**Use AI, of course.**

# About Predictive AI Document Review

- Not a new technology (has been offered commercially since 2009);
  - Only checked for relevance and coded documents based upon the control group;
- Around 2012, the adaptation by the program became continuous (it learned as the review proceeded);
- After that (2016-2017), the programs developed to be less reliant upon control sets and improved continuous learning;
- Today, the programs utilize random sample guides and elusion-based quality control samples;
- Production can be in the many millions of pages of data

# Active Learning Project

Project Home | Review Statistics

| Project Size | Coded Responsive | Coded Non-Responsive | Skipped |
|---|---|---|---|
| | 64 manually-selected | 91 manually-selected | |
| 52,232 | 1,002 | 1,071 | 21 |

**Prioritized Review**

Coded: 1,928 (21 Skipped)
Docs Remaining: --
Active Reviewers: 101 (Add Reviewers)

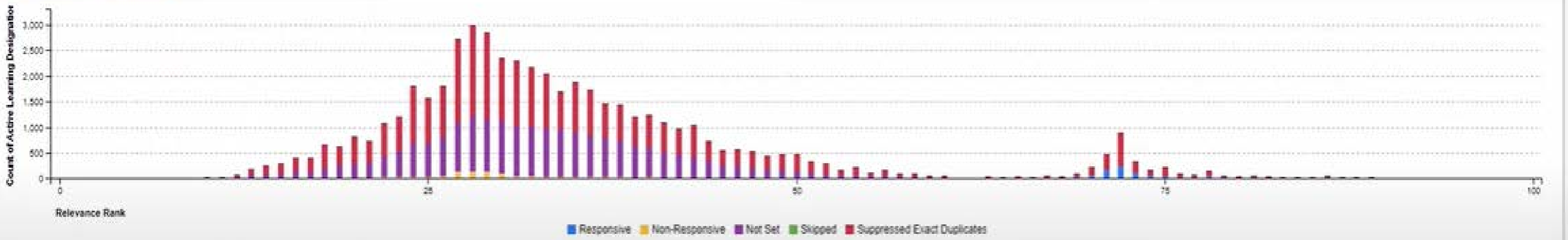
Pause Review

**Elusion Test**

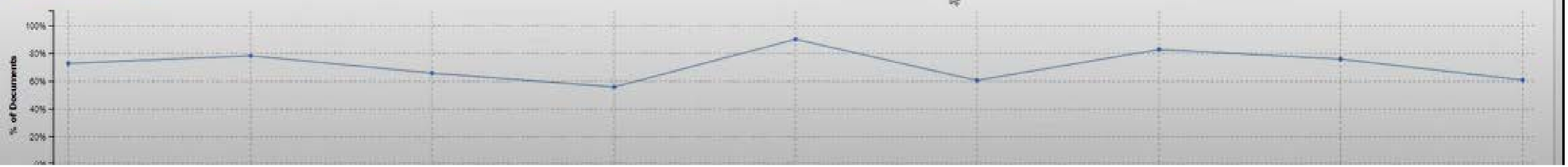
Active Reviewers: 0 (Add Reviewers)

Start Review

## Document Rank Distribution




## Prioritized Review Progress

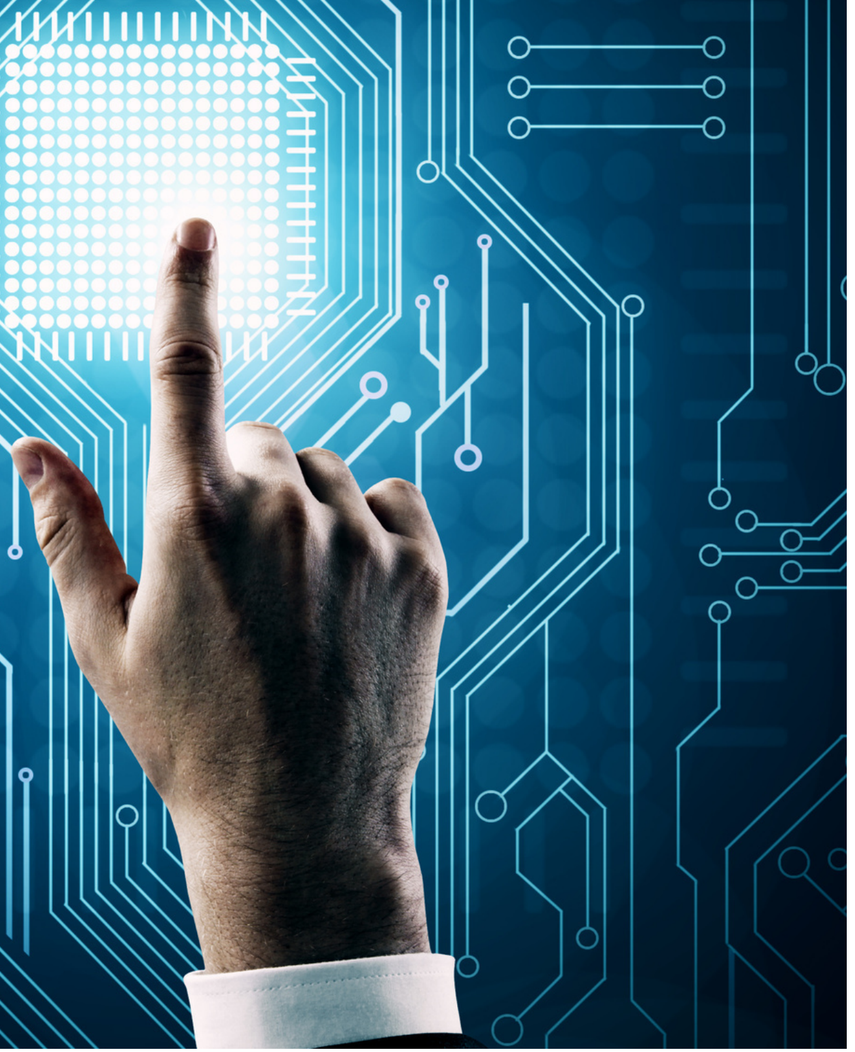


# ELUSION TEST

$$\frac{p + \frac{z^2}{n}}{1 + \frac{z^2}{n}} \pm \frac{z}{1 + \frac{z^2}{n}} \cdot \sqrt{\frac{p(1-p)}{n} + \frac{z^2}{4n^2}}$$

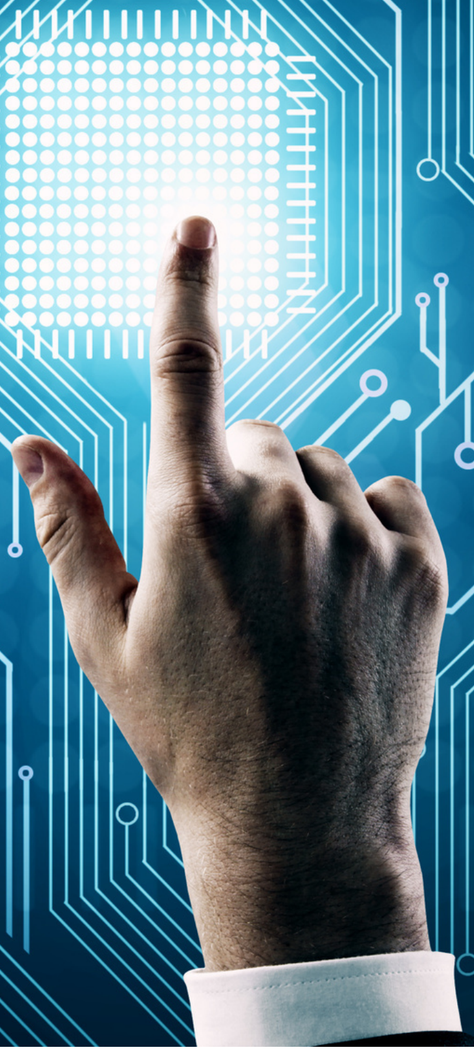
# What is an Elusion Test?

- Test for how many responsive/relevant document **eluded** you;
- Once reviewers stop getting responsive documents fed to them by the algorithm, you take a random sampling of documents from the null set;
- Have an attorney review the random sampling from the null set for responsiveness;
- The elusion test result is the percent of documents marked as responsive from the population that was sampled;
- Equation is the likelihood of responsive documents remaining in null set
- If zero or few sampled documents are found to be responsive, then the results may be considered valid and you will be able to make a strong case for discarding the null set.



# Certification to the Court and Evidence

- These processes can be challenged in court by opposing counsel;
- There must be a preservation of data trail to be able to convince a court that the searching reached a certain level of confidence in the search;
  - Perhaps 95% “Confidence” level in the results of the Elusion Test;
- There are special masters appointed in court to preside over discovery disputes and the forensic document vendors must sometimes file affidavits regarding thoroughness of searches.



# People Are Also Using AI to Steal Trade Secrets

AI is better than any human at identifying patterns in large swaths of data- even when that data may seem to be unrelated.

Bad actors are using AI to review patent filings, scientific publications, and corporate filings to reconstruct or “reverse-engineer” the methods or formulas that companies consider to be trade secret.

Trade secrets can me a compilation of many public data sets. The unique combination and/or use of that public data can be a trade secret – those are especially susceptible to this new kind of corporate espionage.

See the Forbes article in materials.


Questions about anything at all?

# THANK YOU

Houston Harbaugh
ATTORNEYS AT LAW


Henry M. Sneath
Shareholder
Practice Chair of IP & Litigation

Corey A. Bauer
Shareholder