

Managing Risks of Trade Secret Disclosure in the Electronic Age  
Ralph A. Zappala

Lewis Brisbois Bisgaard & Smith LLP  
One Sansome Street, Suite 1400  
San Francisco, CA 94104

Digital communication adds to the demands made upon counsel and insurers. When trade secret and commercially sensitive information may be at the center of litigation, steps must be taken to protect trade secret information. Digital storage and retrieval systems are the target of 21<sup>st</sup> Century litigation.

The following is a brief case of study, based upon hypothetical circumstances, that serves to highlight the demands on counsel and insurers when faced with trade secret matters during the course of litigation.

I. The Case in Controversy

A notice of claim ends up at the desk of the insurance company home office, referring to a lawsuit. The lawsuit has been on file for over a year.

The insured is a privately held cable television service company called Cable, Inc (Cable). The initial lawsuit claimed unlawful commercial interference against a mid-level sales engineer for Cable. Cable used its local law firm in Maine to defend the case. The named defendant and employee of Cable, William Peters (Peters) is alleged to have used an Internet service provider's chat room to spread false information concerning Excessive Enterprises, Inc. (EEI). EEI, a publicly traded company, acquired M&P Services (M&P) that previously employed Peters. Peters disagreed with the EEI's plans for M&P following the acquisition and he and several other middle management employees, working out of the M&P office in Hillsborough, Ohio, quit suddenly and before EEI completed the acquisition of M&P. Cable also operated an office in Hillsborough. Peters and several of his co-workers decided to quit EEI and go to work for Cable after Cable's executives recruited Peters' manager, Jim Spence (Spence).

Peters is said to have used the internet to pose as an insider at EEI and he proceeded to make disparaging and uncomplimentary statements about EEI, its business practices, its investment plans, its Board of Directors and its Executive Officers. Peters is also said to have used the internet chat rooms to make statements designed to drive down the price of EEI's publicly traded stock and steer customers away from EEI.

Cable, through its local law firm in Maine, provided defense counsel for Peters in response to the lawsuit filed against him in Nevada. Nevada was selected as the place to sue primarily because EEI had its corporate headquarters there; the Internet service provider was located there; and, most importantly, EEI's attorneys had a practice in Nevada.

During the course of the year prior to advising the insurance company of the suit, Cable's attorney, defending Peters, produced Peters for deposition testimony and turned over to EEI Peters' personal laptop computer. EEI through discovery also took deposition testimony from Peters' co-employees, including Spence, who were also former employees of M&P.

Armed with this additional information from discovery, EEI filed an amended complaint, alleging numerous causes of action, including unfair trade practices, wrongful interference with contract, trade liable, and theft of trade secrets. EEI claimed that the establishment of Cable's business in Hillsborough could not have occurred without the theft of client and contract information stolen from EEI by Spence, Peters and other alleged conspirators formerly employed by M&P. Following this amended complaint, Cable put its liability carrier on notice, and the liability carrier engaged counsel selected from the FDCC to defend Cable. Defense counsel immediately removed the case to Federal Court. Cable fired its former attorney. Peters hired his own attorney, and the case proceeded with no holds barred. EEI assigned six attorneys to its legal team. Peters hired the best first amendment attorney he could find, and he was able to convince Cable's liability carrier to pay for his defense.

## II. Litigation & Discovery During the First 120 Days

EEI sought \$25,000,000 in damages in its claim against Peters and Cable. EEI was armed with information, obtained by subpoena from Bahoo, the Internet service provider. The information clearly identified Peters as the source of disparaging information about EEI. EEI also had Peters' personal laptop computer. EEI had its electronic information specialist scour the hard drive. The result of this discovery was a printout of every email sent to or received by Peters, including emails exchanged with co-employees and executives of Cable that were incriminating for various reasons including the sharing files containing pornographic information and sensitive commercial information regarding Cable's customers.

The case, having been removed to Federal Court, subjected the parties to all of the rules and requirements of the Federal Discovery statutes and in particular Rule 26. The depth of discovery seemed without limits. The amount of damage that could be caused to Cable and its

Managing Risks of Trade Secret Disclosure in the Electronic Age

customers, business relations and reputation could not be overstated. Additionally, EEI had considered Cable a potential acquisition target and was competing head-to-head with Cable in various metropolitan markets for market share. EEI's litigation could be described as acquisition of a target company by means of litigation and attrition.

Cable's insurer was required to provide a flawless defense while at the same time avoiding the destruction of Cable by the litigation process.

Cable, convinced that EEI was over-extended, wanted to delay discovery and trial. Cable believed the current Chairman of EEI would be replaced when earnings for the company fell off due to poor acquisitions and business plans for expansion.

Peters, having found the ultimate defender of first amended rights as it pertains to use of the internet, wanted to have the free speech case for the 21<sup>st</sup> Century with his name on it, and he wanted the insurer for Cable to pay for that process at least to some extent.

### III. The Use of a Confidentiality Agreement

Nothing can be more frustrating to an insurer and its counsel than having to deal with discovery in Federal Court, particularly when steps are necessary to protect the confidential information of the defendant insured in a case alleging that the defendant insured wrongfully acquired trade secrets. In the hypothetical case of Cable, it was faced with having to disclose information concerning over 500 customers that were also customers of M&P and EEI. EEI contended these customers were doing business with Cable as a result of the wrongful theft of trade secret information by Peters and other former employees of M&P that went to work for Cable. The trouble with being sued for wrongfully acquiring trade secrets is that as the target of that lawsuit is your "trade secrets". They become subject to scrutiny by your competition. In this case, EEI and Cable were in the same market looking for and working with the same clients and vendors. Attached hereto as Appendix A is an exemplar Stipulation and Order for Protection of Confidential Information. It is expensive, time-consuming, confusing, and intimidating to operate under such a stipulation and order. Without such an agreement, the insured-client defendant has no means of protecting itself against the loss of information through discovery that ends up in the hands of the competition.

### IV. The Discovery Plan

The next consideration has to do with conducting discovery. Explaining to a Federal Magistrate how information should be removed  
Managing Risks of Trade Secret Disclosure in the Electronic Age

from a hard drive without destroying the integrity of that information is not easily accomplished. This leads to the added expense and complication of a court-appointed special master for all discovery matters. Of course, this cannot occur without approval of the court. There is no guaranty the court will grant such an order. The parties may find that the magistrates do not want to relegate authority to a discovery referee for hire.

The next step is organizing and preparing for disclosure of discoverable information under the very broad and over-reaching provision of Federal Rule 26. Cable has offices in several cities. The employees and offices communicate by computer. Customer information is tracked in no consistent or organized fashion except when it comes time to write an invoice for services and product. That information is stored electronically at a mainframe computer at the company's headquarters in Maine. A conservative estimate is that if all information was reduced to paper, there would be 90 banker boxes of documents that would be subject to disclosure.

It is little consolation that counter-discovery can be directed to EEI. The cost of photocopying documents downloaded from computers and identified for the first round of document discovery is equivalent to the price of a Ford Explorer.

The court's adoption of the Confidentiality Agreement requires that prior to disclosure the documents must be reviewed and designated as to whether or not they come under the Confidentiality Agreement. The same is true for any deposition testimony taken in the case or any portion thereof. Cable is not just concerned but scared to death its customer information; its costing analysis; its competitive bidding procedures; and, its outstanding competitive bids will be put in the hands of EEI, resulting in the instant down-turn and demise of Cable's business. Identifying documents for designation as confidential and policing EEI for compliance under the confidentiality order is no small task. From a practical standpoint, Cable is forced into asking its customers to essentially turn in EEI for violations of the confidentiality order. (No one on Cable's sales staff wants to do this.) There is no solution short of labeling each document that requires protection under the confidentiality agreement. This is accomplished by using a transparency with the confidentiality inscription placed over the top of each numbered document as it is copied for production and disclosure in response to discovery.

## V. The Computers and Servers

A consultant is retained for the purpose of coming up with a plan for capturing all relevant information off of all computers and servers. This requires a protocol, developed and approved by the discovery referee and

Managing Risks of Trade Secret Disclosure in the Electronic Age

ultimately signed off by the judge assigned to the case. It is the equivalent of an audit. The computer and electronic data consultants for both sides are then faced with selecting a neutral third-party electronic data and computer expert to perform the search of the various servers, desk top computers, and laptop computers, based on the protocol which turns out to be a very complex series of names, words, numbers, and characters that would reveal information about clients, customers, witnesses, transactions, bids, projects and products that have allegedly been stolen by Cable as a result of its use of wrongfully obtained commercial information. Managing this process in many respects is impossible. Both companies are now on the verge of destruction. They are tying up their staff and resources for the purpose of discovery while at the same time potentially alienating customers by asking them to take sides in the dispute between EEI and Cable.

## VI. Law and Motion

What would litigation be without motions to compel and the hearings on motions for protective orders? Attached hereto as Appendix B is an example of a motion for protective order to prevent discovery from going forward until after a discovery plan has been adopted that will take into account all of the challenges of the litigation, including adopting a confidentiality order.

Next, there is the challenge regarding protected speech that Peters is compelled to pursue in his own defense. Attached hereto as Appendix C is an example of a motion, designed to strike claims allegedly arising out of wrongful interference with commercial relations on the grounds that the communications were a lawful exercise of protected speech.

On October 15, 2003, the First District Court of Appeals for the State of California certified for partial publication the opinion in the case *Barrett v. Rosenthal*, 112 Cal.App.4<sup>th</sup> 749. This case discusses how libel and slander occurs on the Internet, and how the courts have struggled to apply new legislation and old judicial concepts in an effort to balance protected speech against the rights of individuals and companies not to be maligned in cyberspace.

Required reading for the cyber litigant is the Communications Decency Act of 1996 and the *Barrett decision*.

## VII. Conclusion

When it comes to litigation involving trade secrets, the impact of the electronic age cannot be overlooked. The most mundane commercial disputes where trade secrets and sensitive commercial information come

Managing Risks of Trade Secret Disclosure in the Electronic Age

into play may lead to a massive exploration of numerous sources of electronically stored information. If there is a workable approach, it begins with defining the area of discovery in very specific terms. The court or discovery master must be persuaded that the plaintiff should first demonstrate credibility in the process. This may be accomplished through a step-by-step discovery plan that initially limits discovery to a specific claim. Next, the court needs to examine the results of the initial discovery to see if the disclosed information supports the specific claim. If a pattern can be established that discovery approved by the court or magistrate reveals little or no probative information, that pattern may be used to convince the court to further limit the discovery plan. At some point, attrition may take hold, and the case may go away.

In the hypothetical matter of EEI, it turned out that most if not all of the allegedly fabricated and demeaning statements about EEI and attributed to Peters turned out to be true, and EEI suffered a terrible financial downturn. EEI had to consider and then accept a nominal settlement amount rather than incur the cost of regulated discovery. The pacing of discovery prevented EEI from using the litigation to financially pressure Cable into selling out to EEI. The cost of continued discovery could not be justified by EEI and EEI could not convince the court it had a legitimate purpose for demanding millions of pages of documents and the contents of countless computer servers and hard drives in view of the adverse public disclosures that were embarrassingly similar to the remarks allegedly made by Peters on the Internet. EEI had to abandon the litigation and focus on earning money the old fashion way. As part of the settlement, Peters, EEI and Cable were all bound to a non-disclosure agreement preventing any public comment on the case.

Managing Risks of Trade Secret Disclosure in the Electronic Age