FTI JOURNAL

ARTICLE

# Extending Your Reach: Best Practices for Collecting Data in a Remote Investigation

September 2020

This third article in a series on planning and managing remote investigations looks at data collection. The first article provided a general overview on the state of remote investigations today, and the second article covered best practices for planning and managing remote investigations.

Traditional methods for collecting data in an internal investigation typically include physically scanning paper documents, imaging hard drives, capturing email from servers, and extracting structured data. When investigations are conducted remotely with little opportunity for close supervision on the ground, those seemingly straightforward tasks may prove difficult.

Even prior to restrictions imposed by COVID-19, today's work environment has accelerated the need for investigators to develop ways to work through the obstacles imposed by distance. Changing business practices — such as the growing reliance by organizations on cloud-based storage systems — have also led investigators to re-examine their methods for uncovering, preserving and collecting essential data securely and defensibly.

When considering best practices for remote data collection today, it's useful to examine the optimal ways to approach three distinct sources of information: (1) paper documents, (2) electronic data and (3) structured data. Here is a look at each.

## Paper Documents

Although the volume of hard copy generated by an organization has largely decreased over the last decade, investigators still encounter paper records, especially in global investigations. Determining their location is a primary task for investigators — at times records may be stored offsite at storage facilities. Once located, ensuring the secure conversion from paper to electronic document by a reliable third party for examination by the remote investigative team becomes paramount.

There are several best practices for doing so:

— **Select a vendor.** Investigators should find and use a reliable, remote third party to collect, scan and upload documents for remote access by the investigative team. Established vendors will send boxes to an organization for trusted employees to pack up (while practicing social distancing) and subsequently retrieve, scan and upload the documents for investigators' review. Some vendors are able to bring their own equipment onsite to perform the scanning.

— **Ask for originals.** When possible, investigators should request original paper documents from third parties like banks to ensure document accuracy and to increase the quality of the image.

— **Stay skeptical.** Investigators should maintain a high baseline level of skepticism due to the physical inability to review original documents for red flags such as signs of alteration.

— **Sequester documents if necessary.** If the steps outlined above come up short, investigators should sequester documents in a relatively safe location, such as a general counsel's office, where they can be protected and either scanned in-house or held until a suitable solution is determined.

## Electronic Data

Previously, electronic data largely came from three primary sources: computers, email and file servers. Now, in addition to collecting from these sources, investigators should review other areas, including "the cloud" (which also encompasses platforms such as Dropbox that are being used extensively by employees working from home) and mobile devices. Determining the scope of this unstructured data and ensuring completeness of recovery can be a daunting task. Further, establishing a defensible chain of custody for the data is crucial.

Here are some considerations for locating and retrieving this information remotely:

— **Collect from mobile devices.** As investigators know, the prevalence of mobile devices has blurred the lines between professional and personal boundaries. Evidence can be found in a text or instant messages across several platforms. Indeed, people sometimes feel more emboldened when communicating on mobile devices as opposed to email. There are ways to effectively capture mobile device data remotely. This could include having a digital forensic practitioner create a remote backup of the device, or having the device sent to a forensic lab via a same-day courier. The process may vary depending upon the type of device and location.

— **Gain access to cloud data.** As noted earlier, organizations are storing an increasing amount of data in the cloud. A key element is the identification of relevant data that exists in the cloud. Examples include the use of Microsoft Office 365 and Dropbox. Often an organization's IT professionals can facilitate access to this data, which allows investigators to remotely capture it. In situations where employees have their own personal accounts, investigators may need the cooperation of the employees to gain access.

— **Provide a link for remote imaging.** It's possible to provide a screen-sharing link to a custodian that facilitates remote imagining by the investigative team. The investigators can take control of a system remotely and create a "live" image or target certain files. If the volume of data exceeds the capabilities of such a session, investigators may need to send an encrypted hard drive (encrypted so that if lost in transit, it is unreadable by third parties) to custodians for connecting to their devices and securely extracting data from them. The remote team can assist and shadow this collection by virtually monitoring the imaging process.

## Structured Data

Structured data is typically defined as transactional data that is stored in a database, like accounting or sales data. This category of information presents some of the biggest hurdles in a remote investigation.

— **Ensure data is complete and accurate.** An important step normally would be to monitor how an employee extracts the data, which includes using dedicated written code and understanding what, if any, data filters have been applied. In situations where an organization has created their own bespoke system, it would require working with the organization's computer code developers to understand the underlying data model. But with in-person meetings no longer possible in the current environment, this takes on a new dimension of difficulty.

  Additionally, the collection of structured data is rarely limited to only the information technology department. For example, if collecting accounting system data, it would be imperative to discuss with the accounting and finance teams as well. Comparing the collected data to contemporaneous financial statements ensures accuracy and completeness. If in-person meetings are impossible, coordination of multiple departments and identifying the right resources becomes crucial.

— **Consider all security measures.** Because of limitations noted above, remote teams may need to discuss additional security measures — such as using external encryption applications — to ensure adherence to client security and data transfer policies. Many organizations are wary of screensharing data due to security and data protection concerns. An upfront discussion with an organization's information technology security team will allow for the development of an approach that is approved by the organization and secure.

— **Establish broad data parameters.** With these concerns in mind, the remote team may want to consider being overly inclusive in establishing data parameters at the outset to minimize the need for subsequent back-and-forth in collection. If investigators and clients are unable to work through feedback on data extractions needed in real time, a phased approach to collection can establish accuracy and save time. Remote investigators must consider time lags when collecting structured data remotely, especially if the client uses offshore storage and teams to extract it. By confirming that a smaller sample is correct and complete, one can avoid a large delay due to extracting large data sets over days and weeks that ultimately need to be re-pulled.

## Conclusion

Collecting data remotely can be accomplished effectively and securely, even with categories of data that raise more challenging issues, while navigating data protection rules. In many cases, remote investigators can use successful work-arounds to ensure the integrity and completeness of their collections of paper, electronic and structured data.

In the next article in the series, we will look at best practices for conducting remote interviews, from planning to technological considerations.



AUTHORS

**MAURICE CRESCENZI**
Managing Director
maurice.crescenzi@fticonsulting.com

**VEERAL GOSALIA**
Senior Managing Director
veeral.gosalia@fticonsulting.com

**HANNAH HAMBURGER**
Managing Director
hannah.hamburger@fticonsulting.com

**TARA MULKEEN**
Senior Managing Director
tara.mulkeen@fticonsulting.com

**BRIAN C. ONG**
Senior Managing Director
brian.ong@fticonsulting.com

**EDITH WONG**
Managing Director
edith.wong@fticonsulting.com