Shadow AI: A Thorny Problem for Law Firms

by Sharon D. Nelson, Esq., John W. Simek, and Michael C. Maschke

Remember Shadow IT? Say Hello to Shadow AI

There were plenty of articles written about Shadow IT – defined by Cisco as "The use of IT-related hardware or software by a department or individual without the knowledge of the IT or security group within the organization." – Shadow IT included cloud services, software and hardware.

Welcome to the sudden rise of Shadow AI. Its use, like that of Shadow IT, is often unknown to a law firm's IT or security group. As lawyers gravitated with haste to using generative AI in 2023, the conversation at law firms rapidly turned to controlling the use of Shadow AI.

Do you have any idea how many of your firm employees are using AI? The likely answer is no. We've all been so busy exploring what AI can do in our practices that only the largest of law firms are likely to have thought about AI policies, much less tracking the actual use of AI in their firms.

While law firms and companies don't like reporting on shadow IT problems, in 2023 Samsung issued a temporary ban forbidding any unauthorized AI applications after an internal data leak. We are sure similar edicts have been issued elsewhere, but that's the kind of subject that companies and law firms prefer to keep quiet.

Why is it so Hard to Track Shadow AI?

AI is everywhere, but it's not always visible. We forget that AI is embedded in videoconferencing programs, in many legal research programs, in our e-discovery software, in the browsers we use to search for information, in our smartphones – and the list goes on and on.

Sometimes it is more apparent that we are using AI – we understand that we are using it when working with ChatGPT, Harvey (which some major law firms use), Bard, Bing Chat, etc.

Has your law firm authorized you to utilize an AI? There's the rub. In general, employers are often unaware of what generative AI is being used by their employees. And the employees like their AI – you might send a survey asking employees if they use AI and they might well say no even if the correct answer is yes – they don't want to get in trouble, but they have no intention of giving their beloved AIs up. AIs have become addictive.

Do You Need an AI Usage Policy?

Absolutely. At least you need to document what is and is not allowed. You may choose to identify generative AIs which your lawyers and staff may utilize. However, you will certainly want to underscore certain things. Do they need to tell the client if they are using AI? Most ethicists

would say yes. Do they need to get permission for that use? If time is saved, is billing reduced? Do you ensure that no confidential data is given to the AI, either placed in its database or used for training?

In the end, your policy will constitute a set of guidelines and regulations which make sure that the law firm's use of AI is ethical and responsible. The policy should address any cybersecurity issues, data privacy laws, federal/state regulations, ethical considerations, etc.

Finally, it should be made clear that no unauthorized AI may be utilized. This may reduce the amount of Shadow AI at your firm, but never imagine that a mere policy will put an end to the use of shadow AI by rogue employees.

Another Tool to Combat Shadow AI: Employee Training

AI training is an industry these days – and the dangers of Shadow AI can certainly be addressed in a training session. We also suggest that Shadow AI be addressed in employee cybersecurity awareness training.

Many cyberinsurance companies require such training, so it is an additional "guardrail" to include a segment on the dangers of Shadow AI – indeed, on the cybersecurity dangers that may come with authorized AIs as well.

While most lawyers know they shouldn't give client information to an AI, they may not realize how dangerous it is to give information about the firm itself to an AI. As an example, don't construct a prompt along the lines of "How do you configure a TZ500 SonicWall firewall to allow FTP traffic?" Anyone who has access to that data (whether authorized or unauthorized) may use such information in a cyberattack. You'll certainly want to underscore that danger in the training.

How Can You Monitor the Use of Shadow AI?

That's the hardest question. There are solutions which provide full visibility into what applications are running and who is using them. Basically, you can scan for installed software and/or devices that are used to access your data and environment. What if you do not allow personal devices to access firm information? It's a simple matter to check the device "partnerships" in your Microsoft 365 account to see if any of the phones appear to be non-firm issued devices used to synchronize a user's mailbox.

There are also software monitoring tools to capture a user's activity even if a browser is used to access an AI environment. To be totally transparent, make sure you notify employees that you may be monitoring their activity. Some states even require that such notice be given to employees in a very prominent way.

Final Words

Embracing AI unreservedly is tempting. But go slow and be careful. Expect rogue behavior and have a plan to deal with it!

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com*

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm. jsimek@senseient.com*

Michael C. Maschke *is the CEO/Director of Cybersecurity and Digital Forensics of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional. mmaschke@senseient.com*