

THE UPDATE

SUMMER 2020 | ISSUE 2



SAN DIEGO
DEFENSE LAWYERS



IN THIS ISSUE

4. Client Confidences

While Working from Home

5. Lawyer's Obligations

After an Electronic Breach of Cyberattack

6. The Price of Incivility

8. New Emergency Law Passed by California Governor

Which Provides for Worker's Compensation Liability When Workers Get COVID-19

9. COVID-19 Puts Inequality Under a Microscope

10. Past Presidents – Then and Now

13. California Supreme Court Favors

Policy Holders in Excess Insurance "Vertical Exhaustion" Decision

14. California Case Summaries

15. The New Discovery Obligation

Imposed by CCP 2031.280(a) and How Civil Litigators Should Respond

MEMBERSHIP INFORMATION

Membership is open to any attorney or paralegal who is primarily engaged in the defense of civil litigants, as well as retired defense attorneys. Dues are \$125.00 for new members for the first year and \$160.00 per year for renewing members. The dues year runs from January 1 to December 31. Applications can be downloaded at: sddl.org.

The Update is published for the mutual benefit of the SDDL membership, a non-profit association composed of defense lawyers in the San Diego metropolitan area. All views, opinions, statements and conclusions expressed in this magazine are those of the authors, and they do not necessarily reflect the opinions or policies of the SDDL or its leadership. The SDDL welcomes the submission of articles by our members on topics of general interest to its membership.



**SAN DIEGO
DEFENSE LAWYERS**

2020 SDDL UPDATE

Editors-in-Chief | David Hoynacki, Rachel Fisher, Codie Dukes

Design | April Woodard Design
www.aprilwdesign.com

2020 SDDL OFFICERS

President | N. Ben Cramer
Carroll, Kelly, Trotter & Franzen

Vice-President | Vanessa C. Whirl-Grabau,
Thomas Lucas

Treasurer | Lawrence Zucker, Haight Brown
and Bonesteel

Secretary | Christine Y. Dixon, Dunn DeSantis
Walt & Kendrick

Executive Director | Dianna Bedri-Burke

2020 SDDL DIRECTORS

Rachel A. Fisher
Neil Dymott Frank McCabe & Hudson

Nicole Melvani
Neil Dymott Frank McCabe & Hudson

David Hoynacki
Wilson Elser Moskowitz Edelman & Dicker

Codie Dukes
Tyson Mendes

Ian Friedman
Wingert Grebing Brubaker & Juskie

Danielle C. Hicks
Dummit Buchholz & Trapp

Nicholas Schechter
Tyson Mendes

SDDL UPDATE c/o David Hoynacki
Wilson Elser, 401 West A Street, Suite 1900,
San Diego, CA 92101
P: 619.321.6208
david.hoynacki@wilsonelser.com



What Must Lawyers do to Maintain Client Confidences While Working From Home?

By Ian R. Friedman, Esq.

As the COVID-19 Pandemic persists, law firms and lawyers continue to face previously unanticipated ethical issues associated with unique forced work-from-home circumstances. While most attorneys understand how the duty of confidentiality applies when working in an office, new issues arise when lawyers work from home.



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. This intersection is now particularly prevalent with much of the work force working from home for the first time.

In Formal Opinion No. 2010-179, the State Bar considered “Does an attorney violate 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?”

There, COPRAC 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.”

In Formal Opinion No. 2012-184 COPRAC considered ethical issues associated with lawyers running a “Virtual Law Office” or “VLO.” There, it was determined that “[w]hile an attorney may maintain a VLO in the cloud where communications with the client, and storage of and access to all information about the client’s matter, are conducted solely via the internet using a third-party’s secure servers, Attorney may be required to take additional steps to confirm that she is fulfilling her ethical obligations due to distinct issues raised by” the VLO environment.

Recommended additional steps relevant to today’s work from home environment include establishing a secure VLO by conducting “reasonable due diligence both in the selection, and then in the continued use, of the VLO vendor”; ensuring the VLO vendor “employs policies and procedures that at a minimum equal what

Some specific issues that immediately come to mind are:

- What precautions must lawyers take when using their in-home Wi-Fi?
- May a lawyer allow other persons inside their home to access the Wi-Fi if confidential client information could be accessed?
- What precautions must be taken to prevent family members from overhearing the lawyer’s calls/zoom conferences when working from home?
- What in-home encryption requirements must be satisfied to keep client information secure?
- How must hard copy client files be secured in the home?

There are obviously many other potential issues; this only scratches the surface.