New PBA Committee Focuses on Emerging Cybersecurity and Data Privacy Laws and Regulations

Cybersecurity and data privacy threats are daily critical business concerns in virtually every industry and with every client, large and small. With no overarching governing laws or standards, clients (and law firms, too) must navigate a patchwork of statutes, regulations and agency "guidance" reports — often industry-specific — to comply with data protection and data privacy requirements. Furthermore, with ever-evolving cybersecurity threats, lawyers must keep constant watch for new risks and legislation and to anticipate new legal expectations.

To that end, the PBA has created the Cybersecurity and Data Privacy Committee to help Pennsylvania lawyers be prepared to advise clients in cybersecurity and data privacy risks and requirements. It will also help lawyers prepare to address their own law firms' cybersecurity needs and requirements to adequately protect their clients' information.

Joshua A. Mooney, a partner at White and Williams LLP, Philadelphia, is chair of the new committee. The idea for the committee grew out of discussions with Charles Eppolito III, PBA president-elect and also a partner at White and Williams.

"We thought a committee focused on data protection and privacy will provide a valuable service to the PBA and its members," Mooney said. "It's a critical area, and the law is growing fast. Federal agencies and state governments are recognizing the importance of cybersecurity. For instance, in February, the U.S. Securities and Exchange Commission (SEC), when offering guidance on corporate disclosure of cyber risks, analogized the importance of data management to the importance of electricity in the last century. Commercial entities are placing cybersecurity requirements in their contracts. Cybersecurity and data privacy is having an impact on almost every facet of the legal profession: litigation, regulatory compliance, mergers and acquisitions, commercial contracting, corporate investigations and governance, and insurance," Mooney said.

The committee's charge is as follows: To analyze cybersecurity issues and educate PBA members about legal, regulatory and industry standards that preserve the con-fidentiality of protected information. The committee will advocate for best practices and legal and regulatory requirements that address data privacy concerns; for best practices to prevent, detect and mitigate data breaches, and for unified standards.

Mooney added that lawyers, whether in solo practice or part of a large firm, will have a need to know about data liability and privacy, whether for their clients or for their own firms. "Law firms are prime targets for cyberattacks, and lawyers face the same cyber risks as their clients. Many law firms are grappling with the same challenges that companies face when complying with data protection and privacy requirements, whether legal or contractual."

Some of the areas the committee will focus on are the challenges of complying with the patchwork of data protection and privacy laws, helping clients understand their scope and helping to better define what constitutes reasonable cybersecurity measures.

"One of the challenges in the field is that everyone talks about reasonable cybersecurity protections, but few are very clear on exactly what that means. We need to develop a better and more uniform understanding of that concept to help advise our clients, as well as courts and legislative and regulatory bodies. The committee is looking for attorneys who have an interest or focus on data protection or data privacy, whether it's in the context of insurance, regulatory compliance, corporate or litigation," Mooney said.

Data protection and privacy laws exist, but they are patchwork. "Forty-eight states have their own data breach laws. HIPAA and Graham-Leach-Bliley have significant reach, while the Federal Trade Commission and SEC maintain oversight authority. The E.U. General Data Protection Regulation goes into effect this May, and there is risk that many U.S. companies will be caught flat footed," Mooney said. Closer to home, last year the New York State Financial Services Department promulgated 23 NYCRR Part 500, requiring companies that are subject to the state's banking, financial services or insurance laws, to implement data security programs and policies based on cybersecurity assessments. "The regulation is the first of its kind," said Mooney. "It's having an impact in Pennsylvania, and we anticipate many states will copycat it." The National As-sociation of Insurance Commissioners, for instance, just authorized a model law for insurance that is based on the New York regulation. "Law and risks are changing, and that requires attorneys to keep their heads on a swivel," Mooney said.

Mooney said he didn't learn cybersecurity and data privacy law in law school. "I always think of the assistant dean who told our class 'the law you will be practicing at the midpoint of your career hasn't even been thought of yet.' That's so prescient."

Under the heading "You Never Know Where This Will Lead," one of Mooney's earliest privacy cases was representing a school district accused of spying on its students using webcams in student laptops. "That case started me on the path to where I am now," he said.

Mooney is co-chair of White and Williams' Cyber Law and Data Protection Group. As such, he advises corporate clients on matters involving compliance with data protection and privacy requirements and regulations, and assists with corporate investigations and responses to cybersecurity incidents, including data breaches and notification requirements. He also helps companies conduct cyber risk assessments and implement cybersecurity programs and policies. In addition, Mooney advises insurance carriers on complex and emerg-ing coverage risks involving cyber and privacy rights, e-surveillance and media.

Joshua A. Mooney

Mooney writes and lectures regularly on cyber liability, privacy and coverage, teaching CLEs and providing in-house seminars and training. He is also a member of an X9 working group charged to draft a national standard for data protection and data breach response for the financial services industry. He will use his professional experience to help guide the PBA committee.

"Areas that the committee tackles first will depend somewhat on the constituency of the membership. I want to get an idea of what the members want to do as we set an agenda," Mooney said.

PENNSYLVANIA BAR ASSOCIATION

Your Other Partner

Reprinted from the March 19, 2018, issue of *Pennsylvania Bar News.*