

The Metropolitan Corporate Counsel[®]

www.metrocorpcounsel.com

Volume 18, No. 10

© 2010 The Metropolitan Corporate Counsel, Inc.

October 2010

Evidence Considerations In Employment Disputes – Part I

Paul Neale

DOAR LITIGATION CONSULTING

This is the first of a two-part article focusing on the management of employment disputes. The second article will discuss how to best prepare an employment litigation for trial based on the jury research we have conducted and the verdicts and settlements that have resulted in cases that we have supported during trial.

There are three general classes of employment disputes that we are most often involved in during the pre-trial, discovery phase – 1) internal investigations and ensuing litigation associated with theft of trade secrets claims primarily surfacing when employees resign from a corporation; 2) investigating and defending sexual harassment and/or wrongful termination allegations; and 3) multi-plaintiff/class actions alleging violations of the Fair Labor Standards Act (FLSA) or relating to claims of race, sex and/or age discrimination. The second category is particularly relevant in light of all of the downsizing that has occurred in companies across the country resulting from the past year's economic crisis and the third category represents one of the largest areas of litigation concentration for corporate counsel (see *Fulbright & Jaworski's 6th Annual Survey*).

The proper management and analysis of information in all types of employment disputes are particularly critical as

Paul Neale is President and CEO of Doar Litigation Consulting.



Paul J. Neale

the allegations most often involve very recent events within relatively short timeframes and almost always hinge on 1) who said what (or sent what) to whom, and 2) what information was taken from where and when. In multi-plaintiff/class action matters there is the added consideration of how to manage a large amount of information relating to wage and hour data originating from human resources systems and payroll databases. Each of the three categories is discussed in more detail below.

Theft Of Trade Secrets Claims

A group of employees resign and it is well known that they are going to a company that is in direct competition. Furthermore, there is a concern that they collected and copied information that is proprietary to the client organization. What the former employees do not know is that a tremendous amount of informa-

tion regarding what files were accessed and whether and to where they were copied can be gleaned in a relatively short timeframe through a forensic investigation of the computer systems used by those employees. Unfortunately, in most cases the corporation most often doesn't know it either as evidenced by their attempts to conduct their own non-forensic investigation which often alters, or at least makes less reliable, critical information.

For instance, in the Windows operating systems, when an external storage device (e.g. USB drive) is connected to a computer, an entry is created within the registry on the computer that pinpoints the exact time the drive was connected and the make, model and sometimes the serial number of the drive. Not coincidentally the timing of the drive connection almost always coincides with the timestamps which are created when a computer accesses a file or files. A listing of several (often dozens or hundreds of files) that were accessed chronologically in very short time intervals is a clear, tell-tale sign that files were copied from one location to another. While this evidence is strictly circumstantial, the company is immediately much better informed than they were previously and is in a much better position to question the former employee about their actions preceding their departure. Oftentimes, the device that was connected to the computer turns out to be a drive that is not owned or in the control of the company. The serial number of the external drive can be determined through a quick analysis of the computer's system files.

Other evidence of copying/moving electronic files includes references to

For more information about DOAR, visit www.DOAR.com or call (800) 875-8705.

URLs or Internet addresses that indicate file transfer sites or other remote systems to which information was copied as well as other logs that reveal when an employee accessed the company's systems or servers (e.g. evenings, weekends, holidays) prior to his or her departure. Determining what files were deleted from the former employee's computer through forensic analysis can also provide a lot of information regarding the employee's intent and, in many cases, can be used as the basis for a possible referral to the district attorney for a criminal case depending on the venue.

In these types of cases, data most often exists on the computer of the former employee and on the other systems that the employee used during the course of his or her tenure at the company. Therefore, it is important that the company obtain these systems from the former employee and secure them as soon as the theft of information is suspected so that the evidence is properly preserved. Another word of caution – do not conduct your own data investigation unless you have a certified forensic examiner on staff as we often see well-intended technical efforts destroy critical evidence.

Sexual Harassment/Wrongful Termination Suits

Unlike theft of trade secrets claims, these types of suits most often involve verbal and/or written communication and, of course, oftentimes physical interactions. From an evidentiary standpoint, the increase in the number of methods available for communication has provided both a challenge and an opportunity for corporations. While email communication is still the most prevalent way in which employees communicate, other sources such as instant messaging (e.g. AOL, Blackberry Messenger, etc.), social networking sites (Facebook, LinkedIn, MySpace, etc.) and texting are widely used for the communications that are often the basis for these types of suits.

One challenge in managing communications from these sources is that the potential plaintiff may retain more damaging communications while the alleged offender is unlikely to actively retain any of the communications. Out of context, these communications can take on a very different meaning than if the entire conversation string was available making

these suits very difficult to defend. Of course, having access to more information may allow the corporation to make a quick determination that the suit has merit and avoid the time and expense of defending a suit that should be settled.

Immediately upon learning of a potential suit the corporation should secure all of the computers and devices that may have been used to communicate with the complainant. This includes, to the extent possible, those used by the complainant. Depending on the type of communications, vital information may only reside on those computers and devices. While email communications are often stored on a corporate email server, instant messages and chats are stored, if at all, on the devices themselves unless a corporate instant messaging service has been set up otherwise, which defeats the purpose of an IM service. Instant messaging services such as AOL, Yahoo and others are sometimes configured to store the conversations on the individuals' computers in a form that can be collected and reconstructed by a qualified individual with the correct software. Therefore, home computers should be considered in scope as well as company computers.

One should also investigate whether IM or text conversations were stored by the user in another form and/or forwarded to an email account. This is occasionally the case as a potential plaintiff may be collecting these conversations to bolster his or her case. However, the plaintiff may not provide all of the conversation strings in his or her possession when the complaint is made so you should collect and analyze available email messages from all parties involved. You should also consider putting the complainant on notice of his or her obligation to properly preserve any relevant information on computers, handheld devices or other systems (e.g. cameras, tape recorders, voice mail).

Multi-Plaintiff/Class Action Employment Litigation

There has been a notable rise in the number of employment class action filings over the past two years. As these are most often related to wage and hour claims, the information to defend the litigation is voluminous and disparate. The data that proves or disproves the plaintiffs' allegations are usually in corporate enterprise systems used by human

resources, accounting, sales and/or operations. The details are often among hundreds of thousands or millions of database records. For instance, data relating to wage and hour claims will not be limited to the payroll system. Emails, calendar items, security access control entries and telephone records may also be data points that need to be analyzed to determine an employee's exempt or non-exempt status in a case arguing that the plaintiffs should have been receiving overtime pay. Information from disparate systems can be as effective in defending these suits as in asserting them.

Corporate defendants should, as in any litigation, take immediate steps to identify and preserve potentially relevant sources of data. Plaintiffs' counsel should be proactive in learning more about the corporation's systems and indicate what information they think will be needed to support their claims. The parties should work together to come to an agreement as to what data from which systems will need to be collected and produced and should consider taking a sample from each system for a subset of employees to verify that the information sought is actually available and statistically relevant.

Attorneys should formulate a voluminous records management plan that most effectively summarizes the many data points in a way that can be most easily supported by their experts and most effectively presented to the jury. A well-designed, interactive chart that pulls data from a database containing all of the data points is much more effective than a dense, data-intensive report or statistical analysis.

While information management is always a challenge in any legal dispute, it is even more challenging in employment disputes as there is a more intense focus on data due to the forensic expertise required in theft of trade secrets disputes, the technology available for interpersonal communications in sexual harassment and wrongful termination claims, and the voluminous records contained in disparate enterprise applications in multi-plaintiff/class action litigation. The key to successfully managing information in these types of disputes is creating an effective data management plan that takes all of the potentially relevant sources into account.