UPL-AI Agenda Item B.6.
05-13-19 Meeting

The State Bar
of California

Task Force on Acc
of Legal Services – Subcommittee on
Unauthorized Practice of Law
and Artificial Intelligence

To: Subcommittee on Unauthorized Practice of Law and Artificial Intelligence
From: Simon Boehme and Daniel Rubins
Date: May 2, 2019
Re: B.6. Recommendation: If an entity is permitted to practice law using technology, then that entity should be required to provide adequate data security.

Section V(D)(3) of the UPL/AI Report

Data security is critical to preserving client trust, maintaining confidentiality, and protecting the integrity of both the legal service provider and the legal profession as a whole. A small selection of modern data security practices includes:

1. Physical security of data and computers
2. Modern Transport Layer Security (TLS) for websites and applications
3. End-to-end encryption for sensitive data
4. Never store sensitive information like passwords in plain text or easily reversible hashes; always use salted and hashed password algorithms with appropriate difficulty
5. Systematically verify code integrity
6. Patch and resolve bugs and other software issues in a timely manner
7. Use a firewall to scan network traffic.
8. Change default passwords and related vendor defaults.
9. Control browser features and security with HTTP security headers
10. Accurate asset inventory, scanning, and monitoring
11. Avoidance of untrusted 3rd party code and supply-chain vulnerabilities
12. Presence of an Intrusion Detection System (IDS) and Security Information and Event Management (SIEM) system, with appropriate internal procedures and 3rd party certifications (e.g. ISO 270001)
13. Regular testing of *all* relevant assets (networks, endpoints, applications, databases, middleware, etc)
14. Existence of a bug bounty program and engagement with ethical hackers
15. Information security policies and response plans
16. Strong access control measures and auditing
17. Adequate cyber incident insurance
18. Disaster recovery planning and regular disaster recovery exercises

However, this list is hardly comprehensive of the minimum data security features that a legal technology provider should provide to guarantee adequate data security. Because so many technological features, system architectures, and design patterns exist, all with varying security requirements, a panel of experts should regularly update and add to the standards, with consideration for not placing unnecessary barriers in the path of innovators. However, for some smaller use cases, or early-stage companies, some of these requirements may be unnecessarily onerous or not applicable and should be waivable by a panel of experts. For example, a seed-stage company serving 100 individual customers may not need a SIEM system and ISO 27001 certification, but a legal technology provider serving 10,000 customers likely should have such security infrastructure, policies, and external audits or certifications.