



The State Bar of California

Task Force on Access Through Innovation of Legal Services – Subcommittee on Unauthorized Practice of Law and Artificial Intelligence

To: ATILS Task Force
From: Subcommittee on UPL and AI
Date: June 28, 2019
Re: B.5. Recommendation: Regulated entities should be required to provide enhanced privacy and data security protections, scalable to consumer risk. At a minimum, they should also be required to comply with the equivalent ethical standards required of lawyers.

Recommendation not yet voted on by the Task Force: Regulated entities should be required to provide enhanced privacy and data security protections, scalable to consumer risk. At a minimum, they should also be required to comply with the equivalent ethical standards required of lawyers.

(Recommendation and Report approved by the Subcommittee – 5 yes, 0 no, 0 abstain)

How the Recommendation Relates to the Charter: This recommendation addresses Task 3 of the Charter.

3) With a focus on preserving the client protection afforded by the legal profession's core values of confidentiality, loyalty and independence of professional judgment, prepare a recommendation addressing the extent to which, if any, the State Bar should consider increasing access to legal services by individual consumers by implementing some form of entity regulation or other options for permitting non lawyer ownership or investment in businesses engaged in the practice of law, including consideration of multidisciplinary practice models and alternative business structures.

Pros: Requiring enhanced privacy and data security protections protects the public from risks concentrated to technology providers. Requiring compliance with equivalent ethical standards required of lawyers at a minimum ensures users will receive the same protections they would get from a lawyer. By doing so, it also enhances the confidence and trust in the administration of justice.

Cons: Application of these principles will increase the barriers to entry for technological providers, perhaps substantially. This would reduce consumer access to services. The certifying entity will have to ensure that the standards and protocols are not unduly burdensome as a matter of practice, and that it is straightforward and adoptable by a large number of entities. It may impose significant costs on technology providers to meet minimum security requirements and that cost may be passed on to the consumer.