3 KEY TAKEAWAYS

New York State Bar Association IP Section Annual Meeting: Cybersecurity/Data Privacy

During the New York State Bar Association IP Section Annual Meeting on January 17, 2024, Kilpatrick's Tony Glosson spearheaded the "Cybersecurity/Data Privacy" panel with fellow speaker Sharfy Salek of LexisNexis® Risk Solutions. The firm's Marc Lieberstein, Co-Chair of the Annual Meeting program, served as moderator for the panel. Kilpatrick's Ted Davis also presented his annual "Recent Developments in United States Trademark and Unfair Competition Law" program.

1

The emergence of AI has had significant cybersecurity implications. Like any other type of technology, AI-based solutions can serve as threat vectors because they are susceptible to vulnerabilities in their development and integration with existing systems, and these vulnerabilities can in turn provide a foothold for threat actors targeting an organizations systems and networks. However, there are also cybersecurity risks specific to AI, such as data poisoning attacks, in which a threat actor gains access to training datasets. Such attacks can present significant operational and reputational risks to organizations using the model at issue by producing manipulated and inaccurate outputs, leading to system failures, loss of user trust, or even infringement or defamation liabilities. Additionally, AI's capabilities have been co-opted by threat actors, who are able to use AI to enhance their ability to profile potential victims' behavior, tailor phishing scripts more effectively, and produce dynamic responses that further entice and deceive their targets. This sophistication in AI-driven attacks presents a new frontier in cybersecurity challenges.

2

In contrast to its role as a potential cybersecurity threat, AI also serves as a formidable ally to cybersecurity professionals, enhancing their ability to secure and defend systems and networks. One significant advantage of AI in cybersecurity is its capacity for real-time threat detection and response. For example, AI-driven systems can analyze vast amounts of network data at a speed and scale beyond human capability, quickly identifying and isolating anomalous behavior that may indicate a security breach. This rapid detection is crucial in mitigating the impact of cyber-attacks, as it allows for immediate response and remediation. Additionally, AI algorithms are being increasingly employed in predictive analytics, where they help in forecasting potential cyber threats based on existing data trends and patterns. An instance of this is the use of AI in intrusion detection systems (IDS). These systems, empowered by AI, can learn from past intrusions, continuously refine their detection algorithms, and thereby become more effective in recognizing and thwarting complex, previously unknown attacks. This evolving intelligence of AI in cybersecurity tools demonstrates a proactive defense mechanism, adapting to the ever-changing landscape of cyber threats. Through these applications, AI not only strengthens the defense mechanisms but also transforms the cybersecurity field, making it more agile, intelligent, and capable of facing the sophisticated threats of the digital era.

3

In addition to cybersecurity considerations, AI raises compliance challenges in ways that have remarkable parallels to traditional privacy and data protection compliance. In particular, the principles that have long been at the heart of privacy regulations often apply with equal force in the AI space, such as transparency, data minimization, and data subject rights. AI systems, by their nature, process vast amounts of data, so such principles are essential to maintaining user trust and regulatory compliance. And as has often been the case in data protection matters, the rapid pace at which AI is evolving requires a compliance strategy built around not only current regulations but also potential future legal landscapes. These challenges underscore the significance of industry participation in the regulatory advisory and rulemaking processes, both to understand where future regulations are likely headed and to help shape them in a way that reflects the risks and preserves the potential of emerging AI technologies.

For more information, please contact: Tony Glosson, tglosson@ktslaw.com.

www.ktslaw.com