KEKER
VAN NEST
& PETERS

# Trade Secrets in the Life Sciences: Litigation Strategies for a High-Stakes Industry

Association of Corporate Counsel
March 12, 2026

# Introduction

**Laurie Mims**
Keker, Van Nest & Peters
lmims@keker.com
(415) 676-2227

**Cody Harris**
Keker, Van Nest & Peters
charris@keker.com
(415) 676-2294

# Agenda

**Trade Secret Basics**

**Trade Secret Litigation**

**Case study:**
***Genentech v. JHL***

**Current Challenges in Protecting Trade Secrets**

**Questions?**

# 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*.

# What is a Trade Secret?

## Very broad definition

A wide variety of information in the life sciences sphere has been found to be a trade secret, including:

- **Testing protocols, procedures, and test results**
- **Manufacturing methods and techniques**
- **Formulas and specifications**
- **Product road maps**
- **Pricing information and sales data**
- **Negative know-how**

# What is a Trade Secret?

## Negative know-how in practice:
## *Genentech v. JHL et al* (ND Cal) – February 2019 hearing

JHL attorney: [Plaintiffs] have the burden of putting in evidence that whatever they've identified as a specific trade secret qualifies as a trade secret, and that JHL is using it…

Judge Alsup: No, see, that's an incorrect test. "Is using it" is not the standard. It could be that it's like negative know-how … They could use negative know-how 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 improve on it, 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.

JHL attorney: And that may qualify as misappropriation. But that doesn't give them a basis for an injunction. To get an injunction –

Judge Alsup: Yes, it does. Where do you get that idea? … Because you steal their stuff and then you get a head start, and now you're saying: Well, we're doing something even better, we don't need -- well, yeah, but you wouldn't even be there if you hadn't taken their stuff and gone to school on it.

# What is a Trade Secret?

## A trade secret may be a compilation of otherwise public information

"[W]hile the SOPs may include some public information, there is no evidence that [they] are simply wholesale copies of public information. There is also evidence suggesting that AllCells invested at least some time and research in deriving specific steps, formulations, etc. in producing the SOPs. This is not to say that Defendants will not have meritorious arguments on some or all of the SOPs—if, e.g., they merely reflect information already known in the industry or were simply small 'tweaks' of publicly available SOPs and were thus effectively generally known. But at this juncture in the proceedings, AllCells has met at least the lesser standard of serious questions going to the merits."

*AllCells, LLC v. Zhai*, No. 16-CV-07323-EMC, 2017 WL 1173940, at *3 (N.D. Cal. Mar. 29, 2017).

# Protecting Your Trade Secrets

## Taking “reasonable efforts”

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

# Taking “Reasonable Efforts”

## Consider ramifications of disclosures to:

- Regulatory agencies (at home and abroad)
- Manufacturing partners
- Broader scientific community (patents, presentations, or publications)
- Customers/Doctors/Patients

# Protecting Your Trade Secrets

## Confirming suspicions: the investigation

- Physical access
- Electronic access
- Flashdrive use
- Wiping software
- Preservation
- Interviews

# Elements of Trade Secret Misappropriation

## Plaintiff must prove that:

(1) the plaintiff owned a trade secret,

(2) the defendant acquired, disclosed, or used the plaintiff's trade secret through improper means, and

(3) the defendant's actions damaged the plaintiff.

*Sargent Fletcher, Inc. v. Able Corp*., 110 Cal. App. 4th 1658, 1665 (2003).

# Trade Secret Statutes

## Several laws barring trade secret theft:

(1) CUTSA (California Uniform Trade Secret Act)

(2) UTSA (Uniform Trade Secret Act – may vary by state)

(3) DTSA (Defend Trade Secrets Act – federal law)

(4) 18 U.S.C. § 1832 (Economic Espionage Act - criminal theft of trade secrets)

(5) 18 U.S.C § 1030 – CFAA (Computer Fraud and Abuse Act)

(6) CDAFA (California Computer Data Access and Fraud Act)

# Identifying Your Trade Secrets

## Trade secret identification

- Under CUTSA
  - CCP § 2019.210:  pre-discovery identification of trade secrets with "reasonable particularity" – no discovery at all before this is done.
  - A plaintiff must identify with particularity to get discovery or to obtain a preliminary injunction.
  - A plaintiff need not identify trade secrets with particularity in its complaint, or to survive a demurrer.
- Frequent litigation around whether the identification is sufficient.

# New Development: Lower Identification Threshold

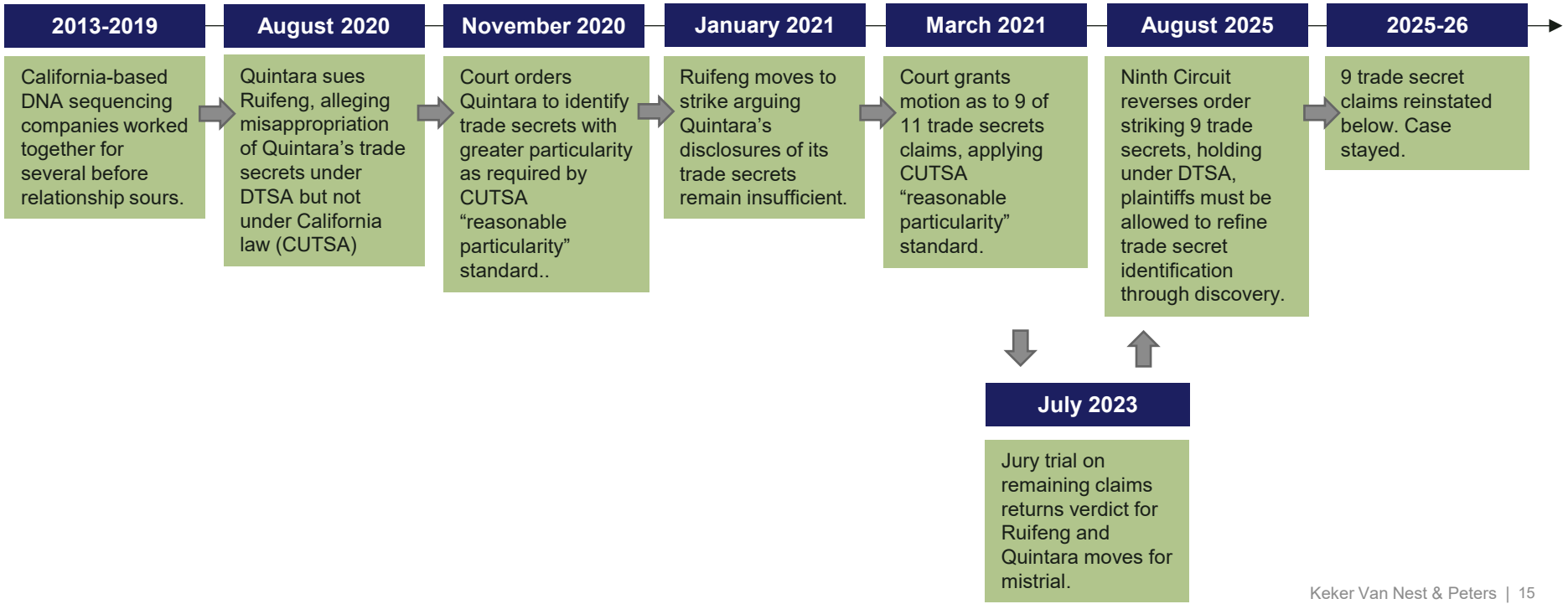
## Pre-2025 Legal Landscape

- Non-California courts may apply CUTSA's trade secret disclosure standards as a case management tool in non-CUTSA cases. *Savor, Inc. v. FNR Corp.*, 2002 WL 393056 (Del Super. Ct. 2002).
- Under CUTSA, plaintiff must make pre-discovery identification of trade secrets with "reasonable particularity" – no discovery at all before this is done. CCP § 2019.210

## 2025 and Beyond: Federal Law Diverges from CUTSA Standard

# *Quintara v. Ruifeng Biztech*

## Overview: litigation timeline



# New Developments: Lower Identification Threshold

## Ninth Circuit's holding

- Stressed that DTSA does not require a plaintiff to identify trade secrets with particularity at the outset. Whether a claimed trade secret is described with "sufficient particularity" is a question of fact, typically resolved at summary judgment or trial.
- Emphasized that trade secret cases require balancing the plaintiff's need to prove its claims without prematurely revealing sensitive information against the defendant's need to understand the scope of the claims to prepare a defense. Courts have multiple tools, including Rule 16 scheduling orders, Rule 26 protective orders, and sequencing of discovery, to manage this "delicate problem" without prematurely terminating claims.

# New Development: Lower Identification Threshold

## *Quintara's* implications for federal cases

- Plaintiffs filing in California will want to consider whether they want to bring a CUTSA case at all, given that statute's strict "reasonable particularity" standard.
- Whether procedural requirements of Section 2019.210 apply in federal court at all is unresolved.

# Taking Action

So, you've protected your trade secrets, you've investigated suspected misappropriation, and you've identified the specific trade secrets at issue.

## 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

# Trade Secret Litigation

## Civil remedies

- Injunctive Relief
- Monetary Damages
  - Actual loss
  - Unjust enrichment
  - Reasonable royalty
  - Exemplary (2x damages)
- Key Question: How to value the misappropriated trade secret?
  - Lost profits?
  - Head-start?

# Injunctive Relief: TROs and PIs

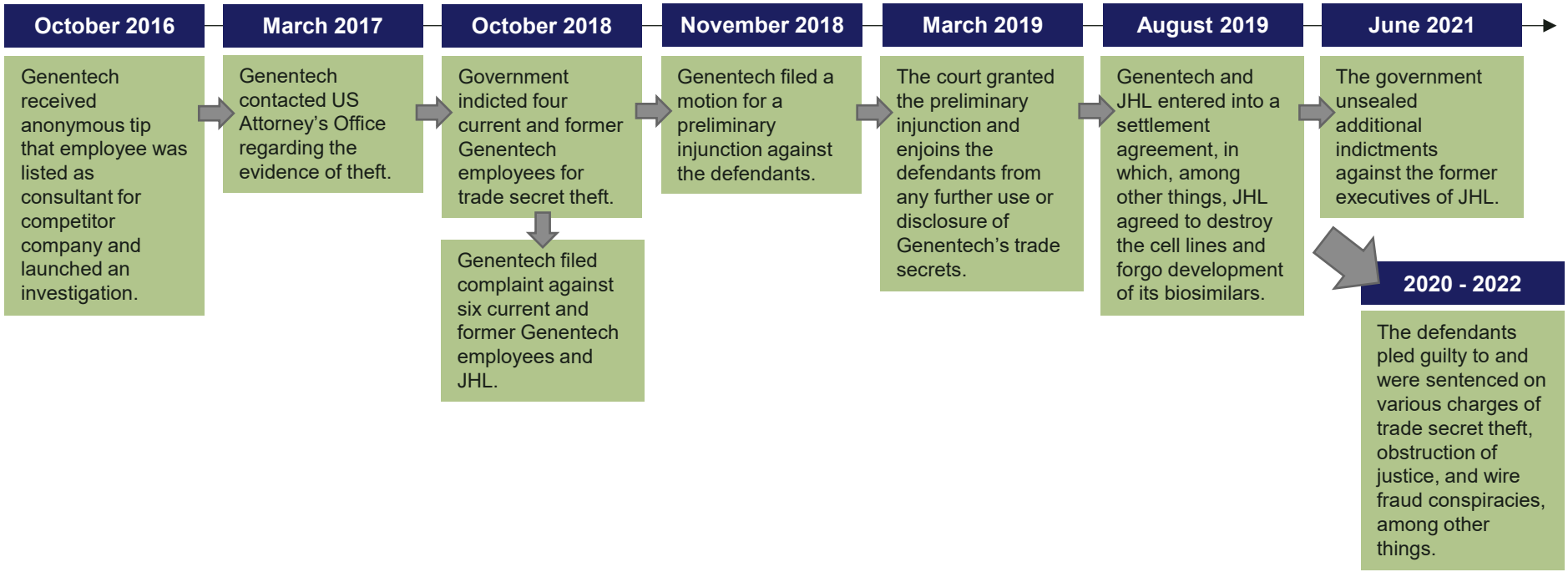
## Injunctions are often litigated early

- Evidentiary Hearing (documents, declarations, testimony, experts)
- Likelihood of Success on the Merits
  - Are actual trade secrets at issue?
  - Was there misappropriation and damage?
- Irreparable Harm
  - Not speculative, but actual and imminent
  - Did plaintiff delay in seeking an injunction?
- Balance the equities

*Genentech v. JHL*

# *Genentech v. JHL*

## Overview: investigation & litigation timeline

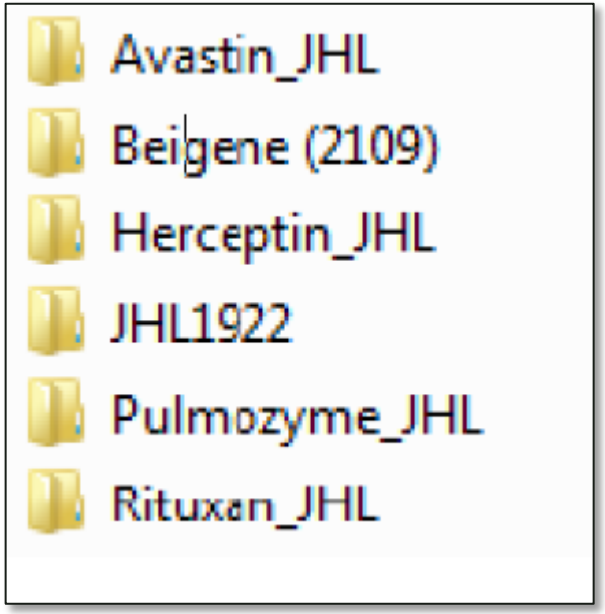


# *Genentech v. JHL*

## The trade secrets at issue

- Analytical methods to test and ensure the stability, potency, purity, and identity of four Genentech biologics (Rituxan, Avastin, Herceptin, and Pulmozyme)
- Manufacturing processes and analytical methods to test and ensure the quality of its biologics; and
- Information regarding development and selection of a formulation for the biologic

# *Genentech v. JHL*




## The misappropriation scheme

Employees downloaded massive troves of documents from Genentech's repository of technical documents.

# *Genentech v. JHL*: The Misappropriation Scheme

**From:** <alam@jhlbiotech.com>
**Date:** 1/7/2014 3:55 PM
**To:** Racho Jordanov <rjordanov@jhlbiotech.com>
**CC:** Rose Lin <rlin@jhlbiotech.com>, Debbie Lou <dlou@jhlbiotech.com>, David Kapitula <dkapitula@jhlbiotech.com>, Wan-Ting Hsieh <wthsieh@jhlbiotech.com>, ML <mlsheung2@gmail.com>

Racho,

Attached is the methyl green activity assay used by the innovator. The assay is rather lengthy, but is doable. At least the assay is familiar to the FDA/EMEA, and acceptable to them.

# *Genentech v. JHL*

## "Reasonable efforts" in practice

Third party confidentiality agreements

Further, he who seeks equity must do equity. That is, Genentech must also account for those sixty-six Genentech documents referenced in (and appended to) its Statement Regarding Trade Secrets. Within **THIRTY-FIVE (35) CALENDAR DAYS** of the date of Genentech's posting of bond, Genentech must provide a log to JHL's counsel (or the Court) explaining the extent to which the aforementioned documents have been disclosed by Genentech — including (1) all persons and/or entities (*e.g.*, vendors, regulatory agencies, hospitals) to whom Genentech has disclosed any of the aforementioned documents and whether those persons and/or entities were subject to a non-disclosure agreement, and (2) all articles, presentations, patents, emails, or any other similar publication by Genentech that disclosed to a third party any of the aforementioned documents or any significant portion contained therein.

# *Genentech v. JHL*

## "Reasonable efforts" in practice

Employee confidentiality agreements

**A. Genentech's Proprietary Agreement**

29. When Ms. Lam was hired in 1986, Genentech required her to sign, as a condition of employment, an "Employee's Proprietary Information and Inventions Agreement" ("Proprietary Agreement"). Ms. Lam signed that agreement on August 19, 1986. Attached hereto as **Exhibit 20** is a true and correct copy of the "Employee's Proprietary Information and Inventions Agreement," signed by Ms. Lam. By signing the Proprietary Agreement, Ms. Lam confirmed that, in consideration of her employment and the compensation received, she would "keep in confidence and trust all Proprietary Information."

# Genentech v. JHL

## "Reasonable efforts" in practice

Ongoing employee training and certification

41. Under both the GGOP and the Code of Conduct, every Genentech employee is required to take training and certify compliance with the company's policy including those regarding protection of Genentech's confidential information. Under the GGOP, managers were directed to "make sure…employees fully understand and adhere to our GGOP." And under the Code of Conduct, managers are directed to ensure that "all employees reporting to them receive the help and advice they need to comply with the Code of Conduct."

42. Ms. Lam was trained on the GGOP in 2008 and certified compliance with the GGOP in 2011. Ms. Lam took Genentech's Code of Conduct training on April 8, 2011, and certified compliance with the Code of Conduct on multiple occasions, including on July 5, 2017; July 2, 2016; July 10, 2015; May 6, 2014; and May 13, 2013.[2]

43. The annual training certification requires Genentech employees to certify that they have not violated the Code of Conduct, and specifically asks whether employees are aware of "any conduct either by yourself or others that has occurred that you believe may violate any federal, state, or local law, regulation, rule, or other requirement, or any Company policy, procedure, or directive."

# Protecting your trade secrets: the investigation

Steps taken AFTER suspected misappropriation

18. HCO's investigation also revealed that, on three occasions in the summer of 2017, Ms. Lam's log-in credentials were used to connect her Genentech-issued laptop to Genentech's Virtual Private Network (VPN), which provides remote access to Genentech's secure network and that hundreds of Genentech documents containing Genentech's confidential manufacturing policies and protocols were accessed and downloaded during those three VPN sessions on July 9, July 16, and July 26, 2017. Genentech was subsequently able to identify the documents that were downloaded during those VPN sessions by reviewing the "Downloads" folder in a back-up of Ms. Lam's laptop. HCO's review of the "Downloads" folder also uncovered additional downloads of manufacturing policies and protocols on August 13, 2017. The list of documents that were downloaded during the VPN sessions in July and those downloaded on August 13, 2017 are listed in Appendix 5 attached to Genentech, Inc.'s Statement Regarding Trade Secrets, filed concurrently with this declaration.

# *Genentech v. JHL*

## Protecting your trade secrets: the investigation

Reasonableness of steps taken depends on the circumstances!

JHL next contends that Genentech failed to take reasonable measures to protect the information's secrecy. It does not dispute that Genentech's policy of limiting access to the information, entering into confidentiality agreements with its employees, prohibiting unauthorized disclosure or use of confidential information during employment, and storing information in password-protected repositories constitutes sufficiently reasonable efforts to maintain secrecy (*see* Kirshman Decl. ¶¶ 26–60). Rather, it argues Genentech lacked reasonable efforts by allowing Xanthe to continue on as normal for eleven months after learning of her consulting work for competitors. Genentech, for example, did not take any action to curb her access to proprietary information, such as using commercially available monitoring software that identify and block email with certain attachments or to certain addresses (Dkt. No. 77 at 16; Racich Decl. ¶¶ 11, 14). This order disagrees. Genentech immediately launched an investigation into Xanthe's conduct but avoided taking any action that might have alerted Xanthe to the FBI investigation because of the government's request. Once the FBI searched her house, Genentech took immediate action and fired Xanthe soon after (Kirshman Decl. ¶¶ 4, 19). Under these circumstances, this order finds that Genentech's efforts were reasonable.

## Referring matters to law enforcement – in practice

- Criminal case timeline
- Effects of criminal investigation on civil lawsuit
- Evidence uncovered by the FBI

# *Genentech v. JHL*

## Importance of preliminary injunction

- Successfully enjoined JHL from further use or disclosure of Genentech trade secrets, and from selling, marketing, or commercializing any drugs that were developed, in whole or in part, with the benefit or use of Genentech's trade secrets.
- Ordered JHL to turn over ALL Genentech documents, whether or not qualifying as trade secret.
- Within five months of the preliminary injunction being issued, the parties entered into a settlement agreement.

# Current Challenges in Protecting Trade Secrets

# Current Challenges in Protecting Trade Secrets: AI

## 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.

# Current Challenges in Protecting Trade Secrets: AI

## More biotechnology companies entering AI space

- AI technologies, which may streamline drug discovery and enhance clinical trial efficiency, represent significant intellectual property that companies need to safeguard.
- Trade secrets in AI are often the key differentiator amongst competitors: proprietary code, model architectures, training data, optimization methods, and deployment strategies. If compromised, they can provide competitors with an advantage that may otherwise take them years and billions of dollars to replicate.

# Current Challenges in Protecting Trade Secrets: AI

## Case Study: *Trilobio, Inc. v. Gandall and Nanala, Inc.* (N.D. Cal., 2024)

Former employee of biotech start-up, Trilobio, created a new company, Nanala, using aspects of Trilobio's machine learning and AI technologies to attract investors.

Court granted Trilobio a TRO against its former employee and Nanala, preventing them from using source code stolen from Trilobio's technology automating the creation long sequences of DNA for medical and genetic research and from using any other Trilobio intellectual property, including Trilobio's robotic artificial intelligence technology for conducting genetic experiments and testing.

# Current Challenges in Protecting Trade Secrets: AI

## 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

# Current Challenges in Protecting Trade Secrets: 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
- “Bring Your Own Device” (BYD) policies makes it harder to track potential misappropriation

# Current Challenges in Protecting Trade Secrets: The Cloud

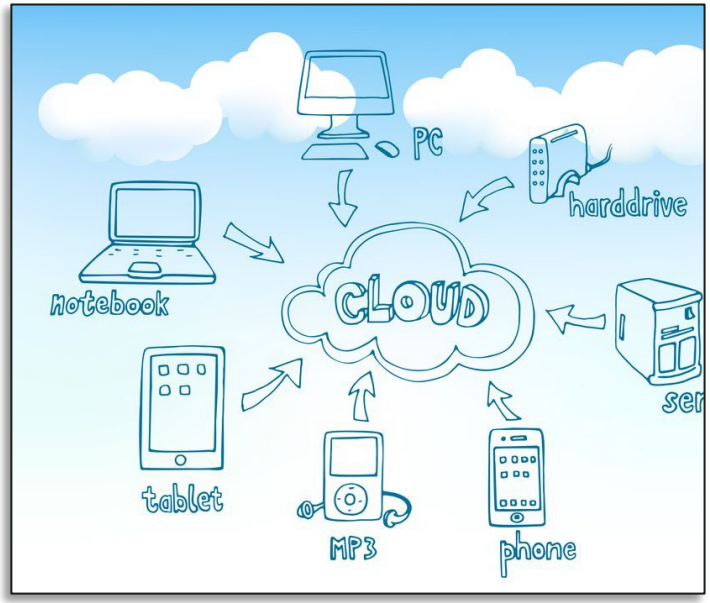
## Case Study: *Pfizer v. Li* (S.D. Cal., 2021)

Pfizer alleged that its former employee uploaded 12,000 documents from her company-issued laptop to a personal Google Drive account. The documents pertained to Pfizer vaccines, including its COVID-19 vaccines and related monoclonal antibodies.

The parties settled, with the former employee allowing Pfizer to thoroughly search her personal accounts to ensure she no longer held any confidential company information.

# Current Challenges in Protecting Trade Secrets: The Cloud

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




- Require use of company-issued Apple or Google accounts
- Implement Data Loss Prevention (DLP) software
- Conduct exit interviews to ensure files on personal devices cloud storage systems have been deleted
- Ask new employees to confirm existing cloud systems do not contain third party confidential information

# Current Challenges in Protecting Trade Secrets

## Implications for “reasonable efforts”

Courts consider the foreseeability of the conduct through which the secret was acquired and the availability and cost of effective precautions, evaluated in light of the economic value of the trade secret. Restatement (Third) of Unfair Competition.

In the AI landscape, companies may need to take greater precautions to meet this burden, such as:

- Stronger encryption methods
- Avoiding digitization of data
- Restricting employees’ AI usage
- Conditioning access to proprietary information on agreement to not utilize data in connection with any AI system

# Questions?

KEKER
VAN NEST
& PETERS

# Thank you!