Updates on Trade Secrets in the U.S.

By: Linda Shudy Lecomte
Wuersch & Gering LLP
June 2017

AIPLA
Serving the Creative and Legal Communities

Disclaimer

The purpose of this presentation is to provide educational and informational content and is not intended to provide legal services or advice. The opinions, views and other statements expressed by the presenter are solely those of the presenter and do not necessarily represent those of AIPLA.

U.S. Government

Note:

We will not be discussing any takings of trade secrets by the US Government – invoking the 5th Amendment to the Constitution.

Additional Applicable Laws May Include:

Federal Tort Claims Act, 28 U.S.C. § § 1346(b), 2674

Tucker Act, 28 U.S.C. § 1491(a)(1)

Digital billboard image posted in various regions of the US having a concentration of high-tech research and development companies, laboratories, major industries, and national defense contractors.
https://www.fbi.gov/news/stories/2012/may/insider_051112/image/locked-doors/view

Overview: Federal and State Laws

Traditionally, States Applied

Common law and/or State-Enacted Statutes

Thus, Litigation in State Court

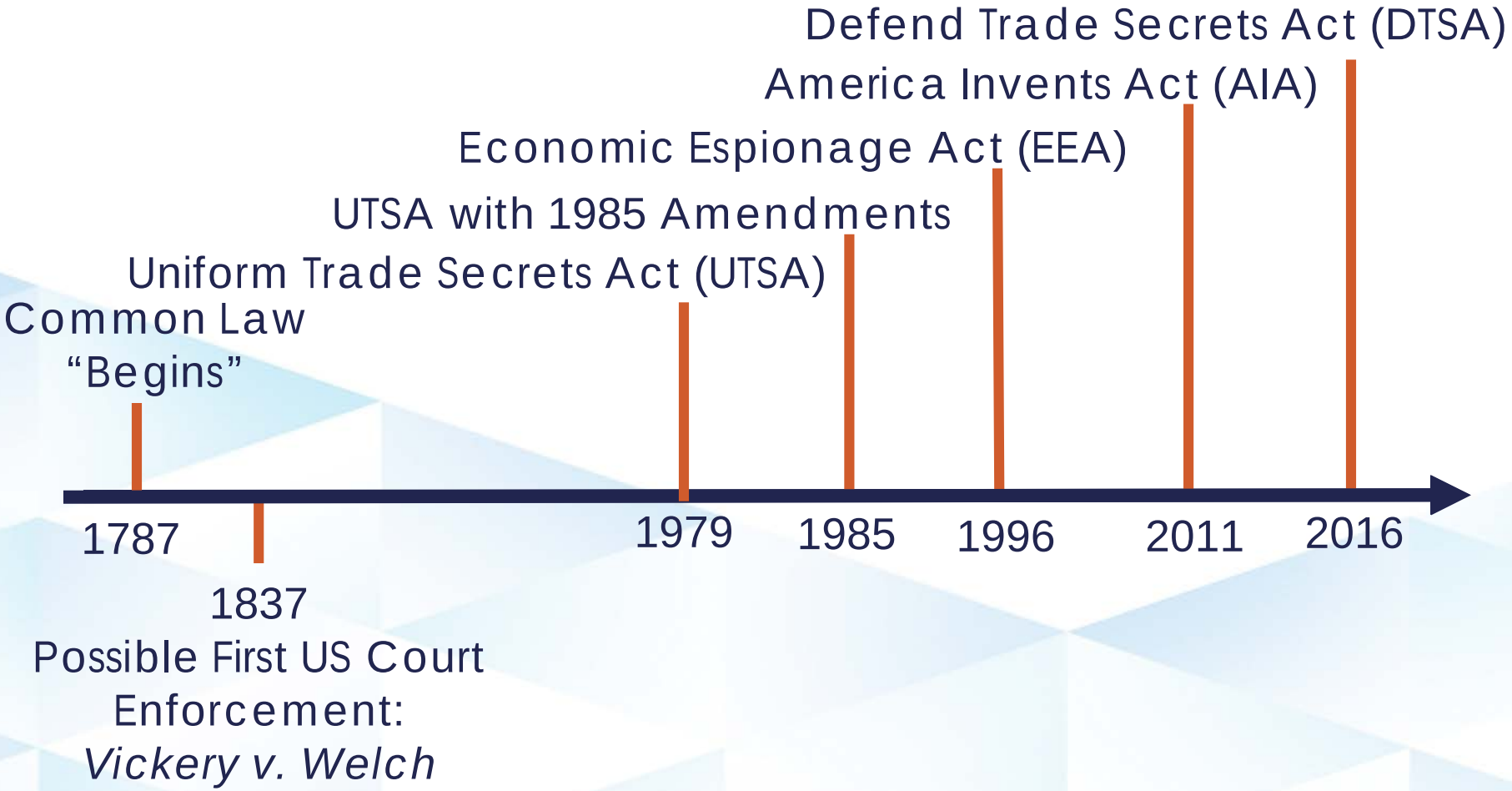
In Effort to Align the States: Uniform Trade Secrets Act (UTSA), USTA with 1985 Amendments

Most US States Have Now Enacted

Trade Secret Law Similar to UTSA, and

the US Federal Government has provided more Enforcement Options with the EEA and DTSA.

AIPLA Trade Secret Laws in the US



Oftentimes, US practitioners will refer to " § 757, Restatement of Torts" and the subsequent second edition, authored in late 1970s re trade secrets. Restatement of Torts Second, issued by American Law Institute, is an influential treatise summarizing general principles of common law tort law.


Information
Kept Secret
Commercial
Value
Trade
Secret

AIPLA 1787: Trade Secret Laws

U.S. Constitution – 1787 (when ratified by 9/13 states)

Article I, Section 8:

The Congress shall have Power…

To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries….

Trade Secrets Defined

UTSA (1979) (Same Definition in UTSA (1985)):

(similar definition adopted in most US states)

"Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and

(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Trade Related Aspects of Intellectual-Property Rights (TRIPS), Article 39, paras. 2 & 3

Article 39

1. In the course of ensuring effective protection against unfair competition as provided in Article 10*bis* of the Paris Convention (1967), Members shall protect undisclosed information in accordance with paragraph 2 and data submitted to governments or governmental agencies in accordance with paragraph 3.

2. Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as such information:

(a) **is secret** in the sense that it is **not**, as a body or in the precise configuration and assembly of its components, **generally known among or readily accessible to person**s within the circles that normally deal with the kind of information in question;

(b) **has commercial value because it is secret**; and

(c) **has been subject to reasonable steps** under the circumstances, by the person lawfully in control of the information, **to keep it secret**.

3. Members, when requiring, as a condition of approving the marketing of pharmaceutical or of agricultural chemical products which utilize new chemical entities, the submission of undisclosed test or other data, the origination of which involves a considerable effort, shall protect such data against unfair commercial use. In addition, Members shall protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use.

1996: Trade Secret Laws

Economic Espionage Act (EEA) (1996 and later amendments)

18 USC § 1831 – Economic Espionage

(a) In General.—Whoever, **intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly**—

(1) **steals**, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception **obtains a trade secret**;

(2) **without authorization copies**, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;

(3) **receives**, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) **attempts to commit any offense** described in any of paragraphs (1) through (3); or

(5) **conspires with one or more other persons to commit any offense** described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined **not more than $5,000,000 or imprisoned not more than 15 years, or both**.

(b) Organizations.— **Any organization** that commits any offense described in subsection (a) shall be fined **not more than the greater of $10,000,000 or 3 times the value of the stolen trade secret to the organization**, **including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided**.

(Added Pub. L. 104–294, title I, § 101(a), Oct. 11, 1996, 110 Stat. 3488; amended Pub. L. 112–269, § 2, Jan. 14, 2013, 126 Stat. 2442.)

1996: Trade Secret Laws

Economic Espionage Act (EEA) (1996 and later amendments)

18 USC § 1832 – Theft of Trade Secrets

(a) Whoever, **with intent to convert a trade secret**, that is related to a product or service **used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly**—

(1) **steals**, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) **without authorization copies**, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) **receives,** buys, or possesses such information, **knowing the same to have been stolen** or appropriated, obtained, or converted without authorization;

(4) **attempts to commit** any offense described in paragraphs (1) through (3); or

(5) **conspires with one or more other persons to commit** any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), **be fined under this title or imprisoned not more than 10 years, or both.**

(b) **Any organization** that commits any offense described in subsection (a) **shall be fined not more than $5,000,000**.

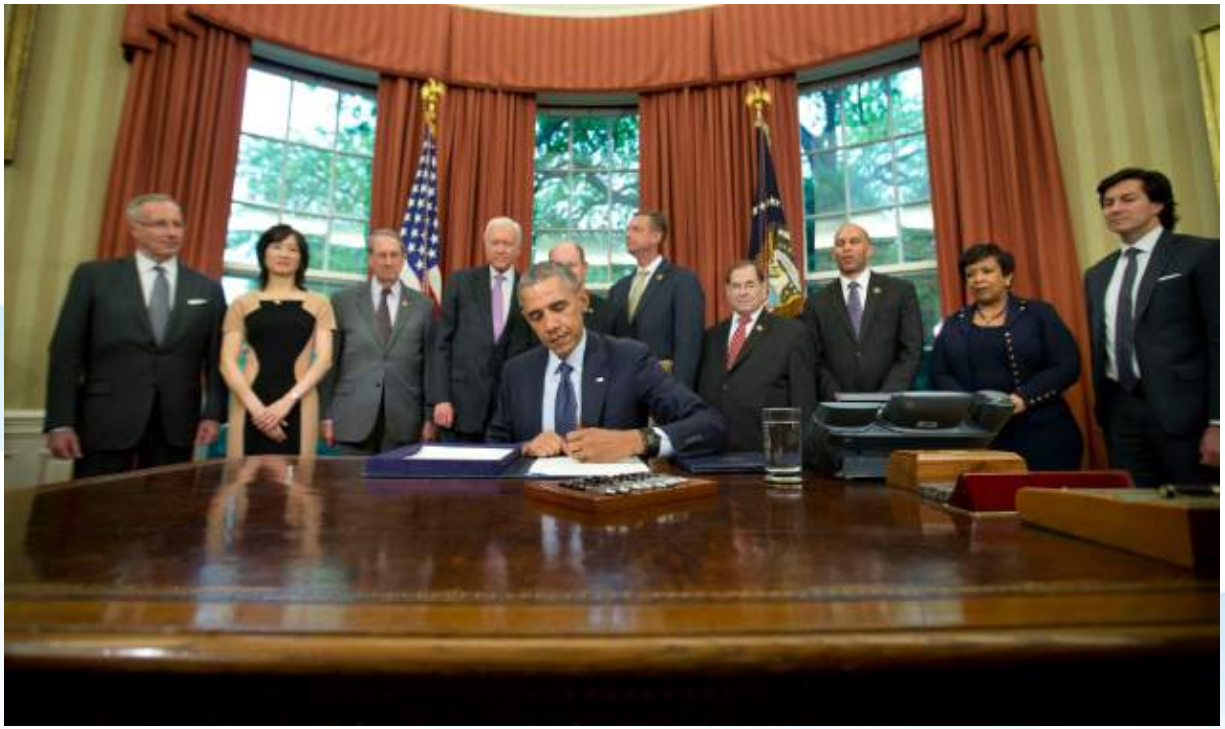
(Added Pub. L. 104–294, title I, § 101(a), Oct. 11, 1996, 110 Stat. 3489; amended Pub. L. 112–236, § 2, Dec. 28, 2012, 126 Stat. 1627.)

1999, 2011 – Trade Secret Laws

America Invents Act (AIA) (2011) Amended the Prior User Defense of the American Inventor Protection Act of 1999 (35 USC § 273)

- Expanded Applicable Subject Matter
  - Expanded from "Method of Doing or Conducting Business" to "Process, or Consisting of a Machine, Manufacture, or Composition of Matter Used in a Manufacturing or Other Commercial Process"
- Broadened Personal Defense:
  - 1999: "asserted only by the person who performed the acts necessary to establish the defense"
  - 2011: "asserted only by the person who performed or directed the performance of the commercial use… or by an entity that controls, is controlled by, or is under common control with such person"
  - Additional changes were made concerning transfer of the business and assignment of rights occurs, et al.
- Restricted Commercial Requirement:
  - 1999: "use is in connection with an internal commercial use or an actual arm's-length sale or other arm's-length commercial transfer of a useful end result, whether or not the subject matter at issue is accessible to or otherwise known to the public"
  - 2011: "commercially used the subject matter in the United States, either in connection with an internal commercial use or an actual arm's length sale or other arm's length commercial transfer of a useful end result of such commercial use; and such commercial use occurred at least 1 year before the earlier of either… the effective filing date of the claimed invention or … the date on which the claimed invention was disclosed to the public in a manner that qualified for the exception from prior art under section 102(b)"
- Added University Exception:
  - 1999: <none>
  - 2011: "may not assert a defense… if the claimed invention with respect to which the defense is asserted was, at the time the invention was made, owned or subject to an obligation of assignment to either an institution of higher education… or a technology transfer organization whose primary purpose is to facilitate the commercialization of technologies developed by one or more such institutions of higher education" and this section does not apply if "any of the activities required to reduce to practice the subject matter of the claimed invention could not have been undertaken using funds provided by the Federal Government"

DEFEND TRADE SECRETS ACT OF 2016 ("DTSA")



U.S. President Barack Obama signs the Defend Trade Secrets Act of 2016 (DTSA), in the Oval Office of the White House in Washington, Wednesday, May 11, 2016. (L-R) Deputy US Trade Representative Ambassador Robert W. Holleyman, Commerce Undersecretary Michelle Lee, Rep. Bob Goodlatte, R-Va., Sen. Orrin Hatch, R-Utah, Sen. Chris Coons, D-Del., Rep. Doug Collins, R-Ga., Rep. Jerrold Nadler, D-NY., Rep. Hakeem Jeffries, D-NY., US Attorney General Loretta Lynch, and US Intellectual Property Enforcement Coordinator Danny Marti. (AP Photo/Pablo Martinez Monsivais)

2016: Trade Secret Laws

Defend Trade Secrets Act (DTSA) (2016)

- Broadens Definition of Trade Secret
  - "the public" is replaced with "another person who can obtain economic value from the disclosure or use of the information"
- Eliminates need to satisfy General Diversity Jurisdiction
- Does not preempt currently available State Remedies
- Allows for double damages, reasonably attorney fees for willful and malicious violations, and attorney fees for actions brought in bad faith
- Provides additional protections for Whistleblowers
- Provides Ex Parte "Civil Seizure"
  - Only in "extraordinary circumstances"
  - Requires:
    - 1. other forms of equity "inadequate" because the party "would evade, avoid, or otherwise not comply with such an order"
    - 2. "immediate and irreparable harm" if no seizure
    - 3. harm to applicant outweighs the harm to the legitimate interests of the other person
    - 4. applicant is "likely to succeed" in showing:
      - *-information is trade secret; other person misappropriated trade secret and conspired to use improper means to misappropriate the trade secret; and person has possession of the trade secret and property to be seized*

How Do US Trade Secret Laws Compare with Europe's Trade Secret Laws? For the Moment, Let's Just Observe the Definition of Trade Secrets:

In May 2016, the **European Union's Directive on Trade Secrets** was adopted by the European Union Council, and defines Trade Secrets in Article 2(1) as:

(1) 'trade secret' means information which meets all of the following requirements:

(a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

(b) it has commercial value because it is secret;

(c) it has been subject to reasonable steps under the circumstances by the person lawfully in control of the information, to keep it secret.

Trade Secret Enforcement in US Federal Court (EEA, DTSA), US State Courts, and Arbitration/Mediation

Sampling of Trade Secret Cases Involving EEA(1831), EEA (1832), Inevitable Disclosure, etc....

- Vickery v. Welch, 36 Mass. 523 (1837)
- Kewanee Oil Co. v. Bicron, 416 US 470, 94 S.Ct. 1879 (1974)
- Ruckelshaus v. Monsanto Co., 467 US 986, 104 S.Ct. 2862 (1984)
- PepsiCo v. Redmond, 54 F.3d 1262, 1272 (7th Cir. 1995)
- United States v. Williams, 526 F.3d 1312 (11th Cir. 2008) (per curiam)(NDGA)
- United States v. Chung, 659 F.3d 815 (9th Cir. 2011), *cert. denied*, No. 11-1141, 2012 WL 929750 (US Apr. 16, 2012)
- United States v. Agrawal, 726 F.3d 235 (2d Cir. 2013)
- United States v. Christina Liew et al., CR-11-0573 JSW, NDCA (2014)

The People of the State of New York v. Sergey Aleynikov, Appellate Division, First Department, New York State Supreme Court, January 2017

- Reinstated guilty conviction for stealing trading software from Goldman Sachs
  - *Due to litigation to determine whether Aleynikov violated state or federal law in making an electronic copy of the software on an external hard drive just before leaving Goldman Sachs to work at competing company Teza Technologies*
  - **February 2010** – charged with violating National Stolen Property Act and Economic Espionage Act
  - **December 2010** – SDNY convicted
  - **April 2012** – 2nd Cir App. Ct. reversed conviction
  - **September 2012** – charged with 2 counts of unlawful use of secret scientific material (June 1 and June 5 downloads) and 1 count of unlawful duplication of computer related material; Penal Laws 165.07, 156.30[1]
  - **July 2015** – NYS Supreme Court, NY County, Jury acquitted on unlawful duplication charge, NYS Supreme Ct, NY County, dismissed charges for unlawful use
  - **January 2017** – NYS Supreme Court, App Division, reversed and reinstated conviction wrt unlawful use of secret scientific material

The People of the State of New York v. Sergey Aleynikov

- ✓ Aleynikov was formerly a computer programmer employee for Goldman Sachs, wrote and maintained software for high frequency trading computer programs which are "central" to Goldman Sachs' business, hired in 2007, to maintain and add to a system purchased by Goldman Sachs in 1999
- ✓ High frequency trading involves use of computer to make rapid decisions concerning pricing of securities, and to rapidly generate trades and orders; speed is essential
- ✓ Lucrative – earned Goldman Sachs about $300 million in profits in 2009
- ✓ Goldman Sachs took several safeguarding measures re the software, including increased security, creation of information security group responsible for ensuring Goldman Sachs' systems were not vulnerable to attack, limiting employee access and requiring employees to sign a confidentiality and nondisclosure agreements; programmers were forbidden from copying the source code outside of the company network, work from home required remote access or use of a company laptop to ensure all source code remained within company network

The People of the State of New York v. Sergey Aleynikov

- ✓ Aleynikov transferred a digital copy of Goldman Sachs' trading software source code to a hard drive outside Goldman Sachs' network
- ✓ Aleynikov transferred copies of the software to his personal computing devices and shared it with his new employer Teza Technologies, a startup high-frequency trading firm. At that time, Teza did not have software, connectivity or equipment for high-frequency trading activities
- ✓ Teza hired Aleynikov as a systems architect for its new trading platform at an annual salary of $1.2 million (3xs his salary at Goldman Sachs)
- ✓ **May 2009** - Teza sent email to Aleynikov that the company had less than 6 months to launch the new system and that they needed to "move fast"
- ✓ **June 5, 2009** – Aleynikov ended his employment at Goldman Sachs
- ✓ **After June 5, 2009** – Goldman Sachs' information security department noticed "unusual activity" – i.e., on June 1, 2009 and June 5, 2009, large amounts of data had been uploaded from the company network to a Germany-based "subversion website" via Aleynikov's computer

The People of the State of New York v. Sergey Aleynikov

- Aleynikov transferred the "thousands of proprietary files" from the company network using a program he created, the program had been backdated by 2 years, and the program was subsequently deleted by defendant from his work computer along with his "bash" history (list of most recent commands typed).
- Police in Germany: located the server of the subversion website, removed the hard drives, made forensic copies of them
- The hard drives contained information that "saleyn" uploaded the information and later retrieved it – saleyn was used by Aleynikov as his personal email address handle
- **End June 2009** – Aleynikov put some of the source code into an account Teza created on a third party website
- **July 3, 2009** – Aleynikov arrested by FBI, Teza terminated his employment
  - *When questioned by the FBI, Aleynikov denied wrongdoing, and then later admitted uploading the source code to the unblocked third party server, downloaded source code to his computers, erased encryption software and bash history because he knew he violated Goldman Sachs' security policies*

The People of the State of New York v. Sergey Aleynikov, Appellate Division, First Department, New York State Supreme Court, January 2017

- Issue:

"Whether the defendant's actions constitute legally sufficient evidence to establish that he made a 'tangible reproduction or representation" of the source code, and did so with the "intent to appropriate… [its] use,' within the meaning of the unlawful use statute."

The Court held that the evidence was legally sufficient.

The People of the State of New York v. Sergey Aleynikov, Appellate Division, First Department, New York State Supreme Court, January 2017

- Law:

  Penal Law 165.07:

  "A person is guilty of unlawful use of secret scientific material when, with intent to appropriate to himself or another the use of secret scientific material, and having no right to do so and no reasonable ground to believe that he has such right, he makes a tangible reproduction or representation of such secret scientific material by means of writing, photographing, drawing, mechanically or electronically reproducing or recording such secret scientific material."

  Side note: this provision was added due to a prior statute which allowed that even a person who stole blueprints of a secret process by making a photographic copy, but did not take the original, did not commit larceny because there was no taking of "property"

AIPLA 2017 Trade Secret Caselaw Discussion

- **The People of the State of New York v. Sergey Aleynikov**, Appellate Division, First Department, New York State Supreme Court, January 2017
- Reasoning:

✓ Evidence sufficient to establish "tangible reproduction or representation" of the source code when copied and saved the code onto the German server (server hard drive is a physical medium; German law enforcement officer described how police removed "physical" hard drives; FBI testified source code "takes up physical space"; Goldman Sachs' engineer testified computer files are "physically present" on the hard drive)

  ✓ **Court determined relevant question is not whether the source code itself is tangible but "whether the defendant made a tangible reproduction of it" which he did when copied it onto the server**

    ✓ ***"physical hard drive" "physical space" and "physically present"***

    ✓ ***Trial Court appeared to mistakenly believe source code had to be printed on paper***

2017 Trade Secret Caselaw Discussion

- **The People of the State of New York v. Sergey Aleynikov**, Appellate Division, First Department, New York State Supreme Court, January 2017
- Reasoning (cont'd):

✓ Evidence sufficient to establish "intent to appropriate to himself or another the use of" where appropriate connotes a purpose to exert permanent or virtually permanent control

  ✓ **Court determined that with defendant's uploading, downloading to his computers as well as his new employer, trying to erase all appearance of copying at Goldman Sachs, no appearance of the defendant trying to return the source code to Goldman Sachs or delete it from new employer's servers, et al., "rational inference that defendant intended to exercise permanent control over the use of Goldman's source code, as opposed to short-term borrowing"**

    ✓ ***Trial Court appeared to mistakenly focus on permanent control rather than intent to permanently exercise control***

- **The People of the State of New York v. Sergey Aleynikov**

The NYS Court of Appeals has agreed to review the case

and so the ~8 year case continues…

Usnews.com

nytimes.com

AIPLA 2017 Trade Secret Caselaw Discussion

- **Dalmatia Import Group, Inc. v. FoodMatch Inc., et al.**, U.S. District Court for the Eastern District of Pennsylvania, February 2017 (transferred from SDNY)
- Considered first verdict under DTSA (Defend Trade Secrets Act)
- Dalmatia Import Group and Maia Magee develop and sell a "high quality fig jam."
- Foodmatch, Inc. and Lancaster Fine Foods, Inc. were distributors for Dalmatia et al.
- Foodmatch et al. sued for: providing a competing fig jam that "impersonates" Dalmatia et al.'s product, stealing the recipe of the fig jam, selling and distributing rejected jars of Dalmatia et al.'s fig jam, and using trademark without authorization. That is, **claims were brought for breach of contract, trademark infringement, counterfeiting, and misappropriation of trade secrets**.
- Jury found Foodmatch et al. liable for misappropriation of trade secrets, trademark infringement and counterfeiting, finding at least ~$2.5 million in damages
- It's not over… issues: truly willful? PUTSA and DTSA differentiation? Et

AIPLA 2017 Trade Secret Caselaw Discussion

Some of the other recent 2017 high profile trade secret cases include:

- **Zenimax Media Inc. et al. v. Oculus VR, Inc. et al. (TX) (decision)**
- **Hughes v. AGE Industries, Ltd. (TX) (decision)**
- **Tesla Motors, Inc. v. Anderson, et al. (CA) (settled)**
- **Waymo LLC v. Uber Technologies, Inc. (filed)**

AIPLA What Do You Do When…

A Client comes to you and says…

"I suspect trade secret theft by a current/former employee."

- **Options:**
  - Civil
  - Criminal
- **Enforcers:**
  - Company/Individual
  - U.S. District Attorney's Office
  - FBI

Keep/Find the Evidence:

For example, in trade secret computer software case:

- **Software Access Logs**
- **Email**
- **Password Usage/Change Logs**
- **Look for Backdoors**
- **Change Encryption Keys and all Passwords**
- **For Remote Server Storage, Check with Provider regarding access**

What Do You Do When…

Get Help:

- Consider hiring a forensics expert if you suspect theft of trade secret software
- Contact local enforcement regarding case… note, sometimes there is a parallel investigation in progress re trade secrets or other bad faith dealings
- Even if you don't see evidence now, consider implementing a Trade Secrets Safeguard Policy which provides for checks after 3 months, 6 months, 9 months… especially after the leaving of a key employee

Some Trade Secrets Best Practices: What Can One Do Preemptively?

1. Limit Access to Entirety!
2. Keep Entirety or at least "Secret Sauce" in Secure Location
3. Exit interviews – emphasize the trade secret importance, consequences if misappropriation
4. Exit docs – sign statement saying nothing on personal computer, do not have company trade secrets or software
5. Logs – have computer checking regularly
6. Encryption keys – make sure all changed
7. Remote Storage locations – check to see whether any are linked for uploading, including BitBucket, AWS, Github, et al.
8. Keep a copy of your code in safety deposit box on disk or keep a copy of your code in an escrow account with a specific holder or inhouse, with attestation on separate drive/server which does not allow deletions/insertions

Trade Secret Best Practices

Your Trade Secret Policy Safeguard / IP Portfolio Strategy Should Also Provide For:

- **IDENTIFICATION** of security for trade secrets in your Company
- **DETERMINATION** re which trade secrets are of value and need to be protected by trade secret law or by patent/copyright law
- **LIMIT** the number of persons having access to the trade secret
- **PROVIDE** only parts (not the whole) of the trade secret to employee, where possible
- **AUDIT your trade secrets and security of same on a regular basis to ensure the above**

WHO should do this?

Person(s) in control of the relevant subject matter along with appropriate legal counsel.

Additional Notes:
Given DTSA whistleblower clauses et al., be sure your US employee contracts reflect the new law!

Thank You For Your Consideration!

Linda Shudy Lecomte, *Partner*
Wuersch & Gering LLP
100 Wall Street
New York, New York 10005 USA
Tel +1-212-509-4745
linda.lecomte@wg-law.com