The Impact of Data Loss Prevention Communications Capture on E-discovery

Naomi R. Fine
President
Pro-Tec Data
Telephone: 650-493-0555
E-mail: nfine@pro-tecdata.com

June 2007

The Impact of Data Loss Prevention Communications Capture on E-discovery

June 2007

I. Executive Summary

Advancements in data loss prevention technologies have implications for compliance with the recently amended Federal Rules of Civil Procedure (FRCP), which address discovery requirements for electronically stored information (ESI).

In interviews with renowned attorneys who spend their days in the trenches of litigation, and whose knowledge of e-discovery and the FRCP amendment is intimate, we learn the following:

1) The FRCP e-discovery requirements to preserve and produce information relevant to litigation do not distinguish between email and any other form of electronic communication. Compliance with e-discovery may therefore require companies to find data across all channels of communication.
2) Use of a system that captures a historical record of communications based on certain criteria and then indexes the information for easy retrieval, is a best practice for complying with the e-discovery rules of the FRCP for companies that are involved in repeated litigation.
3) Information stored by a filter and capture system is not held to a more stringent retention requirement than other of the organization's information. Only if the results of the capture show evidence relevant to actual or threatened litigation, or information subject to statutory retention, would the company be required to save it. In any case, the retention of such information would be in accordance with the company's policies, assuming they are reasonable and uniformly applied.
4) Using a system that captures a historical record of communications to identify, for purposes of a litigation hold under the amended FRCP, and then produce accurate ESI, may save e-discovery costs and reduce the severe risks of spoliation.

The attorneys interviewed encourage companies to think and plan strategically about e-discovery compliance before they are faced with litigation. Based on the experts' responses to the questions presented, it is clear that companies should consider the value of a system that provides an indexed, searchable historical record of communications as a tool for cost-effective e-discovery compliance.

II. Introduction: Data Loss Prevention Meets Electronic Discovery

Data loss prevention (DLP) is not an objective concerning data or information technology alone. Intellectual property, privacy, corporate compliance and establishing organizational trust all rely on DLP. Advancements in DLP technologies have enabled both a new level of DLP and the achievement of diverse corporate objectives.

In her October, 2006 report, *Crown Jewels on the Network: A Benchmark Study of Leading Companies' Discovery and Protection of Intellectual Property*, Naomi Fine described how leading companies use a system that captures a database of historical communications, which is a feature of certain content monitoring and filtering DLP software, for purposes of searching for evidence of wrongdoing after a company is alerted to suspicious activity. When an employee left to join a competitor, for example, one of the companies in the benchmark study used the capture database to determine whether the employee transferred IP, and to whom, before that employee's departure.

In this report, we look at the electronic discovery implications of DLP technology that captures communications with indexing and search tools. Specifically, this report focuses on how such tools are perceived in light of the December 2006 amendments to the FRCP, which address discovery requirements for ESI.

The life's work of the author is assisting leading companies in developing and implementing comprehensive information protection strategies. To get perspective on the question at hand, the author interviewed renowned attorneys who spend their days in the trenches of litigation, and whose knowledge of e-discovery and the FRCP amendments is intimate.

In interviews with Ian Ballon, Eric Sinrod and Cynthia Jackson, whose summary biographies appear below, the author asked the following:

1) Is it important for companies to be able to find data (such as evidence of leakage) across all channels of communication, to include not only corporate email, but also webmail, FTP and various less known protocols, such as IRC?
2) Should companies consider a system that stores a record of communications based on certain criteria and then indexes the information for easy retrieval, a best practice for complying with the e-discovery rules of the FRCP?
3) Is there any reason why information stored by a system that captures a database of historical communications would be held to a more stringent retention requirement?
4) What are the cost implications of using a capture system to identify, hold and produce accurate ESI for purposes of a litigation hold and production of accurate ESI?

The answers provided by the litigation and e-discovery experts are provided below.

II. Conversations with E-Discovery Experts

A. Is it important for companies to be able to find data across all channels of communication, to include not only corporate email, but also webmail, FTP and various less known protocols, such as IRC?

Cynthia Jackson: As far as the FRCP, e-discovery is not limited to email. In the event of anticipated litigation, a company has an obligation to do a good faith diligent search of all those places where relevant electronic information might be stored. No distinction is made in the FRCP between email and any other form of electronic communication.

Eric Sinrod: Electronic data can be found in many different places. Producing only information from servers does not get the job done. You have to get information from live servers and sometimes from backup tapes. You have to consider hard drives, laptops, PDAs, and voicemail systems. In a big case where there is a lot at stake, conceivably a judge could order you to go to all storage devices and all modes of communication to search for, preserve and produce electronic information. While some companies may demand to get to all of the information from their adversary, most will not demand what they are not willing to produce. In some cases, a company will have no choice. They must move forward to produce the requisite ESI. E-discovery is certainly not limited just to email. The definition of ESI is quite broad.

Ian Ballon: Anytime a communication is recorded electronically, it is potentially discoverable. Particularly when you are in litigation, there are heightened obligations to preserve such communications. The most important benefit of a capture database is that it may allow you to discover a problem before it becomes a lawsuit. Any tool that allows you to solve a problem earlier and avoid litigation is worth the cost. This is particularly true for companies with a high litigation profile.

B. Should companies consider a system that stores a record of communications based on certain criteria and then indexes the information for easy retrieval, a best practice for complying with the e-discovery rules of the FRCP?

Ian Ballon: Litigation requires dealing with massive amounts of information, including sorting through email in and out boxes. Typically, lawyers have to sift through millions of records. A system that captures a history of communications in a database with an indexing and a robust search function may be considered best practices, depending on the circumstances. In most organizations, one of the problems is that too many communications are being recorded electronically, including mundane matters. Each time they get recorded, they may exist in multiple, different places in an organization—on hard drives, in an original email, in a forwarded email, in a reply email. The

volume of information has become overwhelming. It has become a significant cost particularly because in litigation, parties typically need to search through these communications. An indexed, searchable capture of communications is a best practice to the extent it enables companies to be vigilant about organizing their electronic communications well in advance of the time they get sued. It might also be considered a best practice to have a record of historical communications that can be searched quickly to discover if there is any evidence of a claimed incident once litigation is threatened. Whether it in fact is appropriate depends on the particular company, its risk factors and the likely threat it faces of particular types of lawsuits.

Eric Sinrod: The negative repercussions if information cannot be found and produced are significant. To the extent there are solutions for companies to get information cost-effectively, such as by searching a database that captures a history of communications, it's in their best interest to do so. No company should put its head in the sand. A company should be in the best position possible to get data wherever it is. Any company that anticipates repeat litigation, and most large companies do, should get their electronic data in order so that they can deal with e-discovery requirements on an ongoing basis. If a communications capture is economical, a company should employ it in the ordinary course of business.

The costs of a communications capture are economical when weighed against the savings in future litigation. For a company that is litigation prone, anticipated e-discovery demands would justify the expense of a capture system. On the other hand, if the system is very expensive and the company never or rarely faces litigation, investing in such a solution may not make sense. But for most companies in the US, litigation is a cost of doing business; it's rare for any company to not face litigation.

Companies are held to a standard of deploying current state-of-the art technology. Deploying technologies that are three years old or not deploying available capture technologies may be insufficient. In any case, it is in the company's interest to monitor communication to ensure compliance with laws and also to ensure the protection of intellectual property. To the extent a state-of-the-art system allows a company to look back into a database to determine if a current event was preceded by communications that indicate unlawful activity, or a compromise of intellectual property, there is high value even if the incident is resolved without litigation.

While using a capture system is beneficial for many reasons, it is not divorced from people making strategic decisions about how it should be used. One must ask in setting up the capture, "Whose communications should be monitored and captured?," "Which will be most relevant?", "Who in which departments, and which executives and employees are the people whose communications will be most relevant?". Technology must be employed with human thinking. It's not sufficient just to plug in a box.

Cynthia Jackson: Attorneys are charged with the obligation of going back and having to look for information relevant and reasonably calculated to lead to evidence. Having a system that allows for retrieval using searches of key words, key individuals and critical dates will improve a company's ability to respond to e-discovery demands. A system that allows you to index information is certainly going to simplify your life.

But a one size fits all is not appropriate. If a company has significant amounts of data (which is increasingly the case), investing in a communications capture system for e-discovery would make sense.

C. Is there any reason why information stored by a system that captures a database of historical communications would be held to a more stringent retention requirement?

For example, if Company A sets a capture system to retain all communications between its chief engineer and any outside organizations, and 98% of those communications are with organizations that are under an NDA with Company A, is there any reason why the Company wouldn't be able to wipe that data according to its wiping/destruction schedule? Under what circumstances might the company be required to retain information in the communications capture on the chance that these communications may become evidence in some future litigation?

Cynthia Jackson: Other than a specific statutory requirement to retain certain types of records, such as tax and HR records, and the requirement to hold documents relevant to anticipated litigation, there is no general obligation to retain information. Companies may choose to retain many documents for business reasons, but other than statutory retention periods or a litigation hold, many companies have good faith and reasonable document retention/destruction polices, because non-mandatory storage can be costly and burdensome. Courts are not going to require parties to retain documents otherwise subject to periodic purging pursuant to a good faith retention/destruction policy "on the chance" that they might be sued, in the abstract. On the other hand, if there is threatened litigation, such that a reasonable person has reason to believe that litigation is contemplated, then the FRCP require a litigation hold of relevant information.

Ian Ballon: If a company creates electronic records, such records are subject to potential retention obligations. However, there is no heightened retention obligation created by a capture database of communications that are already required to be retained. Compared to what is already required, and being done, a capture database, with search capabilities, does not increase the retention burden. Companies are already obligated to retain email. Under these circumstances, a capture database would require no greater responsibility to hold records.

Eric Sinrod: If you have routine retention and destruction policies that make sense in your industry, and you apply them uniformly, then you don't have to preserve a capture of communications any differently. Notwithstanding industry general standards, there is an overriding duty to preserve evidence when you have knowledge of the potential for a lawsuit, or when a lawsuit is filed. The litigation hold doesn't mean you have to preserve everything, only information relevant to the issues that are at stake.

Data takes up real estate. Companies are permitted to have data destruction policies that are reasonable. Assuming the company complies with legally mandated retention requirements, it can dispense information that it does not know to be relevant to a pending lawsuit. A company's obligation to save information depends on the company's state of knowledge. If the fruits of the capture show a likelihood of litigation, only then would the company be required to save the information. But it is a good thing to have a capture system that allows you to know that there is potential litigation. This is much better than not knowing because you can do what is needed as soon as possible. And a capture system that allows you to look back historically to determine if current suspicions or allegations are validated by previous communications can give you a window into whether you have a problem at all.

D. What are the cost implications of using a capture system to identify, for purposes of a legal hold, and then produce, accurate ESI?

Ian Ballon: Any tool that allows an organization to more efficiently identify and retain those business records that in fact may need to be retained, while excluding communications that need not be retained, would certainly save the organization money. And when technology can be used to help retain and preserve evidence, it will help a company avoid the costs of spoliation of evidence. The risks for spoliation have increased dramatically with the recent amendments to the FRCP, which require that parties meet and confer at the outset of a case to discuss electronic record preservation. If the first time a company considers this issue is when litigation is pending, then ultimately the cost of dealing with it is going to be much higher.

A company is at a real strategic disadvantage if it is scrambling with in-house lawyers talking to in-house IT people about what records they have while the other side has a handle on what kind of information they have and want. If a company is not prepared, it is more likely to make a wrong decision under the duress of time pressure of federal court litigation.

Conversely, companies can be much more aggressive in litigation in terms of how they approach the other side if they know what they've got. In situations where I represent a client that fully understands what it has, we are able to be very aggressive at the outset of a case. Sometimes this aggressiveness with e-discovery requests has had the positive benefit of getting a case settled very quickly.

On the other hand, I have had at least one case where my client did not have a good handle on what was being captured and whether and how it was being retained, which put us in a bad position at the outset of the litigation. We were on the defensive and therefore had to be passive and reactive, and not push certain issues that would have put the other side on the defensive because we knew that as soon as we raised certain issues the other side would raise them with us and my client was not yet in a position to be able to address them. If you don't really know what you have, or if there are open questions about what has been preserved or whether relevant records were adequately saved, it puts you at a disadvantage. It can also have a distracting effect on the litigation. If you have to divert resources to evaluate record retention and preservation issues when you have just been served with a complaint, it may be more difficult to focus on substantive strategic issues. You want your resources—especially in-house resources—focused on ways to win the case, not defensive strategies to avoid e-discovery problems.

Eric Sinrod: Non-compliance with e-discovery results in spoliation of evidence. Spoliation occurs if you are on notice of or you are actually in a lawsuit, and you don't make best efforts to preserve information that you know is relevant to the issues in the case. Judges impose serious sanctions for spoliation. A judge may instruct the jury that if the information no longer exists, the jury should assume that the information would have been completely in favor of the party who didn't get access to it and against the party that failed to preserve it. Or, the judge may automatically direct the judgment in the case against the party that failed to produce the evidence. And, there may be severe monetary sanctions for a party that fails to produce relevant electronic evidence.

In a recent case, Microsoft did not produce an email or a database that was requested in litigation discovery by Z4 Technologies. The judge ordered Microsoft to pay a penalty, in addition to the award of damages, of $25 million and $2 million extra in attorney's fees for electronic discovery misconduct. Penalties for e-discovery misconduct can outstrip the value of a case. The effort of locating, preserving and treating electronic data can be very expensive. It can drive out cases and motivate parties to settle when they wouldn't otherwise because they don't want to endure the expense and burden of electronic discovery.

If there is any downside to an indexed, searchable capture of communications, it is that while the technology allows you to be offensive in litigation, to quickly focus on and produce the needed ESI, it deprives the company using the technology of the argument that it would be too onerous to find and produce information that might otherwise only be available from a backup tape. But the counterargument is that the opposing party could have and should have used a similar technology and didn't at its own peril. Counsel could argue that the opposing party should have used the capture technology and had they done so, the requirement to get information from a backup would not be onerous.

A company certainly would not get punished for having a system in place to do the best possible job of capturing and searching for information. If a court is evaluating what a party to a suit has done to comply with e-discovery, they should look favorably on a company that has done everything it can, by employing state-of-the-art-technologies. And the company itself would be much worse off if it did not use a technology that can help them discover a potential problem that may be the subject of litigation.

Cynthia Jackson: The amendments to the FRCP require that counsel specifically address the form and burden of electronic data and retrieval of inadvertently produced privileged information as part of its early "meet and confer" process. The counsel who is able to draw upon technology that allows the search of a database consisting of her client's historical communications across all channels, to identify and ultimately produce evidence related to the litigation, will be in a vastly superior strategic position to negotiate favorable terms at the "meet and confer" conference. The results of a search of a capture database might help counsel know what electronic data her client possesses, how voluminous it is, who are the keepers of the data and the various places that such data may be stored, what forms it takes, what metadata is buried within it, etc. The party and counsel who are only starting to get a handle on these issues once litigation is served is not only putting itself at a strategic disadvantage but also will be scrambling, which is rarely a cost efficient means to respond to anything.

VI. Summary and Key Takeaways

Advancements in DLP technologies, such as an indexed, searchable, historical communications capture function, have implications for compliance with the recently amended FRCP, which addresses discovery requirements for electronically stored information (ESI). .

In interviews with renowned attorneys who spend their days in the trenches of litigation, and whose knowledge of e-discovery and the FRCP amendment is intimate, we learn the following:

5) The FRCP e-discovery requirements to preserve and produce information relevant to litigation do not distinguish between email and any other form of electronic communication. Compliance with e-discovery may therefore require companies to find data across all channels of communication.
6) Use of a system that captures a record of communications into a database based on certain criteria and then indexes the information for easy retrieval, is a best practice for complying with the e-discovery rules of the FRCP for companies that are involved in repeated litigation.
7) Information stored by a filter and capture system is not held to a more stringent retention requirement than other of the organization's information. Only if the results of the capture show evidence relevant to actual or threatened litigation, or information subject to statutory retention, would the company be required to save it. In any case, the retention of such information would be in accordance with the company's policies, assuming they are reasonable and uniformly applied.
8) Using a capture system to identify, for purposes of a litigation hold under the amended FRCP, and then produce accurate ESI, may save e-discovery costs and reduce the severe risks of spoliation.

All of the attorneys interviewed encourage companies to think and plan strategically about e-discovery compliance before they are faced with litigation. Based on the experts' responses to the questions presented, it is clear that companies should consider the value of an indexed, searchable capture of communications as a tool for cost-effective e-discovery compliance.

About the Author

NAOMI R. FINE, Esq., President and CEO of Pro-Tec Data (www.pro-tecdata.com), founded the firm in 1985 to help companies manage and protect confidential information and intellectual property. Ms. Fine is a nationally recognized authority whose depth of knowledge comes from working with hundreds of world-class companies to identify sensitive information, assess needs for protecting it, develop tailored strategies, establish policies and procedures, and provide training and tools that secure competitive advantage. Ms. Fine has been cited by *Fortune, Business Week, Time, USA Today*, the *New York Times Cybertimes*, the *Los Angeles Times* and *The Industry Standard* as a leading expert in her field. Ms. Fine's work for Apple Computer, MCI, and Tandem Computers has been described as exemplary in industry trade journals, including *The Personnel Journal*, *Sales & Marketing Management*, and *Security Management*. Ms. Fine is an authoritative and enthusiastic speaker for many industry associations, as well as being a published author of numerous articles related to information and intellectual property protection. Prior to founding Pro-Tec Data, Ms. Fine was a business attorney counseling high technology companies on protection, licensing and other transactions related to intellectual property. Ms. Fine can be contacted at nfine@pro-tecdata.com.

About the Experts:

IAN C. BALLON is a shareholder in the Intellectual Property litigation group of Greenberg Traurig LLP, and splits his time between the firm's East Palo Alto and Los Angeles offices. Named one of the top 25 intellectual property lawyers in California in 2003 by *The Daily Journal*, Mr. Ballon represents technology, entertainment and media companies in complex copyright, intellectual property and Internet-related litigation and strategic counseling. Mr. Ballon is the author of the 4-volume legal treatise, *E-Commerce and Internet Law: Treatise with Forms*, published by West LegalWorks Publishing (212-337-8443 or www.ballononecommerce.com). He is also the Executive Director of Stanford University's Center for E-Commerce and an advisor to the American Law Institute's International Jurisdiction project. Mr. Ballon may be contacted at Ballon@gtlaw.com.

ERIC J. SINROD is a partner in the San Francisco office of Duane Morris LLP. Mr. Sinrod's trial, appellate, and overall litigation practice, which includes experience before the United States Supreme Court, has covered a number of important Internet, technology, intellectual property, information, communications, commercial, e-discovery, antitrust and insurance coverage issues. He has represented domestic and international clients in major class actions and where hundreds of millions of dollars have been at stake. Mr. Sinrod has been selected by his peers as one of the "Best Lawyers in America" in the area of Cyber Law and as a "Super Lawyer" for Business Litigation. Mr. Sinrod's work has been profiled by the *New York Times*, the *Washington Post*, *USA Today*, the *Wall Street Reporter Magazine*, *Fox News*, *CFO Magazine*, *National Law Journal*, *Cyber Esq. Magazine*, *Business Insurance Magazine*, the *ABA Journal*, the *American Lawyer*, the *California Lawyer*, *Lawyers Weekly*, *Security Management*, *Compliance Week*, *Investor Relations*,

IPFrontline.com, The Village Voice, ROBTV, Newsday, Creditline, Business Credit Magazine, SlashDot and Japanese public television. Mr. Sinrod writes weekly legal columns for CNET News.com, Findlaw.com and CNN.com. Mr. Sinrod teaches Information Law at Golden Gate University School of Law and is a member of the Board of Directors for the Computer Law Association, the Editorial Board of the Journal of Internet Law, the ABA Internet Industry Committee, and the Executive Committee of the Law Practice Management & Technology Section of the State Bar of California. Mr. Sinrod may be contacted at www.sinrodlaw.com and at ejsinrod@duanemorris.com.

CYNTHIA L. JACKSON is a partner in the Palo Alto office of Baker & McKenzie LLP. Ms. Jackson has defended U.S. employers in litigation disputes involving wrongful discharge, state and federal discrimination laws, whistleblower, employment and compensation contracts, work-related tort claims, RICO-related employment claims, ERISA, Section 301 claims and wage and hour disputes. She has also represented employers in administrative proceedings, arbitration and class-actions. Ms. Jackson has represented employers from start-ups to global corporations in a wide range of fields, including biotechnology, aerospace and other high technology companies. Ms. Jackson coauthored the "Age" chapter of Schlei and Grossman's *Employment Discrimination Law* (First Edition) and the "*Reductions in Force and Plant Closings*" chapter of *Advising California Employers (2nd Edition)*. Ms. Jackson is a frequent speaker on labor and employment related issues and has spoken at numerous seminars, as well as at the American Bar Association's subcommittee on Developing Labor Law under the National Labor Relations Act, the National Foreign Trade Council, the State Bar Labor and Employment Law Section, and the Council for Education in Management. She has also been and continues to be a regular guest lecturer at Sciences Politiques in Paris, France. Ms. Jackson was selected as one of the "Best Lawyers of America" and as a "Northern California Super Lawyer" for two years running. Ms. Jackson may be contacted at cynthia.l.jackson@bakernet.com.

