FTI JOURNAL

ARTICLE

Where to Look for the Smoking Gun of Data in Today's Forensic Investigations

June 2021

The large-scale shift to remote working and use of mobile devices means investigators must dig for data and communications in unconventional places.

In Brief

The pandemic accelerated certain trends related to data collection in a forensic investigation. Investigators now have multiple entry points when hunting for potentially incriminating data thanks to employees' use of their own digital devices, communications platforms, and casual attitudes about sharing information with colleagues. At the same time, good old fashioned intuition, knowledge, and pursuit remain unchanged in the profession.

Why would an employee have saved sensitive company information on his 12-year-old son's desktop computer? It sounds a bit fishy, especially to a forensic investigator hired to track down digital documents relevant to a company investigation. Was the employee trying to hide something?

Turns out the father had a reasonable explanation: He used his son's computer because it's connected to the family scanner.

Today's forensic investigators on the hunt for digital evidence operate in a changed world. With the large-scale shift to remote working accelerated by the pandemic, the variety of devices employees use to conduct business and communicate with colleagues and clients has greatly multiplied. We're using our company-issued laptops and smartphones to hit send and reply, we're holding virtual meetings on our personal computers and devices and we're connecting with coworkers through chat in applications such as WhatsApp, iMessage, and WeChat.

It's all about speed and convenience. Since the pandemic, the boundary between our work lives and private lives — already blurred in the years leading up to the shift — has been washed over like a sandcastle built at low tide. Work now demands our attention morning, noon, and night, and that frequently means reaching for whatever device is handy to respond as expeditiously as possible.

At the same time, the methods we use to communicate are evolving. We're firing off IMs and DMs to colleagues through communications platforms — like Microsoft Teams or Slack — that we access on our company-issued and personal devices. We use messaging apps on our smartphones not just to confirm dinner plans back home, but to connect with cubicle colleagues about deadlines, too.

This blurred boundary is a double-edged sword for forensic investigators digging for data. On the one hand, employees may be so casual about communicating on a personal device that they shrug off precaution, which can open the door to their relevance in a corporate investigation. On the other hand, the "technical diversity," or sheer number of devices and applications that employees use to correspond, is vast. Information is far-flung.

That scope can leave companies feeling vulnerable and anxious. Add the pressure of a regulatory inquiry or an ethics breach, antitrust case, or investigation by a regulator, and rooting out cause and culprits can seem overwhelming.

With so many employees working outside of the office, how can forensic experts track down important documents early in the process and help shape the response? Knowing more about this new world of communications and the way in which forensic experts have adapted can help provide companies an opportunity to plan ahead for today's investigation.

Where Is the Data Being Stored?

While the pandemic has brought on new challenges for forensic investigation, remote data collection itself is very familiar to the profession given the move toward the digital office. Investigators have been adapting to the environment for years.

When called in, the investigator typically meets with company officials to understand the scope of the issue and ascertain the type of devices and services the company provisions to the users. From there, the investigator starts to build a map of the known data sources, but this map is only a part of the complete picture.

Pre-pandemic, data collection activities often took place on-site, often with the cooperation of the IT department. Now, forensic investigators must interview individual employees to inquire about other possible locations where they may be storing company data and to assist with securing the credentials needed to access the data. The real-life example of the employee and his son's computer cited above is a case in point.

Examining a company-issued device is fair game, as it is normally the property of the company itself. On-site, the investigator might take possession of such a device temporarily to download relevant information. In today's remote version of that process, the investigator collects data over the internet through a "live acquisition."

The same technique for data collection applies to a personal device but may be more of a challenge as individuals are often uneasy about simply placing a smartphone in the hands of a third party — including virtually. But employees are often reassured when the investigator makes it clear that they are only interested in retrieving business-related records in a "targeted collection."

What Kind of Information Is Being Shared?

The casual nature of today's communications plays a big role in where the investigator looks for evidence. Once upon a time, email was the primary way we electronically exchanged information with work colleagues. In and of itself, the method had a certain formality and could be relied on as a potential source of evidence. But over the years, the speed of business and demand for instant response, plus the sheer variety of informal chat and texting platforms (and perhaps the allure of expressive emojis), have loosened up how we express ourselves.

The result is that we share more information on the fly and sometimes let down our guard on protecting proprietary information. We may chat on our company and personal devices about a business contract or competitive bid through a communication app installed in both places. We may even chat with company outsiders about business under the expectation that nobody will ever see the messages.

For investigators following a string of internal or external communications or seeking to connect the dots from evidence collected elsewhere, a texting app can provide a veritable treasure chest of highly relevant evidence.

What Is the Employee Hiding?

One of the first actions an investigator tells a client to do is to preserve company data and other information for use as possible evidence. That means any unusual digital activity by an employee just prior to or during an investigation — such as using a USB drive to copy a large volume of data, for instance — can raise a red flag.

Consider the employee who suddenly deletes files. While we all send files to the trash regularly, An employee who deletes files just prior to an interview or before granting the investigator remote collection access may raise concerns. The same could apply if an employee withholds the information during an interview that they use a data storage platform privately for storing company data.

Such behavior might be a sign of something untoward — or not. A simple question to the employee about whether he has any work-related items stored on the platform might suffice during the collection process. But if the investigation is potentially criminal in nature, such as intellectual property theft, withholding information can send a signal that further investigation is needed.

Conclusion

The pandemic era accelerated trends already in the purview of forensic investigators who are hired to collect and preserve data. As the way we do business changes, so too does it for investigators, who must always be one digital step ahead.

VEERAL GOSALIA
Senior Managing Director