MARCH 14, 2018

Legaltech® news

ONLINE

An ALM Publication

Data Matters When Investigating Alleged Workplace Misconduct

Forensic technology can help augment workplace misconduct investigations and can help uncover information required to resolve these matters.

BY SEAN TUTTLE AND PATRICIA SMALDONE, STONETURN

Workplace misconduct allegations involving discrimination and harassment complaints have been dominating headlines, giving rise to awareness and prevention campaigns such as the #MeToo movement that surfaced after sexual harassment charges were made against many well-known celebrities.

The advent of social media platforms like Facebook and Twitter, instant messaging (IM) and the use of texting as a preferred means of communication, have made it easier for would-be harassers to engage in non-professional behavior with colleagues and trigger misconduct allegations. Ironically, these communication tools create a data trail that allows forensic technology analysts to expeditiously trace inappropriate interactions between parties and accelerate the lifecycle of misconduct allegations.

This issue continues to be a problem across corporate America, as evidenced by a 2016 study released by the EEOC that states "anywhere from 25% to 85% of women report having experienced sexual harassment in the workplace."

When the employer responds with an investigation, all potentially relevant data must be collected immediately and forensic technology tools should be utilized to analyze the data and build a comprehensive report outlining a sequence of events. Below is a roadmap of how forensic technology augments

workplace misconduct investigations and can help uncover information required to resolve these matters.

Computers and devices tell a story. Forensic technology measures ensure that story is told accurately.

Computer and other device activities all leave an imprint, telling the story of the user's daily activities and communications. Collecting work-issued computers and devices immediately after a claim is filed is of utmost importance for a successful investigation because electronic information can be deleted or altered.

As there are massive amounts of data stored within computer applications and operating systems, most misconduct investigations involve mining for electronic data that is either stored on company computers or electronic devices such as cellphones, laptops and tablets. Even if information is deleted, computer forensics can trace the steps of the parties involved to provide the evidence needed for fair and resolute decisions. Sometimes, even the act of trying to eliminate information will leave tracks. Thus, it is essential to bring in independent, third-party forensic analysts early in the process to ensure that hidden or deleted information can be obtained quickly and used as evidence of relevant actions.

Finally, in "simple" investigations in which data can be easily retrieved (i.e., temporary or intact files on the computer, unscathed recycle bins, clear browser history, etc.) one must be able to prove that the subject of the investigation is responsible for the evidence. Without the use of the right tools and procedures, it is difficult to clearly connect evidence that is collected from a computer or device to the suspected employee.

Mining for data: What type of information can forensic technology tools uncover?

Social media platforms and IM applications not only allow employees to engage in non-work-related communication but can also be used to harass coworkers. These devices and supporting technology serve as evidence in workplace misconduct investigations, emphasizing the importance of an objective analysis of all work-issued devices that are collected from the parties involved.

Using the most advanced software and technology applications, forensic technology analysts can create forensically sound images of work-issued devices and relevant user accounts including:

- Deleted files on the hard drive;
- A list of deleted file names, even those that cannot be recovered;
- Installed software, which identifies suspicious non-work sanctioned programs;
- Temporary Windows files, which show the user's recent work, even if not saved;
- Website activity, including specific websites visited, and corresponding timestamps;
- Sent/received e-mails and text messages; and
- IM conversations.

Wrapping up the investigation: Analyze the forensic data and compile a report.

During the evidence collection process, HR professionals need a "smoking gun" to wrap up the investigation quickly and resolve the matter. But even smoking gun evidence will be of little value if you fail to establish that the data was not tampered with during the investigation.

Therefore, it is important to incorporate sound methodologies and use specialized computer forensic software/hardware to collect the evidence and ensure that the subject's computer or devices were not altered in any way during the evidence acquisition process. For example, even the act of turning on a computer

causes the operating system to write information on the hard drive, thus potentially overwriting information that might otherwise be useful, such as critical date stamps and the eradication of temporary data on the drive.

Once collected and preserved, this data then needs to be analyzed thoroughly and compiled into a detailed report for use by the HR professional investigating the matter and in-house corporate counsel remediating the complaint. A well-written report can help an employer minimize the risk of liability, and the following elements should be included, if available:

- Websites visited (Including the date of the most recent visit)
- Web cookies and Favorites
- Files downloaded
- List of most recently accessed files
- IM friends list (including social media platforms like Snapchat and Facebook messenger)
- IM chat histories
- A list of graphic files that remain on the computer
- E-mails and text messages (keyword searches are performed to narrow down a list of specific inappropriate communication between the two parties)
- Inappropriate or harassing social media posts between the parties
- Badge activity (i.e., was John Doe/Jane Doe in the same building/on the same floor when the alleged incident took place?)

Conclusion

Workplace misconduct investigations are often complex situations for everyone involved—from the person filing the allegation and the person accused of misconduct to the HR professional investigating the claim and the corporate counsel responsible for resolving the matter. However, if a company or employer does not act immediately after an allegation is made, it will become more difficult to collect evidence because documents and data can easily disappear and corporate risk possibly increase. Forensic technology tools, objectivity and expertise are essential to the process, as evidence found through computerized data can confirm suspicions or provide explanations that can result in the need for disciplinary action.

***Sean Tuttle**, a Partner with **StoneTurn**, leads the firm's Forensic Technology practice. He is an EnCase Certified Examiner. **Patricia Smaldone**, VP of Human Resources with **StoneTurn**, leads the firm's Human Resources function.*

StoneTurn

Sean Tuttle
Partner
t: +1 617 570 3773
e: stuttle@stoneturn.com

Patricia Smaldone
VP of Human Resources
t: +1 617 570 3711
e: psmaldone@stoneturn.com