

# The DTSA at One:

## An Empirical Study of the First Year of Litigation Under the Defend Trade Secrets Act



IP Statistics for Decisionmakers (IPSDM) Conference 2017  
November 14-15, 2017

David S. Levine & Christopher B. Seaman  
[dlevine3@elon.edu](mailto:dlevine3@elon.edu); [seamanc@wlu.edu](mailto:seamanc@wlu.edu)

May 11, 2016



Public Law 114–153  
114th Congress

An Act

To amend chapter 90 of title 18, United States Code, to provide Federal jurisdiction for the theft of trade secrets, and for other purposes.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

**SECTION 1. SHORT TITLE.**

This Act may be cited as the “Defend Trade Secrets Act of 2016”.

# WANTED

BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets



Huang Zhenyu



Wen Xinyu



Sun Kailiang



Gu Chunhui



Wang Dong

FILED

AUG 20 2015

AO 91 (Rev. 08/09) Criminal Complaint

UNITED STATES DISTRICT COURT

for the Northern District of California

RICHARD W. WIEKING CLERK, U.S. DISTRICT COURT THE NORTHERN DISTRICT OF CALIFORNIA

JCS

United States of America v. JING ZENG

Case No.

3-15-71060

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of July 9th and 10th, 2015 in the county of San Francisco in the Northern District of California, the defendant(s) violated:

Table with 2 columns: Code Section, Offense Description. Includes 18 U.S.C. § 1832(a)(2) Theft of trade secrets and Max Penalties (Class C Felony): 10 years in prison, \$250,000 Fine, 3 years of Supervised Release, \$100 Special Assessment.

This criminal complaint is based on these facts:

Please see attached affidavit

Continued on the attached sheet.

Approved as to Form:

CANDACE KELLY

Cynthia Ho, FBI Special Agent

Sworn to before me and signed in my presence.

Date: 8/20/2015

JOSEPH C. SPERO, U.S. Magistrate Judge

City and state: San Francisco, California

18

AFFIDAVIT IN SUPPORT OF COMPLAINT AND ARREST WARRANT

I, Cynthia Ho, a Special Agent with the Federal Bureau of Investigation in San Francisco, California, being duly sworn, hereby depose and state the following:

PURPOSE OF AFFIDAVIT AND AGENT BACKGROUND

I am an "investigative or law enforcement officer of the United States," within the meaning of Section 2510(7) of Title 18, United States Code, that is, an officer of the United States empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516, Title 18, United States Code.

A. Summary and Purpose of Affidavit

1. This affidavit is submitted in support of a request for an arrest warrant I am seeking in connection with an investigation of JING ZENG. As set forth herein, probable cause exists to believe that JING has violated 18 U.S.C. § 1832(a)(2).

2. The criminal conduct that is the subject of this Affidavit, and is described in more detail below, can be summarized as follows: ZENG was an employee of Machine Zone, Inc., which makes the on-line video game Game of War: Fire Age. In June 2015, ZENG learned that his job at Machine Zone was not secure and that he would likely need to leave the company. In July 2015, ZENG twice surreptitiously accessed a confidential company database called Tableau from his company laptop and accessed files that contained valuable, non-public information regarding the way customers use and interact with the Machine Zone game. ZENG did this once before he was terminated and once after he was terminated. After he was terminated, ZENG "wiped" and reformatted his Machine Zone laptop before he returned it to the company. The Machine Zone CEO confronted ZENG with evidence that ZENG had taken information from the Tableau database. ZENG admitted that he had done so, but denied any bad purpose. ZENG

# A misguided attempt to “defend trade secrets”

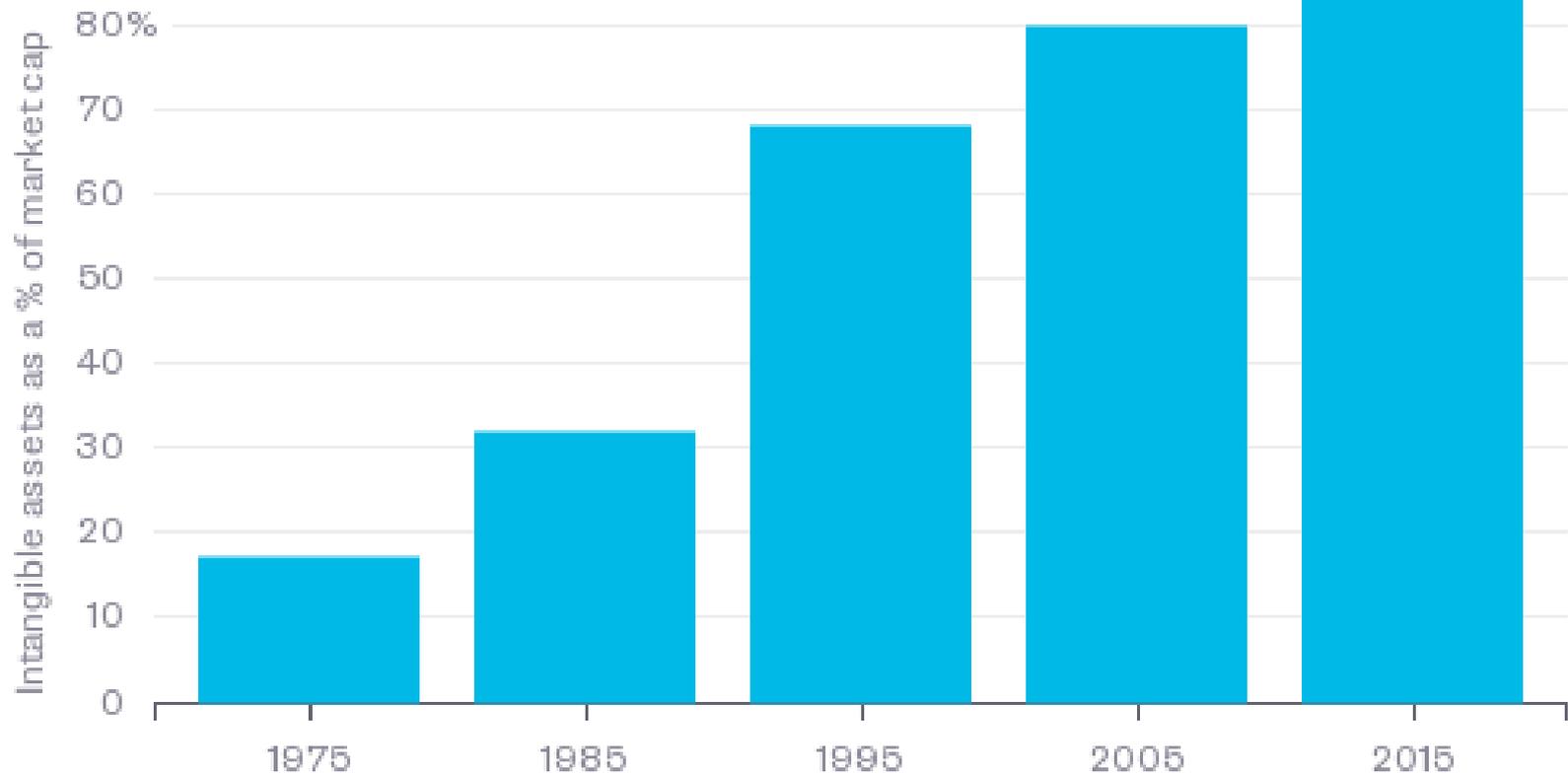
---

By David Post December 2, 2015

Along with 41 colleagues, I recently joined [a letter submitted to the Committee opposing DTSA](#) in which we tried to point out some of the ways in which putting this weapon in the hands of trade secret owners is likely to backfire, becoming a “strategic weapon” that will be used mostly for anti-competitive purposes that have nothing to do with preventing “cyber-espionage.” [A more detailed critique of the ex parte seizure provisions can be found in [this article by Eric Goldman](#), one of the authors of the law professors’ letter]

# The Corporation Has Gone Virtual

The value of the S&P 500 now consists mostly of intangibles



Source: Ocean Tomo

**Bloomberg**View

# Trade Secret Overview

- Prima facie cause of action
  - Existence of a trade secret (UTSA §1(4)) = information that:
    - derives value from being not generally known by those who can find economic value
    - subject to reasonable efforts to keep secret
  - Acquisition by improper means
    - UTSA §1(1): Includes “theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means”
  - Misappropriation (use or disclosure) (UTSA §1(2))
- UTSA: 47 states + DC. (MA, NC, NY hold-outs)
- Remedies:
  - Equitable (preliminary/permanent injunction)
  - Damages (lost profits, disgorgement, reasonable royalty as alternative)

# Empirical Studies

- Trade secrecy an important “appropriability” mechanism
  - Study of 1,478 manufacturing firms found that secrecy ranked first or second in importance for product innovations in 24 of 33 surveyed industries (Cohen, Nelson, Walsh 2000)
- Trade secrets and patents can be substitutes
  - Survey of 650 R&D executives found that patents preferred over trade secrecy (not including start-ups) (Levin 1987)
  - European survey of 2,849 R&D firms finds that they prefer secrecy over patents (based on 1993 survey) (Arundel 2001)
  - Supports standard theory. But can they be complements?
- Trade secrecy litigation appears to be increasing; most cases involve current/former employees
  - See Almeling et al. 2009-2010

# DTSA Purpose

“In today’s electronic age, trade secrets can be stolen with a few keystrokes, and increasingly, they are stolen at the direction of a foreign government or for the benefit of a foreign competitor. These losses put U.S. jobs at risk and threaten incentives for continued investment in research and development. Current federal criminal law is insufficient.”

Sens. Chris Coons (D-DE) and Orrin Hatch (R-UT),  
DTSA Sponsors

# DTSA Key Points

- Creates first federal civil cause of action for trade secret misappropriation in US.
  - Previously, trade secret owners could not sue in federal court unless there was diversity or supplemental jurisdiction.
- Original but not exclusive jurisdiction in federal court.
  - State courts can hear claims under the DTSA
- Liability provisions modeled after Uniform Trade Secrets Act (UTSA).
- Adds new remedy (*ex parte* seizure).
- Limitations on injunctive relief.
- Adds a whistleblower provision.
- Does not preempt state trade secret law.

# Arguments for DTSA

- Massive problem of cyber- and corporate-espionage
  - State actors
  - Internet
  - “Sneakernet”
- State law insufficient and non-uniform
  - Substance: seizure?
  - Procedure: discovery, enforcement
- DoJ overburdened
- No federalism problem
- International trade negotiations

# Arguments Against DTSA

- Trade secret law is already largely uniform
- Anti-competitive/plaintiff-oriented
- Accidental disclosure
- Ancillary impacts
  - Access to information
  - Labor mobility
  - Inevitable Disclosure Doctrine
- Better routes?
  - Espionage laws
  - Computer Fraud and Abuse Act (CFAA)
  - More DOJ funding for criminal enforcement

# Research Questions

- Is the DTSA achieving sponsors' objectives?
- How are trade secret owners using the DTSA?
- What can we learn about trade secrecy generally from litigated cases?

# Methodology

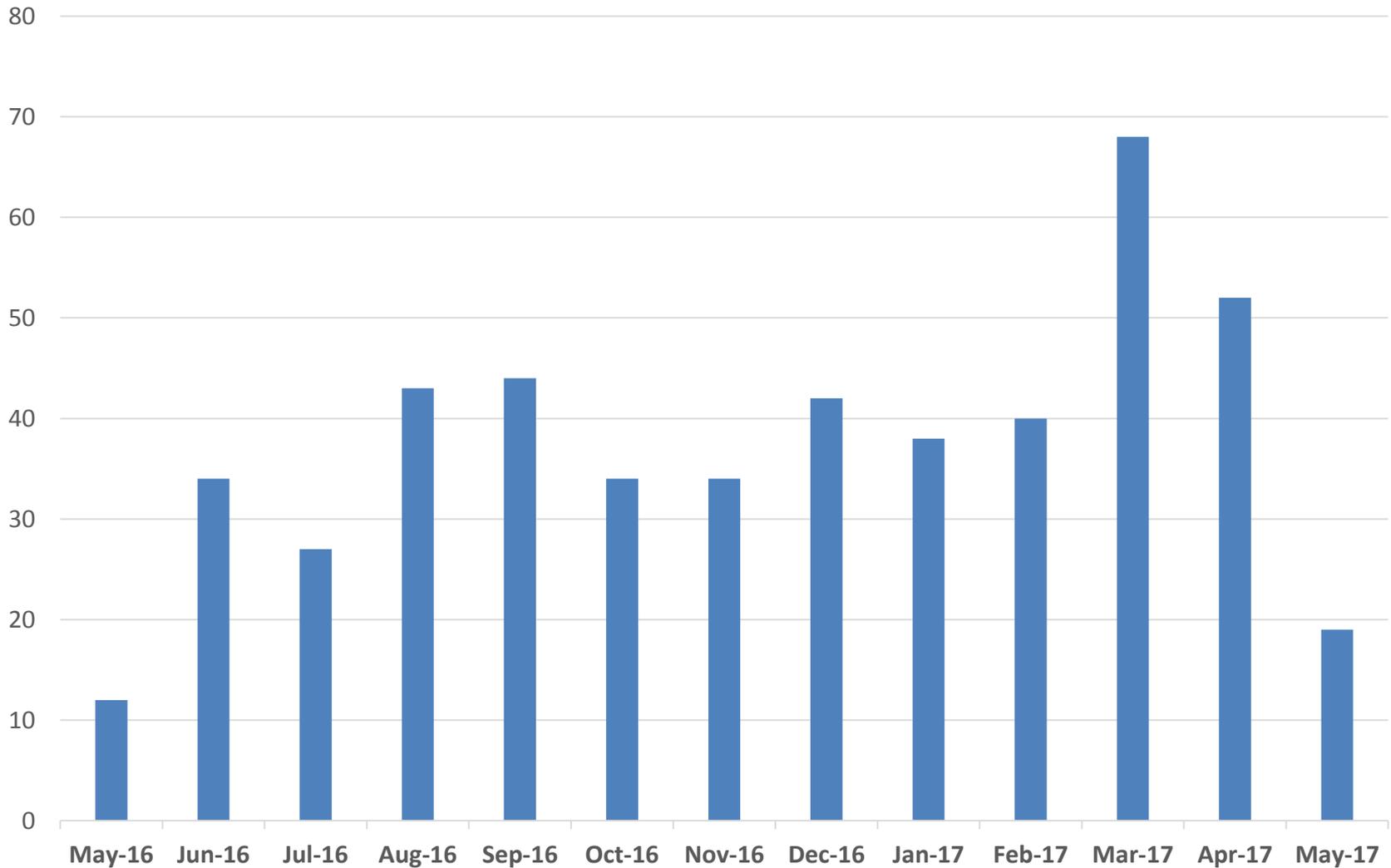
- Identify cases w/DTSA claim (5/11/16 - 5/11/17)
  - Bloomberg Law – court dockets and filings
  - Westlaw and Lexis – opinions citing DTSA
- Hand code data on:
  - Basic case information
  - Allegations in complaints
  - Motions on preliminary relief (*in progress*)

# Data Set

- 486 cases involving DTSA claim
  - 15 cases removed from state court
  - 9 counterclaims
- *Compare to:* 4,537 patent cases filed in 2016

# DTSA Claims by Month

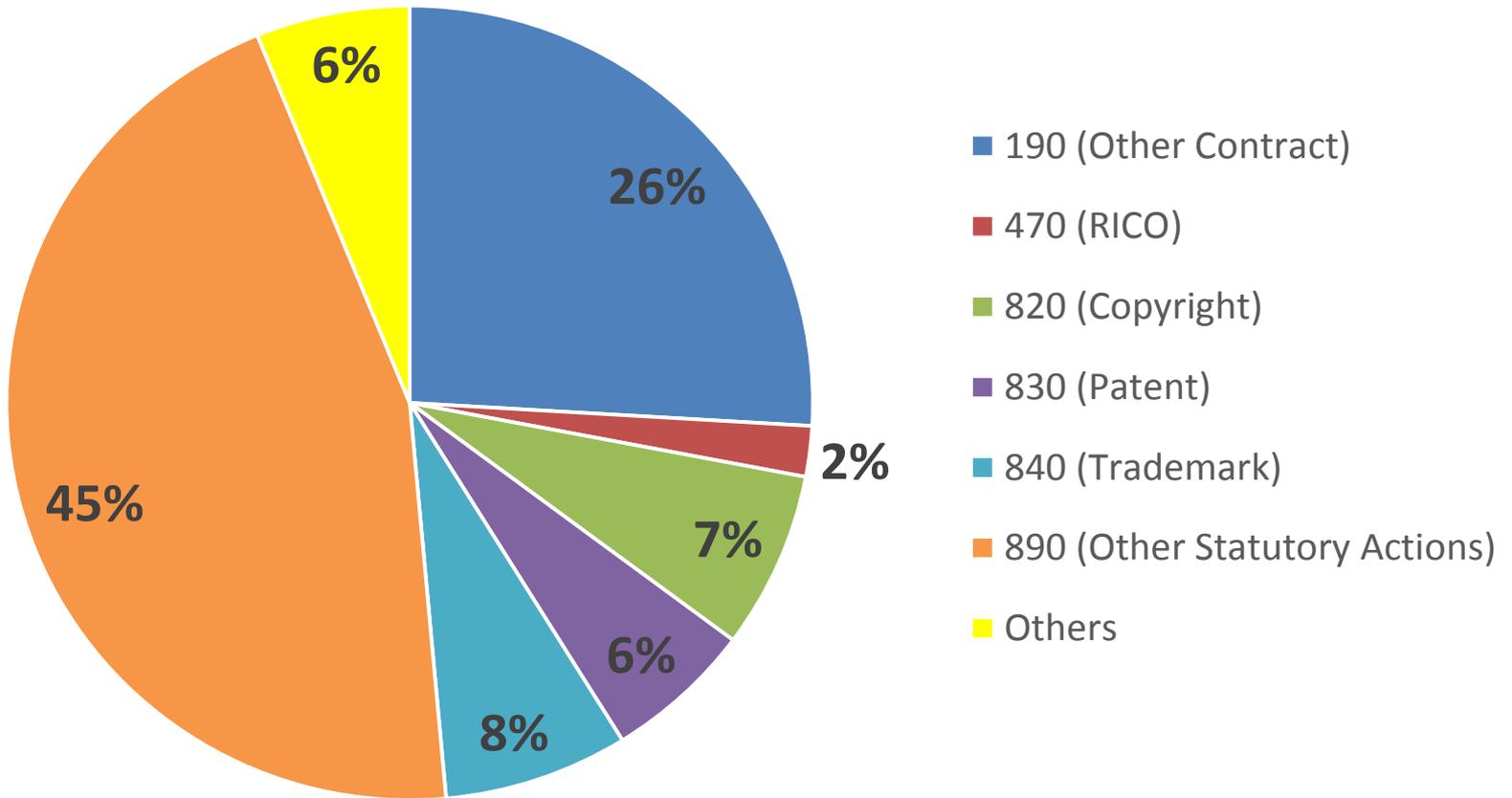
Number of Cases



# Top Districts for DTSA Claims

District	N	%
N.D. Illinois	43	9%
N.D. California	38	8%
C.D. California	30	6%
S.D. New York	29	6%
E.D. Virginia	16	3%
E.D. Pennsylvania	15	3%
S.D. Florida	15	3%
<i>Compare to:</i>		
D. Delaware	10	2%
E.D. Texas	7	1%

# Nature of Suit Codes



# Asserted Bases for Jurisdiction

- Federal question (§ 1331): 96%
- Diversity (§ 1332): 44%
- Supplemental (§ 1367): 78%
  
- 128 cases (26%) would lack fed. jurisdiction absent DTSA (no other fed claim + no div.)

# Add'l Federal Law Claims

Claim	% cases
CFAA	20%
Lanham Act	15%
Copyright	8%
Patent	6%
Civil RICO	2%
Antitrust	1%
Other federal claims	3%

# Related State Law Claims

Claim	% cases
State trade secret misappropriation	84%
Breach of contract	70%
Tortious interference	53%
Unfair competition	41%
Breach of fiduciary duty	40%
Conversion	31%
Unjust enrichment	22%
Civil conspiracy	17%
Breach of implied duty of good faith	10%
Fraud	9%
State computer torts/crimes	8%
Other state law claims	31%

# Trade Secret Information

Trade Secret Misappropriated	% cases
Customer list/information	59%
Business information (incl. financial data, marketing, business plans)	58%
Technical/scientific information	39%
Software/algorithm	22%
Formula	7%
“Negative” know-how	1%

# Who are Alleged Misappropriator(s)?

- Current/former employee (66% of cases)
- Current/former business partner (26% of cases)
- Unrelated third party (10% of cases)

*Totals exceed 100%; 15 cases involve both current/former employee and current/former business partner as alleged misappropriator*

# DTSA's Objectives

“In today’s electronic age, trade secrets can be stolen with a few keystrokes, and increasingly, they are stolen at the direction of a foreign government or for the benefit of a foreign competitor. These losses put U.S. jobs at risk and threaten incentives for continued investment in research and development.”

# Foreign Defendants

- Only 29 cases (6%) ID foreign citizen/national as defendant
  - China: 7 cases
  - Canada: 5 cases
  - Singapore: 3 cases
  - France: 2 cases
  - India: 2 cases
  - Taiwan: 2 cases
  - 1 case each: UK, Japan, Russia, 5 other countries

# Cyberespionage / Hacking

- 22% (109 cases) assert either CFAA or state law computer crime/tort
- But only 9% (42 cases) involve claim of unauthorized access (e.g., hacking)
  - 4 of these cases involve foreign defendant

# NDA / Confidentiality Agreement

- Trade secret owner alleges NDA/written confidentiality agreement in 72% of cases
  - 81% of cases involving current/former employees

# Implications

- DTSA litigation broadly similar to UTSA litigation in federal and state courts
  - Known Ds (mostly former employees)
  - Non-technical trade secrets
- Few foreign defendants; hacking claims uncommon; cybersecurity impact
- Parallel/overlapping federal and state claims; uniformity issue?

# Possible Areas for Further Research

- Other variables:
  - Preliminary relief (*in progress*)
  - Type of plaintiff (e.g., large/publicly traded)
  - Industry
  - Whistleblower defense
  - Non-compete agreements
- Case outcomes (longer time horizon)