Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

10 E-Discovery Challenges Caused By COVID-19

By **David Kessler and Andrea D'Ambra** (March 25, 2020, 4:36 PM EDT)

David Kessler

During the current crisis, there are many more important things to be worried about than e-discovery, most importantly the health and safety of our family, friends, co-workers, colleagues and clients. That being said, like its widespread impact, the COVID-19 crisis also affects how e-discovery is currently being undertaken and will impact discovery long after we overcome this pandemic.

Here are some of the challenges facing producing parties as they conduct discovery during the COVID-19 pandemic.

1. "Work from home" will likely create new data sources for preservation and collection.

Andrea D'Ambra

Depending on the party and how the organization has operationalized working from home, parties should consider whether employees may be transmitting and storing documents in new locations. Are employees storing documents locally (either on work laptops or personal devices) because they are having a hard time connecting to the company system of record?

With many employees working from home and wanting (needing) to communicate with others, they may use nonstandard or nonenterprise communication tools to discuss business (e.g. text messages, Facebook Messenger, WeChat, etc.). Going forward, this may add to the preservation and collection burden parties must bear when responding to discovery requests for information created during this time period.

2. Because of lockdowns and social distancing, forensic collections, except those that can be done remotely, will not be possible.

With some cities, and even entire states like California, being on lock down, and most other locations requiring all but essential businesses to close or work remotely, it may be difficult or even impossible to have in-house or third-party forensic vendors collect many types of potentially relevant documents that require physical access to the device (such as with most mobile device data). Thus, parties may need to find vendors or tools that allow them to do remote forensic collections and defer collection of devices where remote collections are not possible.

Remote collections usually require cooperation and some involvement by the custodian, which may pose other unique challenges. Beyond digital collection, we must not forget that locating and scanning paper documents is even more of a challenge because it requires personnel to be with the documents at each step in the process. Thus, paper files and other documents that require in-person collection will need to be deferred until the crisis abates and travel restrictions are lifted.

3. Collection and data transfer operations may be interrupted.

Even for organizations that have handled data collections and transfers to processing and hosting vendors internally, the work-from-home model may pose a serious problem. This is because many organizations configure their IT systems in a way that prohibits or limits remote data collection and transfer without certain authorizations. This configuration may block collection of data in response to discovery requests and its subsequent transfer to hosting and reviewing vendors.

Moreover, transfers of encrypted media in physical form may be delayed as express delivery services are scaled back because of other priorities or reduced staffing. This may significantly delay the production of electronic documents that could typically be collected remotely (when operating within the company's IT infrastructure).

4. Hosting vendors may be delayed in ingesting, processing and producing data.

While small data volumes may be transferred over the internet using FTP sites, larger data volumes must be sent via encrypted media such as a thumb drive or external hard drive. Those physical drives require personnel to be onsite at the vendor's facility to open, log, load and process the data contained therein. Depending on where the party's vendor is located, they may be shut down or working with only a skeleton crew.

Thus, parties should anticipate delays in getting their data uploaded and published for review. Likewise, productions may require personnel to be onsite to burn media for large productions.

5. There are significant data security considerations that must be addressed around permitting reviewers to access a party's data remotely.

Many of the managed review vendors have prided themselves on their on-site data security and physical security protocols designed to prevent external attacks and rogue document reviewers. In response to governmental remote working and shelter-in-place orders, many vendors had to quickly transition from on-site review to remote review to address discovery deadlines. Many vendors have touted their ability to have their reviewers work from home with some claiming that it is just as secure.

As an initial matter, it is simply not accurate to say that remote review is as secure as review done in a vendor's dedicated facility with all the physical and data security protections and on-the-ground oversight and management that physical locations offer. For instance, when a reviewer is working from home, other family members may be able to walk by and see confidential information displayed on the reviewer's computer.

The reviewer might also have malware or viruses sitting undetected on their operating systems. Moreover, the reviewers are using untested (and possible unsecure) home internet systems, thus absent a VPN tunnel or Citrix-type portal, there is significant risk that bad actors may be able to intercept the

data.

Most parties have contractual provisions within their managed review vendor contracts mandating on-site review and, depending on the sensitivity of the data being reviewed, may have reasonable concerns about permitting remote review to proceed. Even if a party is willing to waive that on-site review right, it must ensure that the contracts have appropriate confidentiality and data security measures in place to mitigate the above articulated risks.

The time spent vetting and testing these remote review technology solutions and workflow arrangements may delay the kickoff of remote review and push back ultimate completion of the review.

6. Universal working-from-home arrangements may stress the capacity of remote access portals to review systems.

As many of us learned during the first week when social distancing and working from home were implemented for many Americans, remote access systems that were originally intended to provide a limited number of reviewers at any given time may not have been designed to handle the types of bandwidth requirements necessary for the entire review vendor's teams to work remotely.

These bandwidth issues can lead to slower performance and lost productivity, and in some cases, denial of access if there are too many users attempting to log in at once.

7. Performance of individual reviewer's personal computers and internet will be significantly diminished from that of the review vendor's normal operations site.

Beyond simply the bandwidth of the remote access portal, there are also challenges with the respective capabilities of an individual reviewer's personal computer hardware and internet bandwidth. Speed is essential in document review, which is why review sites have uniform computer systems with minimal software installed so they are optimized for document review. A reviewer's personal computer, on the other hand, may be several years old with many programs running in the background that slow performance.

Vendor review sites also have robust internet connections that can handle hundreds of reviewers simultaneously connecting to a variety of internet-based document review hosting platforms, while an individual's home internet bandwidth at best is intended for downloading videos, gaming and internet surfing.

The Citrix-portal-type connections necessary to address some of the data security considerations listed below further impede data speeds, which in turn slows review rates and, in per-hour billing models, raises costs. All this means that production deadlines may need to be moved and budgets adjusted.

8. Decentralized remote working will pose additional challenges.

Managed review and e-discovery vendors have successfully solved the communication challenges of hosting data in one location and reviewing it in another where neither location is where the client or the lawyers are located. However, it will also be harder to communicate changes in protocol, provide reviewer feedback, and just get a sense of the review progress that often comes from "walking the floor."

Moreover, inspiring reviewers to meet deadlines will be more challenging, and the friendly competition that often drives reviewers to work longer will not be possible since a reviewer can log off without being seen by their peers. That said, it may be that some reviewers will work longer hours when they can do so from the comfort of their own homes and they do not lose time to commuting.

It's hard to gauge how this factor will impact review timing, but based on our experience with distributed versus centralized reviews, it is likely to add delays that parties will need to address.

9. Remote working creates new cyber vulnerabilities.

While this is true across the enterprise, it is particularly acute here. As discussed before, in many cases, vendors had to stand these systems up very quickly and they may not all have been properly configured. Moreover, hackers are well aware both of the vulnerabilities remote working configurations have and that discovery vendors and reviewers have access to some of their clients' most valuable and important data. This makes such vendors (as well as law firms) an attractive target for hackers looking to make a quick score.

Parties will need to take the time to work closely with their law firms, hosting vendors and managed review providers to make sure they have implemented the necessary protections to make remote working reasonably secure. For example, individual lawyer, reviewer or consultant home computer security may not be reasonable secure because it either uses weak or limited passwords or because a home computer is infected or not properly patched.

Also, just as a client's employee may be storing documents locally to make it easier to work, so too lawyers and consultants may be leaving the information more broadly distributed and, thus, more vulnerable. Finally, to the extent that discovery vendors, including law firms, have not instituted proper remote working protocols and security (e.g. multifactor authentication), it leaves them even more vulnerable in this era of intense cyberattacks. Putting in place these additional safeguards may take time, but is time well-spent.

10. All of these problems will be worse outside the U.S.

Parties should expect that each and every one of these issues will be exacerbated if a party needs documents from outside the U.S., where they are likely even less prepared (and, in all honesty, discovery is even less of a priority). As discovery is far less common and more unfamiliar outside the U.S., it is less likely that the data systems and discovery vendors will have the ability to preserve, collect, process, review and produce data remotely. Discovery architects should account for these delays and points of failure.

Conclusion

Discovery is a means to an end — the peaceful resolution of disputes — and, as such, it should never be the tail that wags the dog. Now, in this time of true crisis, its relative importance is clearly secondary. From that perspective, many of us have more important things to focus on in the near term, but when litigation and investigations reengage and courts start moving their schedules forward, these issues and concerns will need to be addressed.

With a better understanding of the challenges underlying discovery in the time of COVID-19, hopefully, opposing parties will be able to come together to reach reasonable compromises regarding what is

doable and when it can be done, all while maintaining the security and confidentiality of the parties' business information.

David Kessler is the U.S. head of data and information risk at Norton Rose Fulbright.

Andrea L. D'Ambra is a partner and the U.S. head of e-discovery and information governance at the firm.