

## Pennsylvania eDiscovery

By Philip N. Yannella

*Pennsylvania eDiscovery* is a seminal volume on the subject of how litigators can effectively manage electronically stored information (ESI). It is intended as a guide to help legal practitioners navigate new eDiscovery rules adopted by the Pennsylvania Supreme Court as well as the extensive federal case law that has been published on this topic.

Topics covered in the book include the duty to preserve electronic evidence, issues in electronic document production, proportionality, cost-shifting, social media, non-party discovery, eDiscovery in criminal cases, and discovery of foreign documents.

### Key Questions and Answers

#### *What electronic information is discoverable?*

Generally speaking, relevant non-privileged electronically stored information is subject to discovery. Given that 98 percent of documents are electronic and stored in some form, the amount of ESI that is potentially discoverable in an average case can be very large. Typical discovery requests focus will seek e-mail and the “Microsoft Office Suite” of documents—Word documents, Excel spreadsheets, PowerPoint presentations. But many other electronic documents are also potentially subject to discovery, including PDFs, Microsoft Access files, TIFs, JPEGs, GIFs, text messages, instant messages, data stored in social media sites, wikis, digital voicemails, and proprietary databases. Lawyers should assume that in most cases electronic data, regardless of form, will be potentially discoverable.

#### *How do I counsel clients to preserve electronic content to avoid sanctions for spoliation?*

Every case and every client is different, but there are a few golden rules. To begin, once a duty to preserve has been triggered—by, for example, being served with a complaint or subpoena—the client should promptly issue a written legal hold to all employees who are reasonably likely to have responsive documents. Clients also need to coordinate with IT personnel who may have root access to systems in which documents are automatically deleted after a certain period of time. If the client has configured systems in this manner, it’s important that IT disable any automatic deletion functions or develop a technical workaround to ensure that relevant documents aren’t deleted while the litigation is ongoing. These days, many companies are using cloud-based solutions, and their employees may have responsive documents in personal e-mail accounts. Counsel needs to ask clients where their data is being held and review any applicable third-party contracts to ensure that relevant data held in the cloud is being preserved.



*How can eDiscovery be less costly and time-consuming?*

Policies, process, and personnel. Having records retention policies that strictly govern when documents can be destroyed is an important step in reducing data volume, which is the single greatest driver of eDiscovery costs. Once discovery ensues, it is important that the company implement a routinized process for collecting, processing, and reviewing documents. Lastly, using personnel who are familiar with the company's systems and process, as well as lawyers who are experienced in best practices for managing eDiscovery and litigating related issues, is key to reducing costs.

*How do I manage the complexities of an eDiscovery request?*

Due diligence is paramount. Requests that may appear easy to satisfy at first can become extremely burdensome if it turns out that the data is held in archival systems, or is located in servers in other countries, or is replete with customer financial information—to name a few thorny problems. Oftentimes lawyers don't ask the right questions early enough in litigation to get ahead of these kinds of potential problems. (And they are surprised when their emergency motions for protective orders are denied.) Conducting a thorough ESI investigation, early in the case, is critical to anticipating the scope and potential burden of a discovery request and positioning a discovery issue for favorable resolution.