Professional Perspective

E-Discovery Issues During the Covid-19 Pandemic

Timothy Shields, Kelley Kronenberg

Bloomberg Law

E-Discovery Issues During the Covid-19 Pandemic

Contributed by Timothy Shields, Kelley Kronenberg

Amid the Covid-19 pandemic, we were forced to adapt to the "new normal" that included working from home, being on lockdown, and observing social distancing. These restrictions often disturbed our everyday living and increased the challenges we faced at work or home. While that would be enough stress in normal times, managing litigation during the pandemic created a new set of challenges for attorneys and IT professionals.

In this digital age, electronic discovery (e-discovery) plays a vital role in legal operations and litigation. E-discovery refers to the process by which relevant data are preserved, reviewed, and exchanged in electronic forms to be used in investigations, regulations, and other legal matters. During the pandemic, e-discovery questions ranged from "where is the data?" to "how can we retrieve it?" Below are some of the new realities legal professionals had to navigate during the pandemic.

Determining the Location of Data

Even in normal times, locating information subject to an e-discovery request is difficult because of the widespread use of technology including cloud-based software, online folders, and instant messages, as well as a variety of devices including laptops, tablets, and the ubiquitous mobile phone. The physical location of electronically stored information (ESI) has become quite challenging to trace.

In the early days of the pandemic, businesses had to rapidly shift from controlled and orderly office technology environments to personal and home devices. Employees were suddenly taking business calls and sending text messages from their personal cell phones and using home computers, printers, flash drives, and the like.

If a discovery request asked for phone logs, were employee personal phone records now part of that discovery request? What about personal text messages or voicemails? Many employees had to use personal computers at home. Are those devices now subject to review in a discovery request?

With the work-from-home setup, employees could also be transmitting and storing documents in various locations. There have been many instances of employees emailing documents from their secure work environment to their personal email addresses to print on their home printers. Does this then bring in their personal email address as a source of discovery? In a data dump, opposing counsel could see emails going from @work.com to @home.com and begin to question what other data might reside in the personal account. How willing will the employee be to grant access to their personal email?

The rapid deployment of remote work technologies also created some e-discovery challenges. The installation of instant messaging creates new chat logs that may need to be reviewed. In addition, video conferencing also creates meeting logs and potentially meeting recordings. These recordings can be stored both locally on the host's personal computer and in a cloud service. Locating and sharing these logs and recordings are a new burden in the discovery process.

Further, many employees may have relocated during the pandemic to seek shelter close to family and friends. Consequently, it is difficult to determine which state law applies to e-discovery and which guidelines to follow in executing these requests. The "new normal" setup has added to the burden of preserving and collecting data during this period.

Challenges in Privacy and Vulnerability to Accidental Loss

Data security is a primary concern, especially in litigation. With data spread far and wide and across diverse hardware, the risk for accidental removal is high.

As the pandemic response rapidly swept workers out of their offices and into their homes across the country, well designed and implemented data loss prevention strategies were suddenly moot. As workers struggled to piece together home offices that were also being shared with children doing online school, work was being done on a mixture of business and personal devices. These personal devices were not part of the organization's data scheme and as a result, automated systems to preserve data would have been suddenly ineffective. For example, home printers are often not accessible through company-issued equipment. As mentioned prior, users circumvented security protocols by forwarding work to their personal accounts so they could print locally.

In the office setting, that client document, business strategy plan, or budget forecast would be secured in a shred box when no longer needed. Many companies have "clean desk" or "paperless" policies to reduce waste and prevent potential data loss. Now that work document may be on the family desk, under a student's math homework, or in a recycle bucket with no ability for the company to control access, ensure destruction, or preserve for litigation if needed.

While many organizations used remote connections to company assets such as remote desktop sessions, the company has no visibility into the network connection when users were connecting from home networks. Connections to company resources could have been occurring over compromised or hacked connections exposing the company network to a cyber-attack because the user's connection credentials could be captured. Any significant breach during pre-litigation discovery that resulted in a ransomware or data loss could create a significant liability for the company.

The same challenges that faced corporate representatives and legal staff across the litigation spectrum also impacted litigation support teams, such as e-discovery review teams. When the pandemic intensified and document reviewers were sent home to work remotely, the need to ensure client confidentiality took on a new level of importance. It was hard (if not impossible) to ensure data privacy in the respective homes of hundreds of remote reviewers, prompting the need for greater use of external servers, facial recognition software and other biometric security tools. Project managers had to issue stern warnings for remote e-discovery document reviewers not to discuss the case at home within earshot of family members or voice-activated artificial intelligence virtual assistant software programs. Using shared office space with students taking online classes from either K-12 or post-secondary school literally brought the outside world into your office with audio and video streaming. The potential for data breaches or the inadvertent leak of privileged information was very critical.

Physical Access and Costs

Even though e-discovery deals with electronic records, IT staff often need to have physical access to the computer or server to retrieve data and make copies. In some instances during the pandemic, this became almost impossible.

If a large amount of data was needed from a user's computer and that user was in a personal environment with low network speed or bandwidth, the files could not be copied remotely. In this instance, the computer might have to be accessed directly to copy files or run forensic tools to access data. If the data was on a mobile phone or tablet, direct access would also be needed. In situations where the employee relocated, the office was closed, or other high-risk factors existed, retrieving the device could take days or weeks. This is a challenge when meeting discovery deadlines.

Along the same lines, data centers themselves were locked down and many limited the number and time one could visit. During the height of the pandemic, some data centers were completely closed to visitors unless there was an emergent equipment failure. As they began to open, technicians had to schedule appointments, and only a limited number of people were allowed into the data center at once.

Of course, across the U.S., each state varied in the length and severity of local restrictions on movement. In some instances, physical access to equipment was simply not possible until local conditions improved.

Likewise, court proceedings, such as a motion to compel, were altered as courts operated in limited capacities and when they did operate, it was remote. This made discovery dispute resolution more challenging and delayed the overall discovery process.

Applicability of International Laws

Every country has its own emergency laws and regulations in response to the global pandemic. The issues with access, bandwidth, and personal movement were magnified if you had any data outside of the U.S. For instance, if a team had developers in Ireland, or a server farm in Eastern Europe, one would be hard-pressed to gather that data from March to June of 2020. In some areas, the restrictions lasted much longer. One had to understand laws in the relevant countries involved and, when suitable, take measures to contact the appropriate authorities first before commencing any activity. The complexity in the variations of international laws posed more significant challenges than normal during the pandemic discovery era.

Conclusion

The pandemic has laid bare the already complicated world of e-discovery. Some of its unique challenges include increased use of personal devices, and new technologies and sources of discoverable information. The Covid-19 era has broken down otherwise robust data retention and protection policies, and made the collection of data more difficult through geographical and physical restrictions.

The challenges of remote work staff at all levels of organizations made the physical control and supervision of staff extremely challenging. This forced organizations into more secure technologies they might not have otherwise used, such as external servers and biometric security.

As we look to learn from this experience, attorneys and technology professionals will need to educate workers on the proper use of personal devices, redesign data retention policies to prevent the transfer of business data to personal accounts, and adapt to the widespread use of messaging and video tools.