Unexpected Threats to Cybersecurity/Confidentiality: The SEC and ChatGPT

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

The Security and Exchange Commission Subpoenas Covington & Burling for Client Names

This story came out of left field. Since when does the Security and Exchange Commission (SEC) go to court asking a law firm to identify clients impacted by a data breach? The Covington & Burling cyberattack happened in 2020. Covington has said that the attack was aimed at a small group of lawyers and advisors to secure information about the incoming Biden administration's policies on China. The firm said it notified all clients whose information may have been compromised.

Nearly 300 publicly traded companies had their data accessed or stolen in the data breach. Covington was clearly not happy to receive a subpoena asking for the names of the clients impacted.

Has the SEC Lost its Mind?

We confess that was our first thought, but further research indicated that the SEC has a point. When the SEC sued Covington in January to compel identification of affected clients, it was part of an investigation into possible securities law violations associated with the breach. That is, after all, part of the mission of the SEC.

The SEC said that its subpoena was narrowly targeted and did not ask for information that was covered by attorney-client privilege. Why did it make the request? It said it was trying to determine if the breach resulted in insider trading and whether all required disclosures were made to investors about the breach.

Covington didn't see it that way. It accused the SEC of going on a "fishing expedition" and trying to compel the firm to turn over information that might cause its clients to be scrutinized without evidence of misconduct.

"The SEC's effort to compel Covington to help the agency investigate the firm's clients, without any evidence whatsoever of wrongdoing by Covington or those clients, is an assault on the sanctity and confidentiality of the attorney-client relationship," Covington told the Washington, D.C., federal court hearing the case.

Covington also warned that the SEC's action could chill cooperation between law firms and the government during future cyberattacks. It noted that there might be a "cascading series of dilemmas" for firms caught between reporting breaches and protecting their clients.

Law Firms Unite to Back Covington’s Arguments

The rally round the flag movement coalesced quickly. On February 21, some 83 law firms backed Covington’s opposition to releasing client names under the circumstances noted above by the SEC. They underscored the danger of weakening the principle of attorney-client privilege.

We think it is fair to say that we can expect a battle royale in U.S. District Court for the District of Columbia.

ChatGPT Warns Users of the Dangers of Giving it Sensitive/Confidential Data

ChatGPT is quick to warn users about the dangers of giving it sensitive data. A friend of ours asked this question of the AI: When can ChatGPT leak information it receives from its users?

We chuckled at the use of the word “leak” and, predictably, ChatGPT set our friend straight by answering at the outset “As an AI language model, I do not have the ability to leak information intentionally or unintentionally.” A bit of a scolding there we thought!

But it went on to note, “However, it is important to note that any information provided to me is stored in a database, and as with any database, there is always a risk of a security breach.”

Lawyers should read that sentence slowly a few times because we have already seen lawyers giving confidential data to ChatGTP in their research questions. It seems that many lawyers have not fully understood that everything they type into ChatGTP will likely live forever.

Maybe you need another sentence of caution from ChatGTP? Here you go: “It is also important for users to be cautious about the type of information they provide to me or any other AI language model, as there is always a possibility that the information could be inadvertently shared or compromised.”

ChatGTP is doing its level best to make sure attorneys abide by their ethical duties!

Can Cybercriminals Use ChatGPT to Write Malware? Sure

Threat intelligence company Check Point Research has recently noted that while Open AI, the creator of ChatGPT, has imposed restrictions on how ChatGPT can be used, posts on a dark web hacking forum revealed that it can still be used to create malware.

Anonymous users on the forum tell others, “the key to getting it to create what you want is by specifying what the program should do and what steps should be taken, consider it like writing pseudo-code for your comp[uter] sci[ence] class.”

Using this method, hackers can create a python file stealer that searches for common file types “that can automatically self-delete after files have been uploaded or an error is encountered while the program is running. The method is designed to remove any evidence of hacking.”

Well, that's a little scary to folks like us who manage cybersecurity for a living. If we can fool AI into helping us with malware or fixing buggy malware code, we have another obstacle to protecting law firm from cyberattacks.

Cybercriminals Bragging on the Profits from Using ChatGPT

Cybercriminals affirm that ChatGPT is a great way to "make money", claiming they make more than $1,000 per day. Many experts believe that they make their money by impersonating women and engaging in social engineering attacks on vulnerable targets. We won't explain further, but you probably get the idea.

Cybersecurity experts have affirmed to Cyber Security Hub that, according to their forecast, the top cyber security threat of 2023 will be crime-as-a-service. They also say that ChatGPT has expedited the process by creating malware for free.

Want some more troubling cybersecurity news?

A February survey from cybersecurity company BlackBerry shows that, of 1500 cybersecurity experts, 74% said they worried about ChatGPT aiding in cybercrime. 71% believed ChatGPT is likely already in use by nation-states attacking other counties through hacking and phishing.

Final words

After all we've read about misbehaving AI and AI hallucinations (and we have borne witness to some of them), it occurs to us that the final words for this column should go to Stephen Hawking: "Artificial intelligence will either be the best thing that's ever happened to us, or it will be the worst thing. If we're not careful, it very well may be the last thing."

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.*