Building Blocks

First Steps in Starting Your Data Privacy Law Practice

By Jessica C. Engler

Making an investment and effort in a few key areas can set new-to-the-practice attorneys on the right path to success.

Once a series of one-off issues addressed as needed by other practice groups, data privacy and security matters have become both large enough and frequent enough to dominate an attorney's or legal team's practice.

Cybersecurity and data privacy consistently ranks as one of today's top legal practices, and the trend shows very little sign of slowing down. *See, e.g.*, Aebra Coe, *The 3 Hottest Practice Areas for 2019*, Law360 (Jan. 1, 2019), https://www.law360.com. In February 2018, the American Bar Association (ABA) approved a resolution allowing attorneys who meet certain criteria to advertise themselves as "Privacy Law Specialists" through accreditation by the International Association of Privacy Professionals (IAPP). Angelique Carson, *IAPP's Privacy Law Specialist Certification Becomes Official*, The Privacy Advisor, Int'l Ass'n Privacy Prof'ls (Feb. 6, 2018), https://iapp.org. New legislation such as the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and a myriad of privacy-focused state and federal legislation have kept privacy attorneys incredibly busy, making it no small wonder that more law firms have started building up their privacy teams.

Individual attorneys are also investing their time and resources into building privacy practices. In particular, the emergence of data privacy law has presented a unique opportunity for young lawyers to ascend the ranks quickly. Unlike long-time practice areas with decades of precedent and deep practitioner benches, the data privacy field is still new, and young lawyers can quickly become as experienced as their more seasoned colleagues. With that said, there are no age barriers to this practice area for attorneys looking to make a change or expand their practices. For those leaving private practice, data security knowledge is also an asset for an in-house move. *See* Sam Reisman, *In-House Attorneys Must Become*

■ Jessica C. Engler, CIPP/US, is a registered patent attorney in the New Orleans office of Kean Miller LLP. Her practice includes data privacy, intellectual property, and construction litigation. In her data privacy practice, she regularly advises clients on breach mitigation and response, third-party risk management, and Federal Trade Commission regulation. She currently serves as the DRI Cybersecurity and Data Privacy Committee Young Lawyer Liaison and is a member of the Louisiana Association of Defense Counsel.

Data Privacy Pros, Experts Say, Law360 (Apr. 24, 2018), https://www.law360.com.

Having an interest in the field is one thing. Getting started, however, can feel overwhelming. But learning data security law and keeping pace with its changes is not insurmountable. Making an investment and effort in a few key areas can set new-to-the-practice attorneys on the right path to success.

Be Prepared to Commit and Invest in the Practice

Becoming competent in data privacy law takes work and study—a lot of it. Data privacy law is rapidly changing; new laws are continually passed, and first-impression opinions are frequently issued on data privacy topics. Keeping up with new legislation and case law, and analyzing both, takes a significant amount of time. Attorneys committed to entering the data privacy practice should be prepared to invest time and resources to attending seminars and continuing legal education presentations, reading cases, and staying abreast of these changes. Privacy attorneys should have some method—through daily listserv emails or otherwise—of promptly being alerted to new key court decisions and legislation.

A good place to start this data privacy education is with state data management and breach notification laws. All fifty states, as well as U.S. territories, have their own data breach notification statutes. Becoming familiar with them is essential to data privacy practice. The various state privacy laws have been aggregated by the National Conference of State Legislatures. *Data Security Laws, Private Sector*, Nat'l Conf. of State Legisls. (May 29, 2019), http://www.ncsl.org. These statutes govern non-regulated, private companies doing business in the particular states. Often, the first matter that a new data privacy attorney handles is a state law-governed data breach. Having a good handle on these laws, the liabilities imposed, and the deadlines for response can help you quickly and correctly respond when a breach arises.

Beyond that, there are many state, federal, and international laws and regulations about which you can continue to learn. Ultimately, most data privacy attorneys focus their time on the laws that most affect their clients. If you have a number of clients that trade publicly, having a good handle on the U.S. Securities and Exchange Commission's breach-disclosure requirements would be important. For clients with offices in the European Economic Area, familiarity with the GDPR is mandatory. Depending on the extent to which a client has contacts with California residents, the CCPA may become an issue when it becomes effective on January 1, 2020. Understanding the scope of a client's business will provide direction on where to focus your education efforts.

DRI, the ABA, and the IAPP all provide resources and blueprints that can help guide your education. *Cybersecurity Resources*, Am. Bar Ass'n, https://www.americanbar.org. Depending on your personal or firm resources, there are also additional materials available through paid providers such as Westlaw's Data Privacy Advisor. Blog posts by attorneys are also an excellent resource. There is a wealth of information and opportunity available, but it will take time to work through it. Once you have a solid grasp on the laws that your client base is subject to, you can start developing your experience and expertise.

Learn How to "Talk Tech"

To communicate with clients effectively, data privacy attorneys need to be familiar with the technology commonly involved and have a general appreciation of how it works. Not being "tech-savvy" is a disqualifier in data privacy practice.

The specific terminology and background information that you need to know will largely depend on your clients, the laws they are subject to, and the technology that they use. Reviewing the current jurisprudence and references from regulators such as the Federal Trade Commission will provide solid background information. *Data Security*, Fed. Trade Comm'n, https://www.ftc.gov. For hacking, identify theft, and criminal concerns, the Federal Bureau of Investigation and Internal Revenue Service also offer resources. Organizations such as the IAPP also offer glossaries in their resources centers; look up the terminology when you encounter a term you have not seen before. *Glossary*, IAPP (last accessed July 29, 2019), https://iapp.org/resources/glossary/. Depending on the size of your firm, your IT department may also have personnel who can answer questions or explain challenging concepts. Ultimately, when you are talking with clients and their representatives, speaking the same language is essential.

Consider Getting Certified

Some, but not all, data privacy attorneys have earned their Certified Information Privacy Professional (CIPP) accreditation through the IAPP. (The IAPP also offers two additional certifications: the Certified Information Privacy Manager and the Certified Information Privacy Technologist.) The IAPP currently offers four variations of the CIPP certification: (1) U.S. private sector; (2) Canada; (3) Europe; and (4) Asia. Practitioners who earn the CIPP designation hold at least a foundational understanding of privacy and data protection law and practice, including, but not limited to, jurisdictional laws, regulatory issues, privacy concepts and principles, and legal implications for data management. *CIPP Certification*, IAPP.org, https://iapp.org/certify/cipp/. Certification holders are required to complete twenty hours of continuing privacy education every two years to maintain the certification.

Not being "tech-savvy" is a disqualifier in data privacy practice.

Since CIPP certification is frequently listed as a requirement for in-house compliance positions, many attorneys wonder if the certification is a de facto requirement for the privacy practice as a whole. The short answer is that there is no requirement, but it can be very helpful for marketing purposes. Data privacy liabilities can be significant, so clients will want to be confident that they are working with a knowledgeable attorney, rather than someone who merely dabbles. Having an IAPP certification such as the CIPP can communicate to clients that you are dedicated to the data privacy practice and are knowledgeable about the field.

Data Privacy, continued on page 54

Data Privacy, from page 31

Nevertheless, the certification will only get you so far. Much like passing the bar exam establishes minimal competency in a jurisdiction's law, completing the CIPP certification similarly establishes only foundational privacy law knowledge. Study beyond the material tested and keeping abreast of changes in the law is required to succeed in this practice area.

Make Connections with Fellow Privacy Practitioners

Because data privacy is still a niche practice, the privacy law community is relatively small. For attorneys not based in data privacy-heavy locations such New York City, Chicago, or Silicon Valley, making connections can be more difficult. However, there are opportunities out there to connect with other privacy practitioners by attending seminars and participating in local communities.

Attending seminars can be crucial for making connections with private practitioners, in-house counsel, and other "privacy-minded" individuals. Look for opportunities to attend both privacy-focused seminars and general practice seminars that offer cyber "breakout" sessions. For 2020, the DRI Cybersecurity and Data Privacy Committee is currently slated to present mini-sessions at the DRI Women in the Law Seminar, the DRI Business Litigation Super Conference, and the DRI Insurance Coverage and Practice Symposium, which can give interested attorneys an opportunity to learn more about the privacy sphere and network with fellow data privacy colleagues. Local, state, and regional bar organizations often have "Law and Technology" committees that offer opportunities to network. Because data privacy law changes so rapidly, the practice community is a highly collaborative and open group that is welcoming to newcomers.

Check Your Own Backyard

On October 17, 2018, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 483, which identified an attorney's ethical obligations in the event of a data breach. As noted in the opinion, data breaches and cyber threats targeting lawyers and law firms happen on a daily basis, and lawyers are just as likely to be targeted as the clients themselves.

Given this reality, lawyers who practice in data privacy should take care to "practice what they preach." If you are unsure of your firm's security standards and when those standards were last reviewed and updated, those questions should be asked before holding yourself out as a data privacy attorney. If your firm has not yet purchased a cyber insurance policy, now would be a good time to explore that option. Data breaches can have devastating effects on businesses, and law firms are no exception. Experiencing a data breach as a data privacy attorney can severely harm a burgeoning practice and reputation, so making best efforts to avoid or mitigate the risks is advisable.

Conclusion

Breaking into data privacy is not impossible, but it does require dedication, research, and flexibility. Data privacy is a fast-paced, exciting practice area. It keeps you on your toes, but it is also fascinating and extremely rewarding. This time investment may require significant effort outside of normal business hours and a deferral of short-term benefits, but the energy and effort are worth it in the long run. With these tips, interested attorneys can hopefully start laying the foundation for a successful data privacy law career. FD