Trade Secrets & Employee Mobility

Association of Corporate Counsel

August 19, 2020

BAKER BOTTS

Panelists

Sarretta McDonough

Associate General Counsel, Antitrust Commercial Litigation at Intel Corporation.
sarretta.mcdonough@intel.com

Neal Hannan

Managing Counsel, Fastly
nhannan@fastly.com

Cheryl Cauley

Partner, Practice Group Chair - Tech Litigation (Firmwide)
Baker Botts LLP
cheryl.cauley@bakerbotts.com

Jonathan Patchen

Partner, Practice Group Chair - Tech Litigation (Firmwide)
Baker Botts LLP
jonathan.patchen@bakerbotts.com

SECTION 01

INTRODUCTION

BAKER BOTTS

Why does this matter?

- Global Survey by Ponemon Institute & Symantec
  - 59% of employees leaving a job ADMIT to keeping corporate data when they leave
  - 40% ADMIT they intend to use the information in their new job
- Even before the current crisis, studies estimated U.S. companies were losing $300 billion/yr from trade secret misappropriation
- Particularly relevant to tech companies:
  - Tech companies depend largely on human capital
  - IP is a dominant output
- Trend is for *increased* employee mobility
  - E.g., Massachusetts Noncompetition Agreement Act (Aug. 2018)

COVID-19: Heightened Concerns

- Huge numbers of employees now working remotely
  - Decreased oversight
  - Unusual/different processes
- Layoffs and furloughs of employees
  - Morale & desperation
- Opportunistic hiring

Numerous Motivations

- Malicious intent
- Ego
- Curiosity
- Ignorance
- “Value Add”

Processes should be in place to try to address all

SECTION 02

LEGAL FRAMEWORK

BAKER BOTTS

Legal Framework

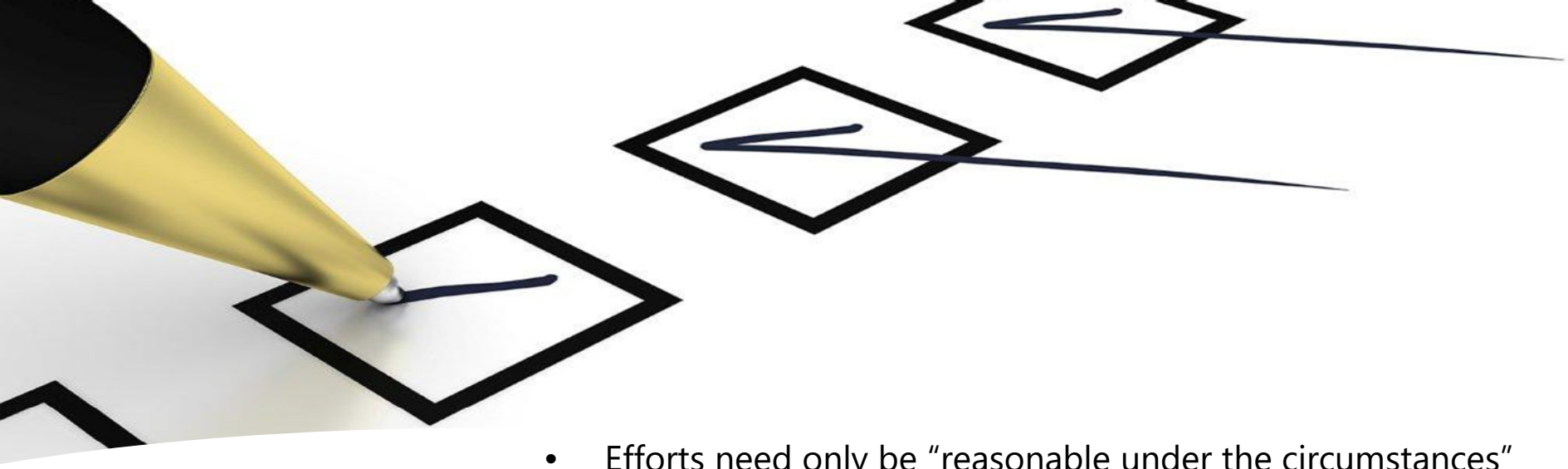
- Statutory Law:
  - Trade Secrets (State & Federal)
  - Computer Access & Use (State & Federal)
- Contracts

What Is a Trade Secret?

- A trade secret is *information* that:

  (1) derives independent economic value from not being generally known

  (2) is the subject of efforts that are reasonable to maintain its secrecy



"Reasonable Efforts"

- Efforts need only be "reasonable under the circumstances"
- Reasonable efforts can include:
  - advising employees of existence of trade secrets
  - limiting access to information on "need to know" basis
  - requiring employees and third parties to sign confidentiality agreements
  - keeping secret documents under lock
- "Reasonable" efforts change as circumstances change:
  - Size: 2-person startup versus Fortune 500
  - Technology: File cabinets versus Cloud accounts
  - Behavior: In the office versus remote work
  - Knowledge: Known versus unknown risks

Misappropriation

- Misappropriation of a trade secret:
  - Acquiring trade secret, directly or derivatively, by improper means
  - Disclosing *or* using a trade secret, without consent, if:
    - Improper means used to acquire
    - Derivatively acquired by improper means
    - Directly or derivatively subject to duty of secrecy
    - Accidentally obtained

Contracts

- Typical Contracts & Terms:
  - NDA
  - Confidentiality Agreement
  - Invention Assignment
  - Acceptable Use Policies
  - Non-Competes & Non-Solicits
  - Severance Agreements
  - Termination Certifications
- Inter-state Employee/Employer issues preclude universal advice

California — Contracts & Employee Mobility

- Business & Professions Code § 16600
  - Can be applied to California employees and California employers
  - Invalidates nearly all post-employment non-competes and customer non-solicits
  - Likely invalidates nearly all post-employment employee non-solicits
  - Potentially invalidates confidentiality agreements reaching beyond trade secret
- Consequence: Employees can — and do — easily move between jobs. Increases the emphasis on *non*-contractual protections:
  - Statute: trade secret & computer access
  - Common Law: duty of loyalty & conversion

SECTION 03

SPECIFIC SCENARIOS

BAKER BOTTS

Four Key Scenarios

SECTION 04

REMOTE WORK

BAKER BOTTS

Case Study: *Jawbone // Fitbit*

- Several employees of Jawbone left and joined Fitbit
- Jawbone sued Fitbit for trade secret misappropriation
- US Attorney's Office gets involved
- Indictments followed
  - Lead case: Trade Secret claim based on former employee retaining documents through use of "Crash Plan" backup software at home
  - Employee disclaimed knowledge
  - Jury acquittal

Risks of Remote Work

- Secrecy & Security:
  - "Reasonable" efforts are different; failure to adapt jeopardizes trade secrets
    - Unsupervised employees might more easily copy data
    - Employees may be using their own computers/phones without standard security measures
    - Employees may use systems that are not secure such as Zoom
    - Smart devices listening in
  - Systems employed in a rush to facilitate work at home may have security flaws
  - Disconnected workforce

- New Scenario; Different Processes

Prevention is the Best Cure

- Proactive Solutions Adapted to Business
  - Multi-disciplinary effort: HR, IT, Legal, others
- Solutions Include:
  - Training/Education
  - Technical Solutions
  - Policy Development

1. Training/Education

- Mandatory training associated with stay-at-home procedures
- Acknowledge what is different:
  - Personal devices
  - People — e.g., neighbors
  - Accessibility
- Provide training & written warnings to employees regarding confidentiality while working at home
- Create culture of mutual responsibility

2. Technical Solutions

- Audit what documents/devices are used and accessible
- Implement technical solutions:
  - Tracking employee copying/print/ email/download of data and company files
  - Logging & audit solution
  - Monitoring employee internet activity
  - Device tracking
  - Remote lock, wipe, and inspection
- Enhance employee home network security
- IT health: anti-virus, malware, spyware software

3. Policies

- Create — or upgrade — applicable policies:
  - Work from Home Policy
  - Personal Device (BYOD) Policy
  - Acceptable Use Policy

- Audit confidentiality agreements — ensure employees who may not otherwise have been working at home are bound by a confidentiality agreement or policy

- Re-evaluate the company's overall trade secret and confidentiality approach
  - Consider a "least privilege" model

SECTION 05

EMPLOYEE LAYOFFS & FURLOUGHS

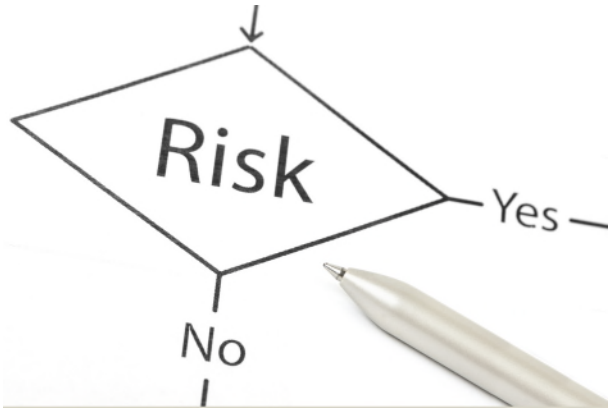
BAKER BOTTS

Case Study: *AMN Healthcare*

- Post-hoc efforts to obtain or reclaim confidential information may be ineffective
  - "section 16600 precludes an employer from restraining an employee from engaging in his or her 'profession, trade, or business,' even if such an employee uses information that is confidential but not a trade secret."

Risks of Employee Layoffs & Furloughs

- Employee Morale & Desperation
  - Increased incentive to misappropriate
- Volume
  - Overwhelm process
- Remote Working
  - Inadequate processes built for in-office terminations
- Speed/Suddenness
  - Failure to update forms; inadvertent exposure
  - E.g., employee non-solicitation clauses — leftover from pre-*AMN?*



Practical Solutions

- Procedures
- Monitoring

Procedures

- What "in office" procedures can be salvaged and repurposed?
  - The "Walk" → Remote lockout and forensic imaging
  - Exit interview and paperwork → Videoconference (recorded?) and e-Signature
  - Return Material → Messenger service or pre-paid FedEx label
- Make checklist covering every task that must be undertaken
  - E.g., Checklist of items needed to be returned: devices and documents
  - Critical not to miss key data sources that can quickly disappear: email; personal accounts left logged in; etc.
  - Coordinated across IT & HR — coverage and compliance
- Re-evaluate the company's overall termination approach:
  - E.g., Re-imagine the "termination certificate" — make a real process, including self-scrubbing, to promote compliance
  - Red-flag for employee who refuses to participate

Monitor Departure & Post-Departure Conduct

- Training off-boarding staff to be sensitive to evasive or unusual conduct in departure process
- Monitor where former employee lands — LinkedIn, etc. — for unusual activity or suspicious circumstances
  - E.g., accelerated development; directly competitive product; large group of employees all joining
- Carefully deploy the "warning" letters
  - Routine, suspicion-less letters can backfire and create exposure

SECTION 06

COLLABORATION & DEAL-MAKING

BAKER BOTTS

Case Study: *Mujae Group v. Spotify*

- Plaintiff meets with Spotify for potential partnership for ad creation
- Spotify passes; four months later debuts its own ad creation feature
- Plaintiff sues on April 30, 2020:
  - Appears to have had no written NDA; relied on oral assurances of confidentiality and limited use
  - Spotify employees took copious notes; not returned or destroyed
  - Gave, and never revoked, credentials to proprietary database

Risks with Third Parties & Collaboration

- Loss of regular processes
  - E.g., NDA upon sign-in
- Informal and impromptu collaboration
- Economic need prioritizes speed over security

Third Party Practices — Practical Solutions

- Paying proper attention to NDAs & trade secret protection despite less formal environment
  - Get legal out of the way: template, pre-signed NDAs, etc.
  - Make this an emphasis of training to external facing team: sales, support, etc.
  - Have a plan in place to have those documents available and able to be signed on the spot via DocuSign or another method
  - Do not share information via unsecure means, such as personal emails

- Virtual meeting best practices
  - Use secure virtual environments — passwords required
  - Create a clear record of who attended the meeting and what was disclosed
  - Consider embedded NDA — like the sign-in NDA — to join conference

SECTION 07

OPPORTUNISTIC HIRING

BAKER BOTTS

Case Study: *Waymo v. Uber*

- Waymo v. Uber
  - Google's self-driving car company, Waymo, sued Uber for theft of trade secrets by a former Google employee
  - Case settled: Waymo received a .34 percent stake in its business (worth around $245 million)

- Criminal Charges Brought
  - Former Google executive, Levandowski, charged with 33 counts of theft and attempted theft of trade secrets
  - He pleaded guilty to stealing trade secrets; 18 month prison term

Risks of Opportunistic Hiring

- Some tech companies will be in a position to snap up talent being shed by other companies in economic distress
- Employees may be *more* willing to voluntarily move:
  - Disaffected by current company approach
  - Risk/reward of startup versus established company
- Infection of new company IP
- Former company perception and reaction

Avoiding Contamination & Clear Signaling

- Hiring process procedures:
  - Clear policies communicated early in process
  - Pre-employment "scrub"
    - Most employees self-scrub and certify — create clear checklist to follow
    - Independent counsel for high value/high risk hires
- Consider voluntary, paid "garden leave" or "cooling period" for new employee
- Repeated, multi-channel, communication of policy to current employees
- Special attention to non-traditional employees:
  - E.g., consultants who concurrently consult for multiple companies
- Have a plan in place if any contamination is discovered:
  - Forensic preservation; leave for employee; outside counsel
- Consider the long-game: Reevaluate current employment documents to implement best practices for eventual exit (e.g., exit self-scrub)

SECTION 08

CONCLUSION

BAKER BOTTS

Panelists

Sarretta McDonough

Associate General Counsel, Antitrust Commercial Litigation at Intel Corporation.
sarretta.mcdonough@intel.com

Neal Hannan

Managing Counsel, Fastly
nhannan@fastly.com

Cheryl Cauley

Partner, Practice Group Chair - Tech Litigation (Firmwide)
Baker Botts LLP
cheryl.cauley@bakerbotts.com

Jonathan Patchen

Partner, Practice Group Chair - Tech Litigation (Firmwide)
Baker Botts LLP
jonathan.patchen@bakerbotts.com

AUSTIN

BEIJING

BRUSSELS

DALLAS

DUBAI

HONG KONG

HOUSTON

LONDON

MOSCOW

NEW YORK

PALO ALTO

RIYADH

SAN FRANCISCO

WASHINGTON

bakerbotts.com

Backup

Statutory Law

- Trade Secret Law
  - California Uniform Trade Secrets Act (“CUTSA”)
  - Federal Defend Trade Secrets Act (“DTSA”)
- Anti-Hacking
  - Computer Fraud & Abuse Act
  - Penal Code 502

Trade Secret

- Trade secret is *information* that:

  (1) derives independent economic value from not being generally known

  (2) is the subject of efforts that are reasonable to maintain its secrecy

Federal Trade Secret

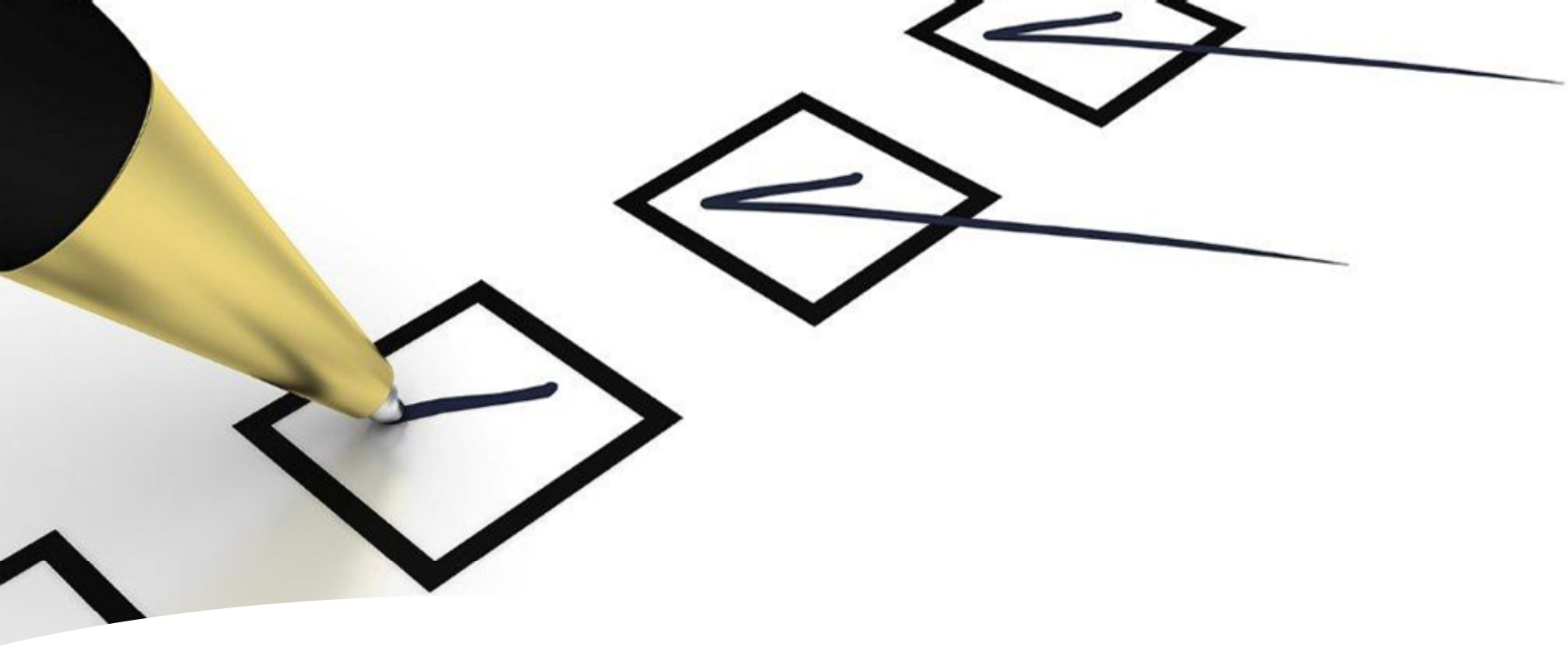
- Under DTSA a trade secret is *information* that:

  (1) the owner has taken reasonable measures to keep secret; and

  (2) derives independent economic value from not being generally known

Trade Secret Claim

- Plaintiff must allege:
  - (1) the existence of a trade secret
  - (2) misappropriation of a trade secret:
    - Acquiring trade secret, directly or derivatively, by improper means
    - Disclosure *or* Use of Trade Secret, without consent, if:
      - Improper means used to acquire
      - Derivatively acquired by improper means
      - Directly or derivatively subject to duty of secrecy
      - Accidentally obtained



"Reasonable Efforts"

- Efforts need only be "reasonable under the circumstances"
- Reasonable efforts can include:
  - advising employees of existence of trade secret
  - limiting access to information on "need to know" basis
  - requiring employees and third parties to sign confidentiality agreements
  - keeping secret documents under lock

Reasonable Efforts

"Under the circumstances"

- Required measures change as circumstances change.
- Size changes: 2-person startup versus Fortune 500
- Technological changes: File cabinets versus Cloud accounts
- Behavioral changes: In the office versus remote work
- Knowledge changes: Known versus unknown risks.
  - *Alamar Biosciences*

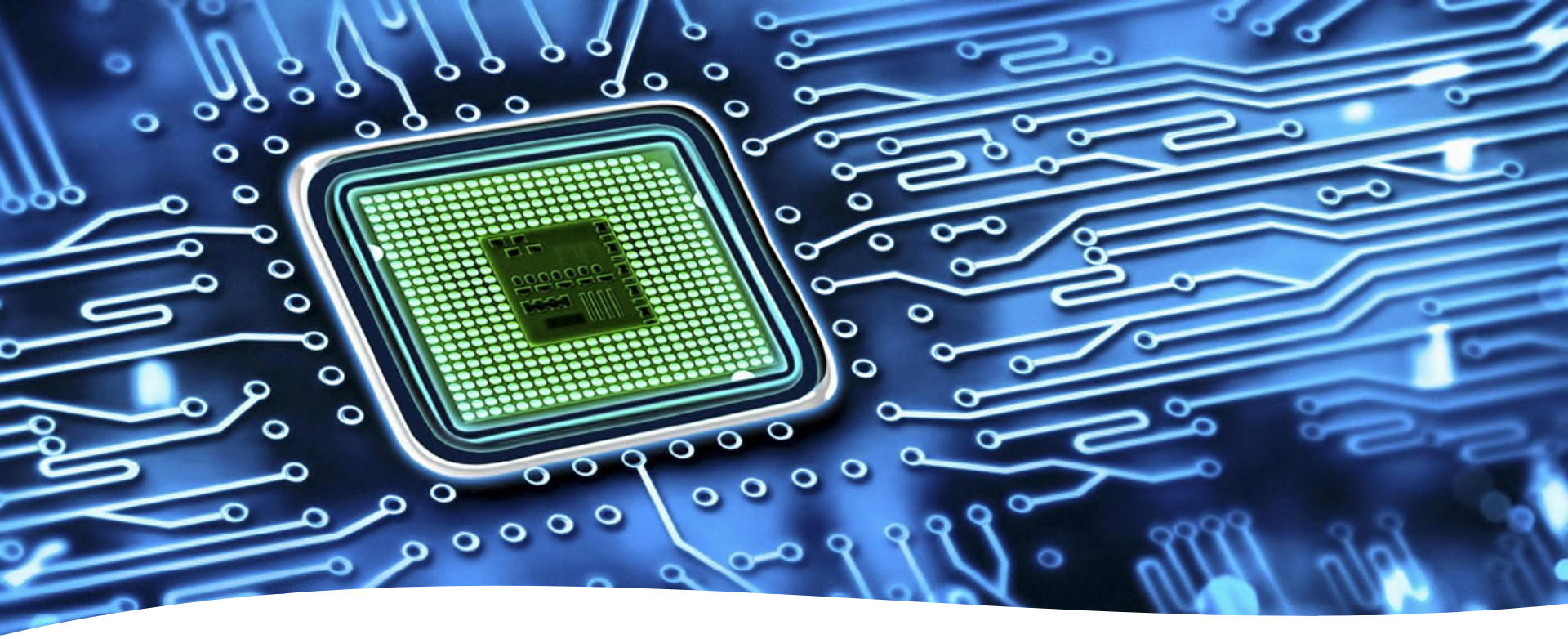
Anti-Hacking Statutes: California Penal Code § 502

- Prohibited conduct includes:
  - Knowingly accessing and without permission altering, damaging, deleting, destroying, or otherwise using any data, computer, computer system, or computer network in order to either:
    - (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or
    - (B) wrongfully control or obtain money, property, or data.
  - Knowingly accessing and without permission taking, copying, or making use of any data from a computer, computer system, or computer network, or taking or copying any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
  - Knowingly and without permission accessing or causing to be accessed any computer, computer system, or computer network.

Anti-Hacking Statutes: The Computer Fraud and Abuse Act ("CFAA")

- The CFAA prohibits unauthorized access to or damage to federal government computers, financial institution computers, or computers used in interstate and/or foreign commerce.

- Specific activity prohibited by CFAA includes:
  - 1) obtaining information without authorization or in excess of authorized access from a financial institution computer, government computer, or protected computer;
  - 2) accessing a computer without authorization or in excess of authorized access with an intent to defraud and obtain value;
  - 3) causing damage while either transmitting a program or intentionally accessing a protected computer; and
  - 4) trafficking in passwords with an intent to defraud.



Key Differences in Anti-Hacking Statutes

- Key Differences:
  - Lower damage threshold for Penal Code § 502
  - Statutory safe harbor in Penal Code § 502 employee misuse:
    - 502 (h)(1) provides an exception to liability for persons performing reasonably necessary acts within the scope of his or her lawful employment.
    - Note: *Van Buren v. United States*.

Contracts

- Typical forms: NDA or Confidentiality Agreement; Invention Assignment; Non-Competes & Non-Solicits
- *California* B&P Section 16600
    - "Every contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void."
    - Non-Competes — *Edwards*
    - Non-Solicits — *AMN/Barker*
    - Confidentiality Agreements? — *AMN*
    - "During Employment" — *Techno Lite*
- Non-employment context — NDAs between companies
- Acceptable Use/Permitted Behavior Policies for Computers & Networks

Non-Compete Agreements in California

- Generally, not permitted in California because of strong public policy against restraints on open competition

- Leading Case: *Edwards v. Arthur Andersen LLP*, 44 Cal. 4th 947 (2008)

  - The California Supreme Court invalidated a noncompete agreement that "prohibited [the plaintiff] from working for or soliciting certain…clients [of his former employer] for limited periods following" the plaintiff's termination from his job, finding the agreement to be an unlawful restraint on engaging in a lawful profession.

  - The Court explained that, "even if narrowly drawn," the agreement would violate Section 16600 as an unlawful restraint on the former employee's lawful profession.

Non-Compete Agreements in California (Cont.)

- "While Employed" Exception
  - *Techno Lite, Inc. v. Emcod, LLC,* 44 Cal. App. 5th 462 (2020)
    - Techno Lite sued two former employees who ran their own business while still working for Techno Lite, though both promised Techno Lite that they would do so on their own time and would not compete with the company.
    - After a break-down in the relationship, Techno Lite sued the employees, accusing them of fraud by falsely promising not to compete and misappropriating trade secrets, among other claims.
    - The employees argued that the fraud claim failed because the underlying promise—an agreement not to compete—was void under Section 16600
    - The Court created a "while employed" exception to Section 16600 and rejected an employee's challenge to a noncompete agreement
- Is "While Employed" broader than Duty of Loyalty?

Non-Solicit Agreements in California

- Employee Non-Solicit agreements are likely void in California under *Edwards* and California Business and Professions Code Section 16600

- *AMN Healthcare v. Aya Healthcare Services*, 28 Cal. App. 5th 923 (2018)

  - The AMN court held that the non-solicitation clause at issue was unenforceable
  - It also permanently enjoined the plaintiff-company from enforcing the clause against all other former employees.
  - In addition, the court awarded attorney fees to the defendants because, by successfully showing the non-solicitation clause was unenforceable, they "conferred a significant benefit on the public."

- Subsequent courts have not agreed with the narrow "travel nurses" reading.

Confidentiality Agreements in California?

- Protecting Trade Secrets by Contract?
  - Not likely in the employment context. *Dowell v. Biosense Webster*, 179 Cal. App. 4th 564 (2009)
  - Square with "reasonable efforts"?

- Protecting Non-Trade Secret, Confidential Information (e.g., Salary Info)
  - *AMN Healthcare* casts doubt: "section 16600 precludes an employer from restraining an employee from engaging in his or her 'profession, trade, or business,' even if such an employee uses information that is confidential but not a trade secret."

- What about non-employment context (e.g., NDAs)?
  - Does 16600 apply to business/business agreements? *Ixchel Pharma v. Biogen*, S256927 (CA9 Certified Question) — Sept. 2020

Case Study: *Jawbone // Fitbit* (Cont.)

- *Jawbone v. Fitbit*
  - Jawbone filed a lawsuit against Fitbit (both makers of wearable fitness trackers) alleging that former employees stole trade secrets and other information when they left the company to join Fitbit
  - Civil case eventually settled

- Criminal Charges Brought
  - Six people were indicted in Federal Court
  - The former employees were charged with violating confidentiality agreements they had signed with Jawbone after they accepted employed with Fitbit
  - Evidence used by Prosecution centered around Jawbone documents found on employees' personal devices
  - Jury acquitted one employee; Prosecutors dropped the other charges

GRAVEYARD

Computer Use Statutes – CONSIDER DROP

- Federal & State Laws
  - Federal Computer Fraud & Abuse Act; California Penal Code § 502
- Prohibited Conduct Includes
  - Accessing, without permission, to extort
  - Access, without permission, for copying or making use of data
  - Access, without permission, of computer system
- Difficult Employee/Employer Question: Exceeding Authorized Access
  - Statutory safe harbor (Penal Code) — § 502(h)
  - Statutory interpretation (CFAA) — *Van Buren v. United States* (cert. granted)