A Discussion on E-Discovery: An Appropriate Rule of Civil Procedure or a Tool for Frivolous Arguments and Invasion of Privacy?

Philip Kim
Walsh University,
North Canton, Ohio, USA
pxkst1@mail.rmu.edu

Richard L. Metzer
Robert Morris University,
Pittsburgh, Pennsylvania, USA
rlmst26@mail.rmu.edu

Abstract

Electronic discovery (e-discovery) is a growing concern for organizations from a legal, regulatory, and compliance perspective. E-discovery refers to the discovery of an organization's electronically stored information (ESI). ESI can include such information as emails, instant messages, office application documents such as Microsoft Word and Excel. Currently as the United States Federal Rules of Civil Procedure stand the E-Discovery Rules require companies to comply with civil litigation requests for legacy data as well as implement legal hold to ensure the appropriate preservation of data going forward. At first glance, it appears that the current e-discovery rules are potentially ripe for abuse, including submitting frivolous lawsuits that can cost the defendant organizations millions of dollars in personnel resources, time, and technical support costs, to an invasion of privacy of proprietary or confidential data under the guise of legal disclosure. And yet since it's inception in 2006 it also seems that within most cases, the e-discovery rules were appropriately applied by reasonable judgments. According to a recent 2008 study nearly 70% of corporations felt that they were not adequately prepared to comply with e-discovery rules and entering into litigation if a lawsuit was presented. The purpose of this paper is to further the ongoing discussion of the benefits and potential pitfalls of e-discovery and to argue the need for additional research on e-discovery rules.

Keywords: E-discovery, legal hold, ESI, discoverable, Information privacy, frivolous lawsuit

Introduction

Electronic discovery or e-discovery refers to the discovery of electronically stored information (ESI) in civil litigation cases. Discovery is the part of litigation where lawyers are able to request information from organizations for use as evidence in support of the claims they will make on behalf of their client, either the plaintiff or the defendant. Frequently the information required is in the possession of one or the other of the litigants but it is not uncommon for important information to be held by third parties such as government agencies or subcontractors that are not parties to the legal action (Withers, 2000). In the United States of America E-discovery rules for Federal cases are documented in the Federal Rules of Civil Procedure. Many of the individual states have adopted the FRCP for use in

state cases as well (Fliegel & Outlaw, 2008). Thurman (2008) explains, "[t]he Federal Rules of Civil Procedure (FRCP) are within the purview of legal counsel. E-discovery is where the FRCP intersect with IT and information security" (p.36). The FRCP requires organizations and individuals to preserve data that is pertinent to legal actions that have been brought or are likely to be brought regardless of what form it is in. Most organizations preserve data on paper or electronically depending on their specific business needs. The FRCP allow lawyers to request a company to produce ESI that they believe to be relevant to their case. What is discoverable? Any ESI that could be stored on desktop personal computers, laptops, network servers and backups, hard drives, removable disks, cell phones, PDAs, social networking sites, and even information exchanged via e-mails and instant messages.

Legal Hold

The rules of e-discovery are clear on the legal obligation an organization has to produce requested information, but when and how does the retention period of requested information begin? According to FRCP, the moment an organization has been issued with a notification of a lawsuit against the company, they are required to be in a legal hold. A hold simply means the company is required to retain every piece of communication as relates to the potential suit (Conry-Murray, 2008).

A legal hold notification requires the company to preserve all forms of relevant data until each of the legal matters have been settled. The key term for the legal hold process here is *relevant*. What is considered relevant within civil litigation? Who determines what is relevant in the case? Is an organization able to withhold information that is considered to be proprietary or highly confidential corporate data?

The organization is responsible for legal holds when they have been formally served with litigation; however there are some interpretations of FRCP that organizations must begin a hold of all data and communication relevant to a potential or even an *anticipated* lawsuit (Dong Ah Tire & Rubber Co., Ltd. v. Glasforms, Inc., 2008; Innis Arden Golf Club v. Pitney Bowes, Inc., et al., 2009). Thus if a company receives a customer complaint and is accused of wrongdoing or negligence, the potential threat of litigation will invoke the legal hold process. Spoliation occurs when evidence is destroyed either with wrongful intent or as a result of a litigant's failure to halt destruction that takes place as a part of its routine data retention or retention media recycle procedure. Examples of spoliation are the shredding of paper documents or the reuse and consequent overwriting of backup tapes that possibly contain evidence relevant to a legal case. Litigants may seek sanctions against opponents who they believe have destroyed evidence. Possible sanctions include costs associated with discovering duplicate records, adverse inference instructions to the jury or even summary judgment depending on how egregious the judge believes the spoliation to be. Adverse inference instructions are instructions to the jury that, in reaching their verdict, they may presume the destroyed records contained information adverse to those responsible.

Potential Inadequacies of the E-Discovery Rule

As more dissatisfied consumers pursue litigation, more companies will bear the burden of storing, maintaining, and managing their massive amounts of data. E-discovery cases have often resulted in extremely high costs in both human and technical resources for an organization. Regarding the high cost of discovery, in its *Protocol on Disclosure of Documents and Presentation of Witnesses in Commercial Arbitration*, the International Institute for Conflict Prevention and Resolution (2009) says the following:

> In making rulings on disclosure, the tribunal should bear in mind the high cost and burdens associated with compliance with requests for the disclosure of electronic informa-

> tion. It is frequently recognized that e-mail and other electronically created documents found in the active or archived files of key witnesses or in shared drives used in connection with the matter at issue are more readily accessible and less burdensome to produce when sought pursuant to reasonably specific requests. Production of electronic materials from a wide range of users or custodians tends to be costly and burdensome and should be granted only upon a showing of extraordinary need. Requests for back-up tapes, or fragmented or deleted files should only be granted if the requesting party can demonstrate a reasonable likelihood that files were deliberately destroyed or altered by a party in anticipation of litigation or arbitration and outside of that party's document- retention policies operated in good faith. CPR arbitrators should supervise any disclosure process actively to ensure that these goals are met. (p. 7)

Fulcrum Inquiry (2008), an e-discovery service provider explains that the high cost is primarily due to the low cost and ease of storing information that encourages organizations to save far more information than is necessary to accomplish their work. When litigation occurs, even though automated searches are far less expense than manual searches, the sheer volume of records that qualify for review by an attorney is far greater than was traditionally the case with paper records. The Sedona Conference (Redgrave, 2007), a legal thought-leading organization, has alluded to the cost and some of the areas of discovery that escalate costs in its eighth principle which states:

> The primary source of electronically stored information for production should be active data and information. Resort to disaster recovery backup tapes and other sources of electronically stored information that are not reasonably accessible requires the requesting party to demonstrate need and relevance that outweigh the cost and burdens of retrieving and processing the electronically stored information from such sources, including the disruption of business and information management activities (p. ii).

In some cases, the organization may not have done *anything wrong or illegal* and yet due to their mistakes or inability to produce the requested information within the litigation timeframe, they could be sanctioned and punished (R & R Sails, Inc., d/b/a Hobie Cat Co. versus Ins. Co. of the State of Pennsylvania, 2008). This appears to be in contrast to the presumption of innocence within the U.S. criminal litigation procedures. Within the e-discovery civil rules of procedure, the burden to provide proof of innocence is on the defendant. In an effort to protect consumer rights, I believe we may have opened a Pandora's Box for frivolous lawsuits and potential invasions of privacy for corporations as well as for employees. As the cases below will show, potential abuses of the e-discovery rules are possible and could lead to significant judgments and legal sanctions.

E-Discovery Cases

Kilpatrick versus Breg, Inc, 2009 WL 1764829 (S.D. Fla. June 22, 2009)

In the case of Kilpatrick versus Breg, Inc., Kilpatrick was able to require Breg to produce all related emails, inter-office memos, and information from network shared drives. Upon review of the initially requested information, the plaintiff argued that additional relevant data for the case may be stored on Breg's back-up tapes (Carder-Kamping, 2009). It was determined during the discovery phase that Breg's back-up tapes were also used for disaster recovery (DR) purposes. Breg was ordered to produce the back-up tapes, so the plaintiff could conduct a thorough search of all the electronically stored information. It should be noted that DR media often contain critical and proprietary company information. For many organizations DR tapes are often rotated on a monthly basis so as to ensure proper back-up version controls and to reuse tapes after they have

gone past the retention schedule. The objective for the organization is to implement reasonable controls to ensure the company is able to access the data on back-up tapes. However, in this instance, the company had not retained the back-up tapes indefinitely? What if Breg had written over the last month's back-up tapes inadvertently or as a matter of everyday course of business? The judge could have imposed an adverse inference sanction. An adverse inference sanction can apply when a company cannot produce the requested ESI. If Breg were not able to produce the tapes, the jury may have negatively inferred that Breg was purposefully or maliciously trying to hide or destroy data. Fortunately for Breg, the IT department was able to produce the appropriate back-up tapes within a reasonable timeframe. Additionally, Breg required that the search of the back-up tapes be subject to a confidentiality agreement.

There are several reasons for concern as the e-discovery rule stands currently. As shown in Kilpatrick versus Breg the cost for producing the requested back-up tapes could have been enormous. From a risk versus cost perspective, an organization may decide to settle the case out of court rather than expend their internal resources and time to answer a discovery request. Although Breg required a confidentiality agreement prior to providing the back-up tapes, what if the tapes contained proprietary intellectual property or prototype data? The confidentiality agreement would require the plaintiff to not share the information, but how could it prevent them from using the information for their own profit? There should be stronger controls on what data the plaintiff can have access to. It should be limited to only what is deemed as relevant to the case and everything else should be redacted. In addition, the plaintiff should bear the burden of the cost of producing and searching through the requested electronically stored information.

Zubulake versus UBS Warburg (S.D. NY 2004)

In April 2005, UBS lost the discrimination and retaliation suit Zubulake versus UBS Warburg. The plaintiff Laura Zubulake, a former saleswoman at the company's Stamford office, alleged her manager had undermined and removed her from professional responsibilities. She alleged that her manager treated her differently from the men within her department. An important event in the case was that UBS had not preserved relevant e-mails *after* the litigation hold had been in place. Because of UBS' inability to produce the relevant emails, the judge gave the jury adverse inference instructions. As Anderson and Barkley (2007) explain, the fact that some UBS employees failed to preserve their e-mails after being instructed to do so was sufficient circumstantial evidence from which to conclude that the missing evidence was unfavorable to UBS. In October 2005, the parties agreed to settle the case privately.

It is important to note that a legal hold notice or lawsuit must always be filed with the courts and submitted to a company at a specific point in time. This date is known as the trigger date. The potential issue here is that while the plaintiff has formally filed a complaint, for legitimate reasons the notice of the lawsuit or hold may not get to its intended recipient for days, weeks, or even months after it has been issued. This is especially true in the case of larger corporations where in-house legal counsel and management are communicating across the country or even internationally. A simple office memo, or inter-office mailing could take several days to be sent and received, the trigger date is a significant piece of the e-discovery maze.

Qualcomm Incorporated versus Broadcom Corporation (S.D. CA 2008)

Several Qualcomm versus Broadcom cases gave the court the opportunity to set precedent in using its power under the FRCP and its "inherent power" (McNeal, 2009, p. 4) to sanction Qualcomm, the plaintiff, for its failure to properly inform a standards development body of its extant patents in the area of the standard that body was developing; failure to properly prepare its witnesses who subsequently gave the court false testimony; and repeatedly concealing documents

during discovery that had been requested and would have prejudiced its case. The court ordered the patents involved unenforceable, awarded defendants more than $9 million in costs and, reported six attorneys to the state bar association for professional sanctioning. Qualcomm had plotted to influence the Joint Video Team (JVT) committee developing the H.324 video compression standard to do so in a way that would necessitate use of two of Qualcomm's patents in order to comply with the standard. Broadcom sought to show that in doing so without advising the JVT of its patents, Qualcomm had waived its rights to enforce the patents with regard to the H.324 standard. Qualcomm claimed in its testimony before the court and in documents filed with the court that it had not participated on the JVT until after publishing of the H.324 standard. Broadcom's sought to discover evidence to the contrary in its discovery. Broadcom was eventually successful in acquiring one e-mail that implied Qualcomm participation on the JVT prior to the H.324 standard. The one e-mail led to 22 others which eventually led to approximately 46,000 pertinent documents and a Broadcom victory.

Conclusion

In today's Information Age consumers are becoming increasingly savvy in their use of technology. Corporations are increasing their reliance and use of electronically stored information (ESI) to conduct their business operations. With the ubiquity of information technology and the wide use of computer systems, there has been an exponential growth in the sheer volume of data output produced (Baron, 2008; Brynjolfsson & Hitt, 1995).

E-discovery rules have opened an avenue for frivolous lawsuits, fishing expeditions, and invasions of privacy. In an effort to provide a framework to protect consumers, e-discovery has created a new revenue stream for attorneys, vendors, and consultants. While the potential for onerous costs of maintaining information so that it can be expeditiously and efficiently produced for litigation exists, there is little evidence in the literature to support such a claim. The same can be said of costs associated with frivolous legal actions. The FRCP have been shown time and again to contain ample checkpoints where litigants have the opportunity to show cause as to why an opponent's requests for information are impossible, too difficult, unreasonable, or that they would result in costs that approach or exceed the alleged damages. A fair reading of the case law on the topic leads one to conclude that judges have been extremely patient and flexible with regard to implementing the FRCP and they have been quite reasonable in ruling on discovery requests and have only ordered sanctions in cases where litigants have been negligent (Withers, 2009). The Sedona Conference has published guidance for jurists as well as for potential litigants (Redgrave, 2007). That guidance teaches how to plan and avoid excessive costs with e-discovery.

Just as e-discovery protocols have been flexible and malleable to enable litigants to obtain justice while keeping costs at a minimum they have also acknowledged legitimate privacy and confidentiality concerns. Creative ways of protecting sensitive information such as hiring a third party to become officers of the court for the purpose of performing e-discovery searches on electronic information and redacting portions of sensitive information before allowing litigants and others to review it (Scheindlin & Redgrave, 2008).

For some organizations properly producing, managing, and retaining a company's electronically stored data has become cost prohibitive, but for most organizations it is not nearly as expensive as *failing* to properly produce, manage, or retain an organization's electronically stored data. Yet there are still some alarming statistics. In a 2008 study conducted by the American Bankers Association (ABA), they found that out of 100 information technology managers from medium to large corporations only 6% felt they could "immediately and confidently" respond to e-discovery requests (Blake, 2008, p.1). The study also noted that less than 10% of respondents felt they received proper legal guidance, while 40% said they received no guidance at all. Over 50% of the respondents said they had no enterprise search tools or effective email searching capabilities. In

total, more than 70% of companies are not ready to respond to litigation (Blake, 2008). Blake (2008) argues that while most organizations are at least vaguely familiar with e-discovery, they do not specifically know how and when the rules apply. While the Federal Rules of Civil Procedure as relates to e-discovery are embarking upon its five year anniversary, a majority of companies are still struggling to find the balance between implementing appropriate and reasonable technical controls and being prepared to comply with the e-discovery rules. The purpose of this paper was to argue the need for further research and cooperation from both the academic and industry research community.

References

Anderson, J. M., and Barkley, R. P. (2007). The brave new world of e-discovery. *The Colorado Lawyer, 36*(8), 83-90.

Baron, J. R. (2008). E-discovery and the problem of asymmetric knowledge. *Presentation at the Mercer Law School Ethics in the Digital Age Symposium November 7, 2008.* Retrieved from http://www.law.mercer.edu/academics/centers/mclep/postremarksfinalx.pdf .

Blake, M. W. (2008). Are you litigation-ready? *Law Practice Today.* Retrieved from http://www.abanet.org/lpm/lpt/tch04081.shtml.

Bryan, K.A. (2009). CPR protocol on disclosure of documents and presentation of witnesses in commercial arbitration. International Institute for Conflict Prevention and Resolution. New York, NY. Retrieved from http://www.cpradr.org/Portals/0/CPR%20Protocol%20for%20distribution.pdf.

Brynjolfsson, E., & Hitt, L. (1995). Information technology as a factor of production: The role of differences among firms. *Economics of Innovation and New Technology, 3*(4), 183-200.

Carder-Kamping, L. (2009). Device maker prevails in pacemaker suit. *Law 360*. Retrieved from http://www.bowmanandbrooke.com/CM/KMSLaw360-Bregverdict.pdf .

Conry-Murray, A. (2008, June). Comply or die: Data disposition must be a priority. *Informationweek, ,* pp. 28-33.

Dong Ah Tire & Rubber Co., Ltd. v. Glasforms, Inc. (2008). WL 4298331 (N.D. Cal. Sept. 19, 2008).

Fliegel, J. & Outlaw, R. (2008). State rulemaking and electronic discovery: An examination of the development of state-specific rules in the area. *For the Defense.* Retrieved from http://www.mayerbrown.com/electronicdiscovery/article.asp?id=4228&nid=11483 .

Fulcrum Inquiry. (2008). Why electronic discovery is expensive. Retrieved from http://www.fulcrum.com/Reduce_electronic_discovery_costs.htm .

Innis Arden Golf Club v. Pitney Bowes, Inc., et al. (2009). U.S. Dist. LEXIS 43588 (D. Conn. May 21, 2009).

McNeal, K. (2009). Note, Qualcomm Inc. v. Broadcom Corp.: 9,259,985 reasons to comply with discovery requests. 15 RICH. J.L. & TECH. 10. Retrieved from http://law.richmond.edu/jolt/v15i3/article10.pdf

Qualcomm Incorporated v. Broadcom Corp. (2008). 548 F. 3d 1004 - Court of Appeals, Federal Circuit 2008. Retrieved from http://scholar.google.com/scholar_case?case=11310044230697690017&hl=en&as_sdt=2&as_vis=1&oi=scholarr .

Qualcomm Incorporated v. Broadcom Corporation (2008). U.S. SD CA Case 3:05-cv-01958-B-BLM Doc. 718 Filed 01/07/2008. Retrieved from http://www.mcbride-law.com/wp-content/uploads/2010/01/Qualcomm-v.-Broadcom-Order-01.07.08.pdf

Redgrave, J. M. (Ed. In Chief). (2007, June). *The Sedona principles (2nd ed.): Best practices recommendations & principles for addressing electronic document production*. The Sedona Conference Working Group on electronic Document Retention & Production (WGI).

R & R Sails, Inc. (2008). d/b/a Hobie Cat Co. v. Ins. Co. of the State of Pennsylvania, 2008 WL 2232640 (S.D. Cal., April 18, 2008).

Scheindlin, S. A. & Redgrave, J. M. (2008). Special masters and e-discovery: The intersection of two recent revisions to the federal rules of civil procedure. *Cardozo Law Review* 30(2), 347-400. Retrieved from http://www.cardozolawreview.com/content/30-2/SCHEINDLIN.30.2.pdf

Thurman, M. (2008). Discovering tricks of e-discovery: Federal rules governing the retention of electronic documents pull info security into the legal domain. *Computerworld*, *42*(5), 36.

Withers, K. J. (Ed.). (2009, August). *Federal court decisions involving e-discovery December 1, 2006 – July 31, 2009*. The Sedona Conference. Retrieved from http://www.fjc.gov/public/home.nsf/autoframe?openform&url_l=/public/home.nsf/inavgeneral?openpage&url_r=/public/home.nsf/pages/196 .

Withers, K. J. (2000). Computer-Based Discovery in Federal Civil Litigation. Fed. Cts. L. Rev. 2

Biographies

Philip Kim, D.Sc. Dr. Kim is the currently the vice president of information security for a mid-sized financial services institution, where he is responsible for managing the bank's network security environment and mitigating information security risks. In the fall of 2010, Philip will join the faculty of the Business School at Walsh University as an Assistant Professor of MIS. He holds a B.A. in Sociology from Indiana University of Pennsylvania, an M.S. in Information Systems Management from Robert Morris University, and a D.Sc. in Information Systems and Communications from Robert Morris University.

Richard L. Metzer, D.Sc. Dr. Metzer is an information assurance engineering manager for a federal government contractor, where he leads a department of cyber security and systems engineers in a variety of information security tasks while personally performing intrusion detection analyst tasks. Richard holds a B.A. in Sociology from the University of New Hampshire, an M.S. in Systems Management from the University of Southern California, and a D.Sc. in Information Systems and Communications from Robert Morris University.