Professional Perspective

Technological Solutions for E-Discovery Professionals

Contributed by Nicole Marie Gill and Emily Plowcha, Cozen O'Connor

Bloomberg Law

Technological Solutions for E-Discovery Professionals

Contributed by Nicole Marie Gill and Emily Plowcha, Cozen O'Connor

The Covid-19 pandemic upended businesses everywhere, and as a result, many employees shifted to working from home. Although vaccines provide hope that companies can reopen offices across the nation, many employees are still working remotely. The pandemic ushered in a new normal that may be here to stay—the remote work environment.

The transition from the traditional office environment to working from home brings an increased reliance on new and existing technologies to conduct business. This remote work environment has significantly impacted e-discovery, created new obstacles in an ever-evolving technological and legal landscape, and is now demanding practical solutions to address these challenges.

Communication & Collaboration Best Practices

Communication and collaboration technologies are essential substitutes for in-person conversations and business meetings. Necessitated by remote working environments, technologically-driven business communication is the rule, not the exception. This increased reliance on various technologies, from email to collaboration tools, has also increased the burden on e-discovery attorneys to ensure that any electronically stored information (ESI) associated with these platforms is properly identified, preserved, collected, and produced in accordance with legal obligations.

Personal Email Accounts & Text Messages

Traditional email use as the primary mode of communication increased with the shift to a work-from-home environment, including the use of personal email accounts to conduct day-to-day business. While there are robust and defensible e-discovery workflows in place to preserve and collect enterprise-level corporate email accounts, similar workflows must now be implemented to preserve and collect personal email when such accounts are used for business purposes.

When faced with an obligation to preserve data, custodians must first be questioned about the existence of personal email accounts and should be advised about their obligations to preserve any potentially relevant business communications in these accounts. While certain cloud-based email providers have made it quite easy to hold and collect relevant emails, other email providers often require more manual processes.

At its core, personal email usage complicates e-discovery because messages are not under a company's centralized control. The best solution to this problem is for companies to forbid the use of personal email for business purposes; however, it seems unrealistic to enforce such strict policies in a remote work environment. Even if an employee is careful to separate work emails from personal emails, one can accidentally respond to a work email from a mobile device with a defaulted personal email account or default to a personal email account when a work email account is not easily accessible. Nonetheless, organizations need to be proactive and create a comprehensive compliance policy surrounding personal email use. Companies can also consider providing easy alternatives to employees who may default to the use of a personal email account by providing remote desktop servers for employees to easily use their work email accounts. Ultimately, employees must understand that business data is discoverable, regardless of the device used, and this data needs to be preserved.

Companies may also consider requiring employees to obtain approval from compliance personnel or in-house counsel if personal email accounts are used for professional purposes, and best practice requires companies to craft policies and procedures surrounding personal email use that are distributed to all employees for review and signature. Follow-up trainings and routine check-ins are also beneficial to ensure employees not only understand the guidelines in place, but are also following these company mandated policies.

Along with personal email accounts, traditional SMS text and chat messages on personal mobile devices have gained popularity in the realm of business communications. While e-discovery professionals have experience in collecting, reviewing, and producing these relevant communications, the increased volume, preservation obligations, and encumbrance to identify the relevance of these communications requires additional expertise and diligence. Preservation becomes especially difficult with multiple personal devices and accounts, and improperly stored data could later interfere with data collection and legal holds.

As such, companies should decide whether to issue company-owned devices or require employees to bring their own devices for business purposes. If the latter, it is imperative for organizations to remind employees to use only company-approved communications platforms and accounts or risk the discovery of their own personal text messages and chats in the event of litigation.

Policies should also be put in place to ensure employees do not delete data, and companies should use back up systems, such as cloud applications, to avoid any accidental loss of data. Additionally, organizations should prepare a litigation-related preservation plan to cover, among other things, preservation obligations, relevant mobile device applications, and identification of personnel with pertinent information.

Business Collaboration Platforms Demand Detailed Electronic Use Policies

Collaboration tools have revolutionized how to conduct business in a remote world. While these platforms enhance efficiency and collaboration among personnel, they also pose significant challenges for preservation, collection, review and production in discovery. Several channel-based communication platforms emerged from the pandemic to allow individuals to engage with each other and collaborate about projects via direct messaging and group chats. Some of these platforms even allow organizations to connect to other shared drives and video platforms. While these capabilities make collaborative work efforts easier, storing sensitive corporate information and data in these types of systems means that a company potentially relinquishes enterprise control over its data. Unlike email or text messaging, a custodian for the messages generated by these platforms can be any individual who belongs to a channel in which a message appears. Thus, to preserve ESI one has to place a hold on the entire channel. Additionally, collaborative conversations could span multiple messages over a long period of time and include irrelevant communication. Preservation again becomes difficult because one needs to produce more than the individual messages that contain keywords in order to fully understand the context of an entire conversation. Some of these collaborative tools have introduced functions to allow organizations to manage these eDiscovery issues. Depending on the platform, organizations can set message retention periods and even place entire channels on a legal hold to prevent spoliation. However, these functions differ depending on the platform and version an individual is using.

Ultimately, companies cannot rely on a collaboration platform's tools to ensure e-discovery compliance. It is important for organizations to first assess which collaboration tools its employees are using and become educated on how the tools store data. As with other technological resources, entities can consider requiring employees to use certain platforms to conduct business.

Additionally, it is advantageous for companies to draft policies that define the type of data and scope of discovery that it is concerned about. These policies should inform employees about establishing different channels, including what each channel should be used for, which individuals are authorized to use such channels, what business and confidential information can be discussed, and whether users have the ability to delete any data.

The use of virtual video meeting platforms has also increased exponentially in the remote work environment. Virtual platforms provide an interactive alternative to faceless conference calls. As video usage continues to grow, it is important to understand the data created and stored by these platforms. For example, these platforms often retain a record of every virtual meeting, including the date, time, meeting name, and ID from both recorded and unrecorded meetings.

Platform administrators often have far reaching access to reports on every virtual meeting that has occurred, regardless of whether the meeting was actually recorded. Meetings that have been recorded can often be stored either locally to the user's computer or to cloud storage. Additionally, various types of files are created during recording, including video files, audio files and text files of any chats sent during the meeting.

This technology and type of storage is common. As such, e-discovery professionals have additional obligations when gathering discoverable information from their clients. Attorneys must identify which, if any, virtual meeting platforms their clients are using and be sure that the files associated with relevant meetings from these platforms are preserved, reviewed, and, if appropriate, produced.

Although attorneys play a significant role in complying with e-discovery standards, entities must take charge and create detailed policies surrounding video collaboration platforms. These policies should inform employees of when to use video platforms, when meetings should and should not be recorded, and where those recorded meetings should be stored.

Moreover, companies must ensure that employees save data to a universal cloud to allow for easy preservation and collection.

Administrators can be appointed to enforce policies, create system-wide permission settings, and be cognizant of deletion timelines and storage capacities. As with all policies, companies should routinely follow up with employees to ensure individuals are compliant and understand the guidelines.

Data Management & Security Challenges

Considering the vast number of communication tools available to keep colleagues connected, data management and security has become increasingly important, especially in the e-discovery space. As such, e-discovery professionals must re-think existing methods of data identification, and companies must continually update security policies to keep pace with this ever-changing landscape.

Rethinking Data Identification

In its most general sense, data management refers to the methods by which a company organizes and maintains its data. In the remote work environment, employees develop a certain autonomy when it comes to the filing and retention of information. As such, employees may create unique electronic filing systems on shared drives and desktops that are as unique as their work-from-home offices. Different filing systems and folder structures make it increasingly difficult to identify the location of electronic information, not to mention any haphazardly kept hard copy documents or corresponding data that has resulted from the evolutionary use of various collaboration tools.

Knowing where data resides is the first line of defense to this problem. Companies can remedy confusion during the discovery identification and collection processes by employing uniform policies of data filing, including naming conventions, folder structuring, and document placement. Furthermore, e-discovery attorneys must be aware that documents may not necessarily be in one place and that documents may be stored locally or on personal devices as opposed to on shared networks. Attorneys should consider refining any existing or future custodial interview outlines to account for this phenomenon.

E-discovery professionals must also consider the management of any new data sources, such as the collaboration tools and virtual meeting platforms discussed previously, that gained popularity in the work-from-home environment. At a minimum, companies should have knowledge of the platforms its employees are using to communicate and have policies for the naming and storing of any information resulting from these company-approved collaboration tools. Likewise, attorneys must account for the existence of information resulting from these tools in custodial interviews and data collection exercises.

Proactive Measures

Greater access to communication tools also comes with greater security risk. As individuals use personal devices and home or work computers to access sensitive business information, such information can be compromised if reviewed on a non-secure network. Additionally, virtual video and collaboration tools can expose stored information to threats of data loss.

At the most basic level, a company should have a cybersecurity policy in place which, in its broadest sense, addresses the storing and accessing of company information. Individuals should be accessing company networks from a secure internet connection, and passwords should be changed regularly.

Cloud-based platforms require additional security protocols. First and foremost, companies must have a complete understanding of which information is stored in the cloud as well as which applications are being used by its employees. Uniform policies regarding data access and storage, including the types of information that can and cannot be stored in the cloud-based environment, can help mitigate potential security breaches when accessing, sharing or reviewing sensitive information. Companies should also maintain a list of approved cloud-based collaboration tools and understand the security features of these tools.

Some cloud-based tools offer integrated security measures that make it easier for a company to comply with increased security demands. For example, some platforms allow for the application of sensitivity labels, encryption, and retention policies to enhance information security. However, while these security enhancements exist, it remains incumbent upon companies and e-discovery professionals to stay abreast of each collaboration tool's security features. Companies must

implement such options appropriately, and develop company-wide policies so that individual users comply with security mandates.

Conclusion

The rapid increase of remote work environments has significantly changed the e-discovery landscape. Given the advancements in collaborative tools and increase in individual work autonomy, e-discovery attorneys and professionals must understand and address the challenges a work-from-home environment poses to the identification, preservation, collection, review, and production of documents.

Ultimately, e-discovery professionals can help ameliorate the e-discovery pains that accompany the remote work environment by developing defensible workflows, drafting and maintaining detailed company policies pertaining to device and application use and storage, and knowing which applications are being used by employees.