# THE UPDATE

SPRING 2023 | ISSUE 9

SAN DIEGO
DEFENSE LAWYERS

# PRESIDENT'S MESSAGE

Greetings SDDL members. This is my first chance as President to say hello to the many defense counsel out there I have not had an opportunity to yet meet. I want to thank our sponsors and everyone who was able to attend our Installation Dinner at Loews Coronado. It was great to be able to gather in person to honor Hon. Tamila E. Ipema (Ret.) and Susan Hack, Esq. for their achievements and their dedication to the San Diego legal community. The Board is grateful to our members and sponsors for the support we received throughout last year. Because of you, it was a success.

I am excited to take on this year as President of the San Diego Defense Lawyers. I am equally as excited to take on this year with a phenomenal Board of Directors. The Board has been hard at work planning our monthly Lunch & Learns for the year, in-person quarterly social events and happy hours. Our first quarter Happy Hour was in April at the Carnitas Snack Shack, and in the spirit of cross-bar relations, in March we co-sponsored "A View From the Bench" Judge's Panel with CASD. We are lucky to have active, engaged leaders in the various Bar-related organizations and we hope to see more joint activities in the near future. This year we will continue the tradition of the Padres tailgate and trivia night. In addition, mark your calendars for the upcoming SDDL Golf Tournament. If it's not broke don't fix it, this year's event will once again take place at Rancho Bernardo Inn Golf Course, on September 22, 2023. Finally we are pleased to announce that our annual mock trial competition is back! We are looking forward to hosting approximately 16 schools in this years competition which will be held in October, please let us know if you would like to be involved.

We will, of course, keep you apprised of the details for all of our social events as we get closer to them.

I look forward to a great year, and hope to see you at the next event.

Aloha, Low


# Exercise Caution and Do Not Disclose Confidential Information to AI Programs

*By Ian R. Friedman*
*WINGERT GREBING BRUBAKER & JUSKIE*

It is hard to go a day or two without getting an email about some new virtual assistant application (i.e., ChatGPT or Bing Chat). While these tools can greatly increase attorney efficiency with things like preparing sample demand letters or draft agreements, it is important to understand how these programs learn and the ethical concerns raised by sharing potentially privileged and/or confidential information with these computers.

First, some background. Virtual assistants are large language models designed to learn from the information they receive from users and the internet at large. This means that all information shared with a virtual assistant becomes part of the database to be accessed and analyzed when future users make requests.

As a basic refresher, California Rules of Professional Conduct, Rule 1.6 requires "A lawyer shall not reveal information protected from disclosure by Business and Professions Code section 6068, subdivision (e)(1) unless the client gives informed consent, or the disclosure is permitted by paragraph (b) of this rule."

Under the State Bar Act, an attorney has a duty "[t]o maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client." (Cal. Bus. & Prof. Code, § 6068, subd. (e) (1).)

The State Bar of California Standing Committee on Professional Responsibility and Conduct ("COPRAC") has attempted to explain how a lawyer's duty to maintain client confidences is impacted by modern technology. (See Formal Opinion No. 2010-179 [addressing whether an attorney violates "the duties of confidentiality and competence he or she owes to a client by using technology to transmit or store confidential client information when the technology may be susceptible to unauthorized access by third parties"].)

COPRAC has outlined "appropriate steps" lawyers should evaluate before using any particular technology in their law practice: "1) the level of security attendant to the use of that technology, including whether reasonable precautions may be taken when using the technology to increase the level of security; 2) the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information; 3) the degree of sensitivity of the information; 4) the possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product; 5) the urgency of the situation; and 6) the client's instructions and circumstances, such as access by others to the client's devices and communications."

Virtual assistants fail in almost every element of the precautions outlined by COPRAC. These programs admit that once information is shared with the assistant, that information becomes part of a larger network of data to be analyzed and used for purposes beyond the client's control.

For example, imagine summarizing a meeting with a client and then submitting a draft letter to a virtual assistant to clean up the writing. Immediately, all information from the client meeting is then saved in the virtual assistant database. That information is then free to be regurgitated to another user in the future if someone asks a question focusing on a similar subset of facts. While the client's name may not be tied to the second output, it is not hard to envision an instance where a competitor or litigation adversary could search for similar information and then learn secret information about your client.

In fact, this exact situation just came up in the context of an involuntary trade secret disclosure by Samsung employees. There, an employee used an AI tool to help fix a source code question and inadvertently disclosed Samsung's trade secret source code and made it available to competitors. (See https://www-businesstoday-in.cdn.ampproject.org/c/s/www.businesstoday.in/amp/technology/news/story/samsung-employees-accidentally-leaked-company-secrets-via-chatgpt-heres-what-happened-376375-2023-04-06.)

If you or any member of your firm are going to use a virtual assistant, it is always good practice to keep clients informed and obtain their informed written consent regarding what information can and cannot be shared with any virtual assistant. This way it is the client's decision regarding how this technology is used.

While virtual assistants, like ChatGPT, can be helpful in many contexts, clients and attorneys should be aware of the potential risks involved in sharing confidential information. Attorneys must understand the dangers of disclosing such information to virtual assistants to that client confidentiality is maintained and respected in all settings.

# California Federal Court Maintains Broad Duty of Insurer to Defend

*By Samuel Frasher*
*TYSON MENDES*

A California federal court has held that the potential for coverage underlying lawsuits arising from the September 2020 Bobcat Wildfire "is clear" and requires Greenwich Insurance Company to defend Southern California Edison Co. as an additional insured under a policy it issued to a vegetation management company whose negligence allegedly caused the wildfire.

## FACTS AND ANALYSIS

Under California law, a liability insurer owes a broad duty to defend its insured against claims that create a potential for coverage.[1] This broad duty encompasses claims that are "merely potentially covered" considering the facts alleged[2] and does not require a showing of actual liability or evidence supporting the claims alleged.[3]

In an opinion issued in January [4], the Eastern District of California held that detailed allegations of negligence in 20 underlying lawsuits against Utility Tree Service (UTS) establish the potential for coverage under the policy.

Edison contracted with UTS to manage vegetation maintenance around its power lines to prevent potential tree-to-conductor contact which allegedly occurred in September 2020 according to the lawsuits. The contract required UTS to have insurance with excess coverage for wildfire liability that lists Edison as an additional insured if UTS negligently performed maintenance.

Greenwich argued that it had no duty to defend Edison without any allegations of negligence levied against the named insured, UTS.

The Court disagreed, reasoning that a bare possibility of liability is all that is required to obtain coverage—saying that it was "reasonable to infer that [SCE's] liability (if any) may arise from UTS's acts or omissions" which triggers Greenwich's duty to defend under the contract. [5]

## TAKEAWAY

This decision echoes the chorus California courts have maintained for decades: construe the duty to defend broadly and in favor of policyholders wherever possible. If there is any possibility for coverage under an insurance policy based on the complaint's allegations, the insurer must defend its insured against the entire lawsuit unless it can prove with undisputed facts to the contrary.

[1] *Horace Mann Ins. Co. v. Barbara B. (1993) 4 Cal.4th 1076, 1081.*

[2] *Buss v. Superior Court, (1997) 16 Cal.4th 35, 46.*

[3] *Isaacson v. Cal. Ins. Guarantee Ass'n (1988) 44 Cal. 3d 775, 793.*

[4] *Southern Cal. Edison Co., et al. v. Greenwich Ins. Co. (E.D. Cal. Jan. 18, 2023) No. 2:22-cv-05984-JFW-JEM.*

[5] *Id.*