

# The Legal Landscape of Privacy: Why Lawyers Must Keep Up with Change

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

We are nearing the end of another year filled with significant advancements in cybersecurity protections adopted by law firms to combat the constant cyber-attacks they face. Law firms are finally embracing Endpoint Detection and Response (EDR) software, cybersecurity awareness training, and phishing simulations. The reality is that the measurement of cybersecurity protections can never be genuinely quantified. The primary reason is because the goalpost everyone aims for keeps moving farther and farther away with each new vulnerability or attack method discovered or developed by attackers. The continually evolving and complex world of cybersecurity shows no signs of slowing down.

## **More Governance.**

What else must law firms endure besides constant cyber and phishing attacks? How about further governance regarding data privacy? Law firms got a taste of this in 2016 with the EU's passing of the General Data Protection Regulation (GDPR), touted as the world's strictest privacy and security law. The GDPR imposes obligations on any organization that targets or collects data related to people in the EU.

The California Consumer Privacy Act (CCPA) went into effect in January 2020, providing residents of California with greater control over personal data collected, including the ability to request a business to delete any harvested personal information. This legislation applies to anyone who does business in California that meets certain thresholds. That's just California's privacy law. There are now 20 states that have varying degrees of data privacy laws.

As a result of governance, law firms have adopted privacy and data collection policies to meet these requirements, including GDPR policies and popup notifications regarding Cookies and the types of data collected when visitors browse their websites. Failure to abide by and comply with these changing regulations may result in malpractice claims, lawsuits, or fines for non-compliance. That certainly has gotten the attention of many law firms. Suddenly, law firms are taking the long-standing regulations seriously, which have largely been ignored in the past.

## **Driven by Client Demand**

It's not just the cyber insurance carriers; clients have also gotten smarter about data protection. Law firms commonly receive cybersecurity questionnaires from larger corporations or defense contractors, which must be completed before engaging with the law firm. Clients demand to know what protections are in place to keep their data safe and, in some instances, want proof—not just self-attestation. These questions are very similar to those asked by cyber insurance providers.

Some of the cybersecurity measures asked about by clients include:

- Are 100% of endpoints protected by “next-gen antivirus” and “EDR” software?

- Have you had a penetration test and vulnerability assessment performed within the last year, and if so, were all the medium, high, and critical vulnerabilities remediated?
- Are your information systems monitored by a Security Information and Event Management (SIEM) solution backed by a 24/7 Security Operations Center?
- Are your critical systems backed up to an offsite location protected against ransomware attacks or infections (immutable backups)?
- Have your employees attended a cybersecurity awareness training session within the last 12 months?
- Is MFA required for access to all firm resources?

These are some very tough questions from clients, but they underscore the importance of data protection and privacy from the client point of view. Law firms that haven't implemented the requested measures often use the request as a catalyst for positive change to implement the solutions before responding to the questionnaire and are willing to take on the cost to get the client. It's a win-win.

### **Risks of Litigation**

It was only a matter of time before the data breach attorneys showed up to the party. Class action lawsuits have now become a nightmare for law firms who have suffered a data breach. Law firms are becoming subjects of class action lawsuits, which often tend to settle relatively quickly without the details being outlined in court. Class action lawsuits, expensive data breach notification requirements, and monetary fines from State Attorney Generals for data privacy violations- what more can be done to drive the point home about the need for rigorous data security protections? For a long period of time, law firms hesitated to take on class action lawsuits against other law firms which suffered data breaches. Those days are long gone.

Mandated privacy and data protection are here to stay, as are cyberattacks. Law firms must remain proactive in adopting these measures which benefit the firm and its clients. Serious reviews of your cybersecurity and annual security changes mitigate risk and exposure and will keep class action lawsuits at bay. As an added benefit, you may even get your cyber insurance carrier to lower your premium (or not increase it as much as they usually do) with all the added security measures you've implemented.

**Michael C. Maschke** is the President and Chief Executive Officer of Sensei Enterprises, Inc. Mr. Maschke is an EnCase Certified Examiner (EnCE), a Certified Computer Examiner (CCE #744), an AccessData Certified Examiner (ACE), a Certified Ethical Hacker (CEH), and a Certified Information Systems Security Professional (CISSP). He is a frequent speaker on IT, cybersecurity, and digital forensics, and he has co-authored 14 books published by the American Bar Association. He can be reached at [mmaschke@senseient.com](mailto:mmaschke@senseient.com).

**Sharon D. Nelson** is the co-founder of and consultant to 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](mailto:snelson@senseient.com)

**John W. Simek** is the co-founder of and consultant to Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), a Certified Ethical Hacker (CEH), and a nationally known digital forensics expert. He is a co-author of 18 books published by the ABA. [jsimek@senseient.com](mailto:jsimek@senseient.com)