ACC Association of Corporate Counsel SAN DIEGO

BELIEVE IT OR NOT

COVID-19 CAN INJURE YOUR TRADE SECRETS AND CAUSE AN OUTBREAK OF MISAPPROPRIATION CLAIMS

Part 2: Best Practices To Protect Your Trade Secrets

February 24, 2021

Presented By:
Elizabeth Balfour, Partner, Sheppard Mullin
Rebecca (Bec) Edelson, Partner, Sheppard Mullin
Rebecca Hanovice, Associate General Counsel of Callaway Golf Company

1

1

Presenters

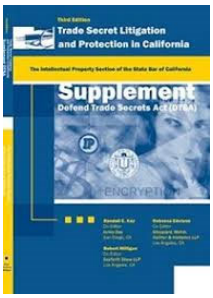
Moderator	Panelist	Panelist
Elizabeth Balfour Partner Sheppard Mullin	**Rebecca (Bec) Edelson** Partner Sheppard Mullin	**Rebecca Hanovice** Associate General Counsel of Callaway Golf Company
Elizabeth handles commercial litigation, including cases involving breach of contract, indemnification claims, enforcement of buy-sell agreements and other disputes arising out of corporate transactions. She counsels clients on document retention, insurance coverage and corporate governance matters. ebalfour@sheppardmullin.com	Bec leads her firm's trade secret practice and is a seasoned business litigator and represents businesses in intellectual property, unfair competition, injunction and other litigation matters. Bec has unmistakable expertise in the trade secrets arena. She is the co-editor and co-author of the treatise, *Trade Secret Litigation and Protection in California*. redelson@sheppardmullin.com	Rebecca created and manages the corporate privacy program at Callaway Golf. She is particularly knowledgeable in the areas of data privacy law, litigation management, patent law and licensing. Rebecca is a Certified Information Privacy Professional – Unites States (CIPP/US) and a USPTO licensed patent attorney. rebecca.hanovice@callawaygolf.com

2 2021 ACC San Diego In-house Counsel Conference

2

Trade Secret Litigation and Protection in California

This twenty-seven chapter treatise provides a comprehensive review and analysis of California trade secret law. (Third Edition, 2014.)



This Supplement to the Third Edition practice guide addresses the Defend Trade Secrets Act (DTSA), which was enacted in 2016.

3

Agenda

I. COVID-19
II. Trade Secret Risks and Potential Proactive Measures
   - Work-From-Home
   - Videoconferencing
   - Layoffs

4

COVID-19 Polling Questions

1. Since the COVID-19 pandemic began, has your company increased its use of a remote work force?
2. Since the COVID-19 pandemic began, has your company increased its use of video-conferencing?
3. Since the COVID-19 pandemic began, has your company implemented new policies regarding use of confidential information while working from home or video-conferencing?

5

Trade Secret Basics

- Trade secret = information that:
  - Is not generally known in the business
  - Derives economic value from its secrecy (our competitors would love to get their hands on it) and
  - Is the subject of reasonable efforts to maintain its secrecy
- Misappropriation =
  - Improper acquisition, use or disclosure (e.g., in breach of a confidentiality agreement)

6

Patent vs. Trade Secret Protection

Patent	Trade Secret
Public invention	Secret information
Finite monopoly	Potentially indefinite but no true monopoly

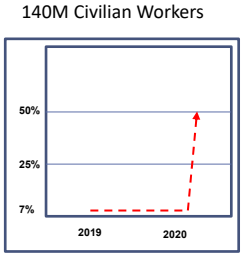
Thus, if there is a choice:

- Consider trade secret protection if the invention is likely to be valuable for longer than the patent monopoly period and can be kept secret.
- Recognize that there may there may be other reasons for opting for patent protection.

7

COVID-19 and WFH

- As a result of COVID-19, many businesses (especially those in states or cities with "stay at home" orders) have implemented a work-from-home ("WFH") directive for employees and independent contractors.
- Important for businesses to address the security of their trade secrets in this new environment:
  - Reduce risk of misappropriation of their trade secrets
  - Reduce risk that their confidential information may lose its status as trade secret.
- We offer some potential steps businesses can take to protect trade secrets given this fundamental change to WFH.
- Current trade secrets policies should be revisited.



8

Potential Directives to Workers During WFH

- Memorialize efforts to protect trade secrets.
- It is their responsibility to ensure that confidential information remains confidential while they WFH.
  - Reference provisions in agreements.
  - Proactively watch for potential vulnerabilities.

9

Aside: Review your confidentiality agreements for vulnerabilities!

- *E.g., Brown v. TGS Management* case from 2020 (overbroad employee confidentiality agreement can be a de facto non-compete agreement which is unlawful under Business & Professions Code 16600).
- Will your employee confidentiality agreements withstand scrutiny?

10

Potential Directives to Workers During WFH (cont.)

- Educate employees as to the reason for these measures.
- Employees may find the measures unduly burdensome and be resistant.
- Employees need to understand the importance of trade secrets to the company.
  - Not just risk of misappropriation.
  - Also, the risk that the trade secrets will lose their trade secret status if the company does not implement reasonable steps to keep them secret.

11

Potential Directives to Workers During WFH

- Remind workers that although they may be working in their pajamas, they must follow the rules to protect confidential information. E.g.,
  - they need to use confidentiality legends and
  - follow other procedures required by NDAs.

12

Potential Directives to Workers During WFH

- Prohibit transmitting or maintaining confidential information except as authorized by the company
  - Address personal email accounts, cloud accounts, social media, etc.
- Require them to keep their homes locked to the extent confidential information is maintained there.
  - Ideally, should work in a room to which only they have access.
  - Be vigilant not to inadvertently give others access to company's confidential information.

13

Potential Directives to Workers During WFH

- Don't unnecessarily print sensitive documents.
  - If hard copy confidential materials are needed, don't discard them in ordinary trash. Instead, shred.
  - If can't shred, retain in secure (locked) locations at home so they can be securely disposed when next at the office.

14

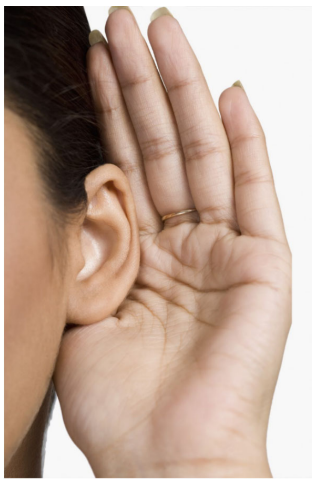
Potential Directives to Workers During WFH

- Connect to your network as securely possible, such as through a VPN (Virtual Private Network).
  - Consider requiring two-factor authentication for access.
- Password-protect home WiFi system.
- Work with IT personnel so that communications are encrypted.
- Consider software that requires email recipient to possess a designated digital signature to review messages and open attachments.

15

Potential Directives to Workers During WFH

- If possible, perhaps prohibit workers from transmitting trade secret information via email altogether.
- Instead, consider using secured shared drives with limited access rights.
- Home assistant devices (ex. Google Home, Alexa) should be turned off.



16

Potential Directives to Workers During WFH

- Home computer screens should lock up after a set period of time of non-use (ex. 5 minutes) and require passwords to unlock the screens.
- Limit trade secret materials at home to those needed for current projects.
- Give employees specific “go to” person at the company for any questions or concerns.

17

Potential Directives to Workers During WFH – Malicious Emails

- Educate workers about malicious emails.
  - Bad actors are sending emails and other malicious messages regarding purported Covid-19 tips to entice users to open malware.
  - Open messages from trusted sources only.
  - Send suspicious messages to IT team.
- Malicious cyber attacks is a huge issue.

18

Potential Directives to Workers During WFH – Malicious Emails (cont.)

- With the move to WFH, employers have made it easier for their remote work force to access their systems but that also can make it easier for the bad guys to access the company's systems remotely.
- Legacy devices are back doors that your company should close.
- Consider updating devices and programs to reduce the risk.
- Consider denying foreign access.

19

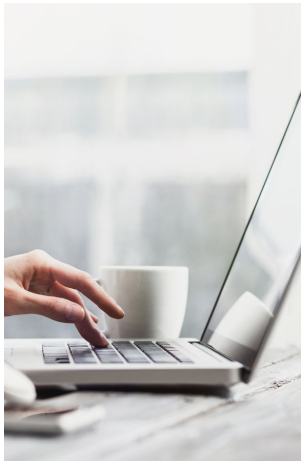
Potential Technical Procedures

- Develop a system to account for all confidential information maintained at workers' homes.
- Create a check-out/check-in process for your workers to use with confidential documents.
- If possible, issue laptops that have anti-virus/malware applications installed and that do not have USB ports.
- Implement a system that notifies your IT department whenever a worker downloads, copies, prints, or deletes a significant amount of data from your business's network.
- If practical, implement remote lock-out and wipe capabilities.

20

Third Parties

- Trade secret protection goes beyond regulation of immediate workforce.
  - Vendors, investors, consultants, suppliers, outside professionals with access to your business's trade secrets.
- Ask what they are doing to protect your trade secrets during the COVID-19 pandemic.
- If you receive an unsatisfactory response, investigate and take appropriate action.



21

Hidden Dangers to Videoconferencing

- Video conferencing -- new popularity in these COVID-19 times
  - "[Zoom] reached more than 200 million daily users [in March 2020], up from 10 million in December….".
- Risk to Trade Secrets
  - Reports of unauthorized access to video conferences.
    - "Thousands of Zoom video calls left exposed on open Web," The Washington Post, April 3, 2020.
    - Not an indictment of Zoom. Zoom addressed.
    - But businesses need to be mindful and implement security measures available and to use provider that offers security.

22

Videoconferencing Best Practices

- Confirm that the video conference is secure.
- Admonish their employees to:
  - Use the video conference application's security features (g., password-protect the video conference; lock the meeting; do not share publicly the meeting ID and/or password).
  - "Kick-out" participants that are not invited to the video conference which they are hosting. If they are not hosting the video conference, contact the host to request that the unauthorized participant be kicked-out.
  - Understand how the private break-out session feature works before sharing information there. Otherwise, other participants to the main video conference may inadvertently be given unintended access to the "private" room and, thus, confidential information.

23

Videoconferencing Best Practices (cont.)

- Know with whom they are chatting when they use the written chat feature. Otherwise, they may find what they thought was a private chat with certain participants was, instead, a chat with all participants and they mistakenly disclosed confidential information to unintended recipients.
- Be aware that the recording feature on some video conference applications records the entire session including private chats.
- Master the "share screen" function so that they do not mistakenly share a screen with confidential information on it. Close everything on their computers that they will not be sharing during the video conference.

24

Videoconferencing Best Practices (cont.)

- Be mindful not to inadvertently circumvent secured access to video conferences.
- Understand the definition of end-to-end encryption as it is provided by the video- conference provider. Although participants that use the native application may have the benefit of encryption, participants that use "out of scope" systems may not (g., cellular connections, landlines, and legacy video teleconferencing systems).

25

Videoconferencing Best Practices (cont.)

- Provide tip sheets to the company's employees.
- Establishing mandates to avoid having to rely on the cooperation of the employees (e.g., set up the video conference settings so that use of passwords is required).
- IT departments should review back-end settings and enforce secure configurations and implement software updates.

26

Videoconferencing Best Practices (cont.)

- The "Record" Feature – A Not So Obvious Concern.
- Risk to Trade Secrets -- businesses may be shocked to learn that their confidential information is no longer confidential.
  - See "New Zoom User Blow: This Is How 'Thousands' Of Video Chats Are Available For Anyone To View Online, " Forbes, April 4, 2020: "…thousands of Zoom videos are available online for anyone to see. The videos include sensitive chats such as business meetings…".)

Videoconferencing Best Practices (cont.)

- Best Practices
  - Exercise careful control over recordings and attempt to ensure that any recordings are maintained securely.
  - Watch for indications that a video conference is being recorded (e.g., a notice that it will be recorded, or a red-light recording message) and raise an objection to the host if recording the video conference is unwanted.
    - Keep in mind that it is easy to record a video conference session discretely with a mobile phone (or other technologies).
    - If recording is undesired, confirm expressly that no one is recording the session.

Videoconferencing Best Practices (cont.)

- Best Practices
  - Get an appropriate NDA in place beforehand.
  - To the extent that only one participant's confidential information is going to be shared during the video conference, ideally that participant should seek to host the video conference
    - It can control whether the video conference is to be recorded and confirm with the other participants that they will not attempt to record.
  - Designate the video conference as confidential in accordance with the procedures set by the NDA.
    - While the participant may have designated a writing shared during the video conference by labeling it "confidential" the NDA may require the participant to also designate as "confidential" what was said about it.

29

Videoconferencing Best Practices (cont.)

- Best Practices
  - If the video conference is recorded and the other participants are permitted to receive a copy of the recording, the host should also be mindful to designate the video conference recording as confidential pursuant to the terms of the NDA.
  - If multiple participants' confidential information is going to be shared during the video conference, address in advance of the video conference: (1) which participant will host the video conference; (2) whether a recording of the video conference should be made; and (3) if a recording is to be made, confirmation that the host will provide permission to the other participant to record as well.
    - Ordinarily, if one party to the NDA has a record of a communication between the parties, it is in the other party's interest to have a copy as well.

30

Videoconferencing Best Practices (cont.)

- Best Practices
  - Consider whether to address expressly in their NDAs the treatment of video conference recordings. E.g.:
    - Recordings may not be made without consent of the party whose confidential information is to be addressed during a video conference.
    - No recordings including confidential information may be uploaded or maintained in an unapproved cloud service.
    - Address the disposition of recordings at the end of the relationship (such as whether they are to be returned or destroyed; whether an archival copy may be retained if the party continues to maintain it securely).
    - Otherwise, recordings of video conferences – a relatively new category of "documents" subject to an NDA – may be overlooked and give rise to potential claims for breach and/or misappropriation of trade secrets.

Protect Your Trade Secrets During COVID-19 Layoffs

- Massive layoffs resulting from the COVID-19 pandemic
  - News Release, Bureau of Labor Statistics, USDL-21-0002, "In December [2020], both the unemployment rate, at 6.7 percent, and the number of unemployed persons, at 10.7 million"…"were nearly twice their pre-pandemic levels in February [2020] (3.5 percent and 5.7 million, respectively)."

Protect Your Trade Secrets During COVID-19 Layoffs

- Risk to Trade Secrets -- Employee mobility inherently increases the potential for compromise of trade secrets.
  - An angry laid-off employee retaliates by taking the only record of the trade secret (or otherwise concealing a trade secret from the employer), or by placing the employer's trade secrets on the Internet.
  - A competitor hires the laid-off employee to benefit from her insider knowledge of her former employer's trade secrets.
  - A laid-off employee sells his former employer's trade secrets as a source of income because he is unable to find a new job.

33

Protect Your Trade Secrets During COVID-19 Layoffs (cont.)

- Best Practices
  - Resist the temptation to give the short shrift to the usual protocols for terminations.
    - May be easier said than done (e.g., the sheer number of terminations in a relatively short period).
  - Mandate that employees promptly disclose during the employment any inventions or other trade secrets that they develop for the employer.
    - Before notice of termination, ask the employee about whether there are any inventions or trade secrets that they have not yet disclosed. Keep an informal tone in these discussions.

34

Protect Your Trade Secrets During COVID-19 Layoffs (cont.)

- Best Practices
  - Conduct an exit interview with the employee even if it has to be conducted by phone or video conference.
    - Can expose an intent by a particular employee to misappropriate
      - if she repudiates her duty to hold the employer's trade secrets in trust;
      - if she refuses to return confidential materials of the employer;
      - if she misstates her new employment.

35

Protect Your Trade Secrets During COVID-19 Layoffs (cont.)

- Best Practices
  - Send a letter to the terminated employee, reminding the employee of her ongoing obligations to protect the employer's trade secrets.
  - Make sure that the employee returns all company property, including materials that contain its confidential information.
    - Probe with the employee whether any trade secret materials of the employer are
      - at the employee's home
      - maintained by the employee on the employee's personal email and/or cloud storage accounts and/or USB and hard drives.
  - Remove the employee's access to its trade secrets (deactivate the employee's email accounts and passwords).

36

Protect Your Trade Secrets During COVID-19 Layoffs (cont.)

- Best Practices
  - If misappropriation is threatened, preserve all potentially relevant evidence.
  - Even if misappropriation is not threatened at termination, preserve for some period the employee's computer and other devices.
  - Watch for misappropriation by the terminated employee
    - abnormal downloads
    - astonishing innovations by the new employer in an unusually short period of time.
  - If misappropriation is perceived, do not sit on the concern.

37

Fluid Situation

- There is no one-size-fits-all approach to protecting trade secrets.
- Each business must assess what is "reasonable under the circumstances" to maintain the secrecy of its trade secrets.
- Depends on the business's size, sophistication and resources.
- A business facing the current COVID-19 environment should consult with its legal counsel to assess reasonable steps it should take to maintain secrecy of its trade secrets that are tailored to its specific business.

38

Questions?

Moderator	Panelist	Panelist
Elizabeth Balfour Partner Sheppard Mullin	**Rebecca (Bec) Edelson** Partner Sheppard Mullin	**Rebecca Hanovice** Associate General Counsel of Callaway Golf Company
Elizabeth handles commercial litigation, including cases involving breach of contract, indemnification claims, enforcement of buy-sell agreements and other disputes arising out of corporate transactions. She counsels clients on document retention, insurance coverage and corporate governance matters. ebalfour@sheppardmullin.com	Bec leads her firm's trade secret practice and is a seasoned business litigator and represents businesses in intellectual property, unfair competition, injunction and other litigation matters. Bec has unmistakable expertise in the trade secrets arena. She is the co-editor and co-author of the treatise, *Trade Secret Litigation and Protection in California*. redelson@sheppardmullin.com	Rebecca created and manages the corporate privacy program at Callaway Golf. She is particularly knowledgeable in the areas of data privacy law, litigation management, patent law and licensing. Rebecca is a Certified Information Privacy Professional – Unites States (CIPP/US) and a USPTO licensed patent attorney. rebecca.hanovice@callawaygolf.com

39

Please complete the program evaluation by opening your mobile device camera and scanning this QR code.

Disclaimer: This presentation is provided for information purposes only and does not constitute legal advice and is not intended to form an attorney client relationship. Please contact your Sheppard Mullin attorney for additional information.

40

Thank you!

Disclaimer

This presentation is provided for information purposes only and does not constitute legal advice and is not intended to form an attorney client relationship. Please contact your Sheppard Mullin attorney for additional information.