Electronic Discovery in North Carolina

A Guide for Public Sector Entities to the Rules and Tools for Litigating in the Digital Age

Kara A. Millonzi

UNC SCHOOL OF GOVERNMENT

Electronic Discovery in North Carolina

A Guide for Public Sector Entities to the Rules and Tools for Litigating in the Digital Age

Kara A. Millonzi

UNC SCHOOL OF GOVERNMENT

The School of Government at the University of North Carolina at Chapel Hill works to improve the lives of North Carolinians by engaging in practical scholarship that helps public officials and citizens understand and improve state and local government. Established in 1931 as the Institute of Government, the School provides educational, advisory, and research services for state and local governments. The School of Government is also home to a nationally ranked graduate program in public administration and specialized centers focused on information technology, environmental finance, and civic education for youth.

As the largest university-based local government training, advisory, and research organization in the United States, the School of Government offers up to 200 courses, seminars, and specialized conferences for more than 12,000 public officials each year. In addition, faculty members annually publish approximately fifty books, book chapters, bulletins, and other reference works related to state and local government. Each day that the General Assembly is in session, the School produces the *Daily Bulletin*, which reports on the day's activities for members of the legislature and others who need to follow the course of legislation.

The Master of Public Administration Program is a full-time, two-year program that serves up to sixty students annually. It consistently ranks among the best public administration graduate programs in the country, particularly in city management. With courses ranging from public policy analysis to ethics and management, the program educates leaders for local, state, and federal governments and nonprofit organizations.

Operating support for the School of Government's programs and activities comes from many sources, including state appropriations, local government membership dues, private contributions, publication sales, course fees, and service contracts. Visit www.sog.unc.edu or call 919.966.5381 for more information on the School's courses, publications, programs, and services.

Printed in the United States of America
13 12 11 10 09 1 2 3 4 5
ISBN 978-1-56011-631-8
This publication is printed on permanent, acid-free paper in compliance with the North Carolina General Statutes.
Printed on recycled paper

Contents

Introduction

The "digital age" has been upon us for many years, but the legal system continues to struggle to keep pace with the fundamental transformation it has caused in the way people communicate and generate and store information. The discovery[1] of electronic information in civil litigation (e-discovery) is one area that presents particular difficulties for litigants and courts, alike. The sheer volume of data that is now created and stored electronically and the dispersion of that data across multiple platforms and repositories poses ever-increasing costs and burdens on litigants forced to search, retrieve, and review electronic information pursuant to even routine discovery requests.

Different rules govern e-discovery in federal courts than in many states' courts. The United States Supreme Court promulgated amendments to the Federal Rules of Civil Procedure (FRCP) in 2006 (hereinafter 2006 amendments to the federal rules), which were subsequently approved by the United States Congress, to specifically address the discovery of electronic information.[2] The 2006 amendments did not significantly alter the discovery requirements, but they did refine the rules to hone in on the unique issues posed by e-discovery and to alert litigants and courts of the need to address these issues. The North Carolina General Assembly has not amended the North Carolina Rules of Civil Procedure (NCRCP) to specifically address e-discovery.[3] Instead, North Carolina state courts have relied on interpretations of the existing rules governing the discovery of documents to address disputes concerning the discovery of electronic information.[4] As a practical matter litigants' experiences in navigating the difficulties posed by the discovery of electronic information, and even the outcomes of e-discovery disputes, have not differed significantly in the two court systems. Recently, though, the Electronic Discovery Study Committee

---

1. "Discovery" is a pretrial phase in civil litigation in which each party to the litigation may request, among other things, documents and other evidence from other parties to the litigation or compel the production of documents and other evidence from nonparties through a subpoena process.

2. A copy of the amendments is available at www.supremecourtus.gov/orders/courtorders/frcv06p.pdf (last visited March 9, 2009). Congress amended the Federal Rules of Evidence in 2008 to address issues relating to the waiver of attorney–client privilege and work product doctrine. For a copy of the amendments and the associated congressional history, see http://federalevidence.com/blog/2008/september/president-signs-new-attorney-client-privilege-rule-fre-502 (last visited March 9, 2009).

3. Note, however, that the North Carolina Business Court has amended its local rules to include directives to counsel to, at the initial case management meeting, discuss certain topics related to the discovery of electronic information, including the volume of electronic information likely to be subject to discovery, the form of production (i.e., native format or paper), the need for retention of electronic documents and backup tapes, the need for cost-shifting with regard to the production of electronic data, and the need for security measures to protect electronic data. The rules are available at www.ncbusinesscourt.net/New/localrules/ (last visited March 1, 2009).

4. *See, e.g.*, Analog Devices, Inc. v. Michalski, 2006 WL 3287382 (N.C. Super. Ct. Nov. 1, 2006) (analyzing claim that production of electronic information poses undue burden on party under Rule 26(b)(2) proportionality factors); Bank of America Corp. v. SR Int'l Bus. Ins. Co., Ltd., 2006 WL 3093174 (N.C. Super. Ct. Nov. 1, 2006) (denying electronic discovery request on nonparty as unduly burdensome after considering, among other things, the factors set forth in the *Conference of Chief Justices, Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information*). The *Conference of Chief Justices, Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information* (hereinafter *Chief Justices' Guidelines)* is one of several reference guides available to help litigants address common issues presented by e-discovery. It is available at www.ncsconline.org/images/EDiscCCJGuidelinesFinal.pdf (last visited March 1, 2009).

Note that both the opinions are from the North Carolina Business Court. As referenced in note 3, *supra*¸ the Business Court is leading the effort to address e-discovery issues among North Carolina state courts.

of the North Carolina Bar Association, headed by former Chief Justice Rhoda Billings, proposed electronic discovery-related amendments (hereinafter proposed North Carolina amendments) to the NCRCP.[5] The proposed North Carolina amendments largely track the 2006 amendments to the federal rules[6] and likely would serve a similar purpose. To date it is unclear if, when, and in what final form the state may adopt these proposed amendments.

What, then, are the current rules governing the discovery of electronic information in federal and state courts in North Carolina? And how effective are the current rules in addressing the unique issues posed by e-discovery? This guide identifies some of the distinctive aspects of electronic information and analyzes the application of the current rules of civil procedure in both federal and state courts to its discovery.[7] It is organized into four sections—each of which addresses a discrete topic related to the discovery of electronic information and may be reviewed and used independent of the other parts. Section 1 details how electronic information differs from paper documents and discusses some of the special problems (i.e., costs and burdens) posed by e-discovery. Section 2 provides a roadmap as to what electronic information generally is discoverable in federal and state courts in North Carolina and in what form or forms it must be produced. It serves as a guide to the mechanics of e-discovery.[8] Section 3 analyzes how litigants may use both the federal and state rules as tools to effectively contain the costs and burdens associated with e-discovery. Specifically, it examines how the rules foster, and in some cases even mandate, collaboration among parties to litigation in confronting e-discovery challenges. It also explores litigants' abilities to both limit discoverable electronic information and share the costs of its production. Finally, section 4 alerts public sector litigants to common challenges for government entities in complying with e-discovery requirements.

5. The proposed amendments are available at www.ncbar.org/download/litigation/eCommittee.pdf (last visited March 1, 2009). The Electronic Discovery Committee has invited comments on the proposed amendments. *See* NC Bar Association, *The Litigator* (Vol. 29, No. 1 Sept. 2008), *available at* http://litigation.ncbar.org/Newsletters/Newsletters/Downloads_GetFile.aspx?id=6996 (last visited March 1, 2009).

6. Note, however, that as currently drafted, there are a few key differences between the federal rules and the proposed North Carolina amendments. *See infra* notes 67, 81, 90.

7. This guide focuses on the application of the current Federal Rules of Civil Procedure (FRCP) and North Carolina Rules of Civil Procedure (NCRCP) to the discovery of electronic information. Where applicable, references to the proposed amendments to the North Carolina rules will be made in the footnotes.

8. A discussion of the issues relating to the admissibility of electronic evidence is beyond the scope of this guide. "Whether [electronically stored information] is admissible into evidence is determined by a collection of evidence rules. . . ." Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534 (D. Md. 2007) (summarizing evidence rules relevant to determining admissibility of electronic data).

Section 1: How Is E-Discovery Different?

How Does Electronic Information Differ from Paper Documents?

In order to successfully navigate the e-discovery process, it is important to understand how electronic information differs from paper documents and how these differences may impact discovery. Thus, before delving into the nuances of applying the federal and state rules of civil procedure to e-discovery, this first section examines what makes electronic information unique.

Volume and Persistence

The most obvious distinction between electronic information and paper documents can be summed up in one word: volume. Computers are constant fixtures in our daily lives, and with the migration from desktops to mobile platforms, the ability to "stay connected" is virtually limitless. The natural result of the ability to produce data anywhere, anytime is an exponential proliferation of actual data produced. The volume of electronic information generated dwarfs that of paper documents.[9] Not only are electronic documents easily produced, they are very difficult to destroy. A discarded or shredded paper document is, for all intents and purposes, irretrievable. But, when a digital file is deleted, the computer merely removes the visible pointer to the electronic data; it does not actually delete the data itself. Only when the space formerly occupied by a "deleted" document is reused is the document truly erased.

The ever-increasing capacity to store all this data further facilitates the data propagation. Whereas a few thousand pages of paper documents fill a standard filing cabinet drawer, millions of printed pages can occupy a single computer tape or disk drive. Organizations—both private and public—easily accumulate stacks of disks and tapes filled with countless documents as they transition to a "paperless environment," thus increasing the volume of information within their possession, custody, or control.

Dispersion

Because of the ease of replication and distribution of electronic information, multiple copies and iterations of documents may exist in a variety of places (some unexpected), such as on an entity's computer networks, CDs, DVDs, external drives, laptops, e-mail systems, personal digital assistants (PDAs), MP3 players, and within an entity's archival or backup systems. In order to search and retrieve data, an entity must first know all the places that the data resides. With paper documents there typically are limited storage repositories. Electronic data, on the other hand, may reside virtually anywhere. The dispersion of this data makes it much harder to manage electronic information.

9. "It is estimated that in 2007 the amount of [electronic] information created and replicated globally surpassed 255 exabytes." An *exabyte* is a unit of information or computer storage equal to one quintillion (1000^6) bytes. *See* George L. Paul & Jason R. Baron, *Information Inflation: Can the Legal System Adapt?*, 13 Rich. J.L. & Tech. 10 (2007).

Dynamic Content

Electronic data often encompasses dynamic, changeable content. Unlike paper documents, it is not readily fixed in a truly final form. And, the changes to electronic information often may be difficult to detect without computer forensics techniques. The ease of transmitting electronic information and the routine modification of it, at times by multiple users at once (such as through shared files and wikis[10]), may obscure the origin, completeness, or accuracy of the data. It also makes it harder for an entity to preserve and ensure the integrity of data that is actively being used within an organization.

Obsolescence

Electronic data also exists in many more forms than paper documents—some of which only may be visible or extractable using specific applications or programs. Applications and programs routinely become obsolete within relatively short time periods. The data generated through these applications and programs, however, may continue to exist indefinitely, due in part to the ease of its dispersion and storage.

Metadata

Another significant difference between electronic information and paper documents is that most electronic data contains information that is not readily apparent to the creator or user of the data—usually known as metadata. *Metadata* is information describing the history, tracking, or management of an electronic document. It also includes information about the document or file that is recorded by the computer to assist in storing and retrieving the document or file. Examples of metadata include a file's designation, dates it was created or modified, its author, and its edit history. Metadata often also serves a valuable function in aiding the searchability of electronic information. "For example, system metadata may allow for the quick and efficient sorting of a multitude of files by virtue of the dates or other information captured in metadata. In addition, application metadata may be critical to allow the functioning of routines within the file, such as cell formulae in spreadsheets."[11] The different types of metadata have different degrees of accuracy and essentiality to the underlying data. Some metadata, such as who authored a document and when and what changes were made to the information, is often not essential to viewing or understanding the information within an electronic document. Other metadata, such as a hidden formula that generates information in a spreadsheet or a programmed field that underlies the information in a database, is inextricably linked with the visible data. That is, the visible data is difficult, if not impossible, to understand separated from its metadata. Other than the possible presence of a watermark, paper documents typically have no comparable component to metadata.

---

10. A *wiki* is a "collaborative website that allows visitors to add, remove, and edit content." *The Sedona Conference Glossary: E-Discovery & Digital Information Management*, (2d ed. The Sedona Conference Dec. 2007).

11. *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production* (2d ed. June 2007), *available at* www.thesedonaconference.org/publications_html (last visited Feb. 21, 2009). *See generally* Craig Bell, *Understanding Metadata: Knowing Metadata's Different Forms and Evidentiary Significance Is Now an Essential Skill for Litigators*, 13 Law Tech. Prod. News 36 (Jan. 2006).

Searchability

A final and significant difference between electronic information and paper documents is that electronic information often is searchable through automated processes. The ability to cull through massive amounts of data with just a few key strokes often provides significant efficiencies and economies in searching and retrieving electronic information.

How Do These Differences Affect Discovery?

How do the differences between electronic information and paper documents affect the civil discovery process? As discussed in sections 2 and 3 of this guide, for the most part, the differences do not alter a litigant's basic obligations under the discovery rules. There is little doubt, however, that the costs associated with e-discovery often dwarf those incurred in traditional discovery (that is, discovery of paper documents and tangible items only). There are three sources of the additional costs and burdens that are specific to e-discovery. First, there is more information that resides in more places, some of which is hidden or otherwise difficult to retrieve. It is not surprising that as the amount of information generated and stored, through increasingly complex methods, has increased, so too have the costs and burdens of searching for and retrieving potentially relevant information from amongst all that data during a civil discovery process. Second, and closely related, e-discovery creates more areas of potential dispute among litigants, which inevitably leads to more litigation. A leading commentator on electronic discovery and educator at the Federal Judicial Center posited in 2005 that "[m]ore money is probably spent litigating electronic discovery problems than in litigating class actions."[12] Third, and perhaps most importantly, the intricacies of electronic data create greater dangers of spoliation of evidence. Spoliation "refers to the destruction or material alteration of evidence or to the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation."[13] Although the costs and burdens of complying with e-discovery obligations are often high, they pale in comparison to the potential consequences of failing to comply, or spoliating evidence. The right to impose sanctions for spoliation in the civil context arises both from the discovery rules and from a court's inherent power to control the judicial process and litigation. Spoliation sanctions may vary from imposing monetary penalties to dismissing the spoliator's claims or entering judgment against the spoliator—all of which impose additional costs and burdens on the spoliating party.

The amount and extent of the costs and burdens varies significantly, based on the nature of the litigation and the litigants, but both private and public sector entities need to be mindful that, in many cases, these additional costs and burdens are a reality of the digital age.

---

12. Ameet Sachdev, *E-mails become trial for courts: Costly electronic discovery 'part of potentially every case in the 21st Century,'* Chicago Tribune Online Edition, April 10, 2005, www.rpost.com/partners/pdf/ChicagoTribune_April10_1005_Emails_becomes_trial_for_courts.pdf.

13. Silvestri v. General Motors Corp., 271 F.3d 583, 590 (4th Cir. 2001).

Section 2: What Is the Process for E-Discovery?

What Electronic Information Is Discoverable?

Generally, a party to litigation in both federal and state courts is required to produce, on request, all documents and tangible things that are within the party's possession, custody, or control and that are relevant to the dispute.[14] This includes documents and tangible items within the physical possession or custody of the party; it also includes other information within the possession or custody of the party's employees and contractors, or even other third parties, that is still legally, or even practically, within the control of the party.[15]

The scope of the discovery obligation with respect to documents and tangible items is broad. How, though, does it apply to electronic information? Are there any limits to what electronic data must be preserved and produced?

Federal Rules of Civil Procedure

Electronically stored information. Before adoption of the 2006 amendments, FRCP 34, which authorizes the discovery of documents in federal courts, defined "document" to include compilations of data. Federal courts interpreted this provision to authorize the discovery of digital information.[16] Some litigators were concerned that data compilations did not encompass all electronically generated information, particularly information created through automatic computer processes without any human interaction.[17] In response the 2006 amendments authorized the discovery of *electronically stored information* (ESI). ESI is defined to include "writings, drawings,

---

14. At least theoretically, the scope of what must be produced is different in federal court proceedings than in state court proceedings in North Carolina. Under the FRCP a party must produce all documents and tangible things that are relevant to the claims or defenses of any party. Additionally, the FRCP require initial disclosure, without awaiting a discovery request, of a copy of or a description by category and location of all documents and tangible items in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses. Under the NCRCP a party must produce all documents and tangible things that are relevant to the subject matter involved in the pending action.

15. A discussion of what constitutes "possession, custody or control" of electronic information is beyond the scope of this guide. Litigants should be mindful, however, that the contours of the obligation may extend beyond information that is stored within an entity's information system. Additionally, under certain circumstances, entities and individuals that are not parties to the litigation may be compelled to produce documents and tangible items that are relevant to the issues at stake in the litigation. *See* Fed. R. Civ. P. 45; N.C. Gen. Stat. (hereinafter G.S.) § 1A-1, Rule 45.

16. *See, e.g.*, Linnen v. A.H. Robbins Co., 1999 WL 462015 (Mass. Super. Ct. June 16, 1999) ("While the reality of [electronic discovery] may require a different approach and more sophisticated equipment than a photocopier, there is nothing about the technological aspects involved which renders documents stored in an electronic media 'undiscoverable.'").

17. *See The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production* (2d ed. June 207), *available at* www.thesedonaconference.org/publications_html (last visited Feb. 21, 2009). Note that the term "data compilations" was not specifically defined in the FRCP. The committee notes to the 1970 amendment that added the term to the definition of discoverable documents under Rule 34 states that "Rule 34 applies to electronics data compilations from which information can be obtained only with the use of detection devices, and that when the data can as a practical matter be made usable by the discovering party only through respondent's devices, respondent may be required to use his devices to translate the data into usable form." And, the 1972 proposed rules advisory committee note to Federal Rule of Evidence (FRE) 803(6) explained that "the expression 'data compilation' is used as broadly descriptive of any means of storing information other than the conventional words and figures in written or documentary form. It includes, but is by no means limited to, electronic computer storage. The term is

graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained . . . ." According to the committee note to FRCP 34, the definition of ESI is "intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments." This definition allows discovery obligations to adjust to new technologies and, at least in theory, prevents litigants from evading discovery obligations by claiming that the definition of document does not keep pace with the technological changes.

Ephemeral data. But is the definition, in fact, broad enough to encompass all types of electronically generated information? The manner in which entities generate and disseminate information is rapidly evolving. Communication is not limited to e-mail; both private and public organizations increasingly are relying on so-called Web 2.0 technologies,[18] such as instant messaging (IM),[19] Twitter,[20] and social networking sites,[21] to communicate internally and externally. Web 2.0 technologies add to the number of data sources and total volume of information generated within an organization. The information is often ephemeral in nature, though. Ephemeral data is information that is not "stored for any length of time beyond [its] operational use and . . . [that is] susceptible to being overwritten at any point during the routine operation of the information system."[22] Although ephemeral ESI can take many forms, common types include information contained in random access memory (RAM),[23] such as information generated by Web 2.0 technologies, and cache files.[24]

Is ephemeral information discoverable? To date there are few cases that test the boundaries of discoverable ESI. Of the few courts to address this issue most have found no duty to preserve or produce ephemeral data, at least in part because the information is not stored in the traditional sense.[25] Recall that the committee notes to FRCP 34 state that "Rule 34 applies to information

---

borrowed from revised Rule 34(a) of the Rules of Civil Procedure." Rule 34 provided limited guidance, however, with respect to when data compilations or other types of electronic documents had to be produced and in what form.

18. Web 2.0 "refers to a perceived second generation of web development and design, that facilitates communication, secure information sharing, interoperability, and collaboration on the World Wide Web." *See* Wikipedia.com, Web 2.0, http://en.wikipedia.org/wiki/Web_2.0 (last visited May 4, 2009, 10:55 GMT).

19. Instant messaging (IM) is a form of real-time, text-based communication between two or more participants over some form of network, intranet or internet.

20. Twitter is a micro-blogging social networking service that allows a user to post text-based messages, known as tweets, of up to 140 characters on the user's profile page to be viewed by other users who have subscribed to "follow" the user that posted the message.

21. Common social networking sites as of this writing include Facebook and MySpace. For a list of other social networking sites, see Wikipedia.com, List of Social Networking Sites, http://en.wikipedia.org/wiki/List_of_social_networking_websites (last visited May 4, 2009, 11:35 GMT).

22. Kenneth J. Withers, *"Ephemeral Data" and the Duty to Preserve Discoverable Electronically Stored Information*, 37 U. Balt. L. Rev. 349, 366 (2008).

23. Random access memory (RAM) is a computer's "temporary" memory in which information is contained while it is in use, rather than on the hard drive, enabling software to operate faster. The contents of RAM may change as frequently as by the second.

24. Each time a Web page is accessed, the computer creates a cache file (a temporary copy) of that page's text and graphics. If the Web page is opened again, the Web browser checks the website server for changes to the page. If the page has changed, the browser retrieves a new version over the network. If the page has not changed, the browser uses the cache files from the computer's RAM or hard drive to display the page. A cache file, thus, facilitates retrieval of previously viewed Web pages.

25. *See, e.g.*, Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey, 497 F. Supp. 2d 627 (E.D. Pa. 2007) (rejecting sanctions on defendant for failure to preserve temporary cache files of archived Web pages accessed through a third-party, public website); Malletier v. Dooney & Bourke, Inc., 2006 WL 3851151 (S.D.N.Y. Dec. 22, 2006) (rejecting sanctions for failure to preserve purportedly relevant chat room conversations with customers on its website where the defendant did not have a means to preserve the transitory online discussions and it was unlikely the conversations

that is fixed in a tangible form and to information that is *stored* in a medium from which it can be retrieved and examined." At least one court, however, has reached the opposite conclusion—holding that ephemeral data is discoverable. In *Columbia Pictures, Inc. v. Bunnell*,[26] a federal district court in California held that data stored in RAM, however temporarily, is ESI subject to discovery under FRCP 34. Although the facts giving rise to the case are fairly unique—the case involved a claim against defendants for knowingly enabling, encouraging, inducing, and profiting from massive online piracy of the plaintiffs' copyrighted works through the operation of their websites—the conclusion that information stored only in RAM may be discoverable in at least some circumstances could lead to tricky preservation decisions by litigants or potential litigants. Arguably, however, the *Bunnell* court did not require production of information contained only in RAM. The producing party had intentionally disabled a logging function in its Web server program so that the data existed only temporarily in its computers as RAM. The court required the producing party to enable the logging function, thereby creating ESI. Thus, what actually makes the *Bunnell* decision exceptional is that the court ordered a party to record information that would not otherwise have been recorded (thus, creating information) and then produce that information.[27] This area of law is still developing, but organizations that employ novel communication and information sharing methods must decide whether the electronic information should be captured and stored and how its decision may impact any future litigation.[28]

"Informal" communications. An equally tricky issue is the discoverability of electronic information that individuals and entities treat as ephemeral but that is, in fact, not.[29] In a recent case involving the City of Detroit, the United States District Court for the Eastern District of Michigan held that the plaintiff was entitled to pursue the production of certain text messages sent or received by specified elected officials and employees of the city.[30] The case arose after a woman was murdered in a drive-by shooting. A complaint was filed on behalf of the woman's minor son, alleging that the city and certain named officials did very little to investigate the crime because of the potential for political scandal. Among other discovery requests, the plaintiff sought production of text messages the defendants sent among themselves over a five-year period on city-issued text-messaging devices. The city had contracted with a service provider to provide text-messaging services to the various city officials and employees, and the service provider maintained copies of at least some of the text messages sent and received during the relevant period. The city opposed the request, arguing that the federal Stored Communications Act[31] protected the messages from

---

would have provided relevant evidence); Convolve, Inc. v. Compaq Computer Corp., 223 F.R.D. 162 (S.D.N.Y. 2004) (rejecting sanctions for defendant's failure to preserve data readings on an electronic device used to tune computer hard drives, where the data collected from the device were routinely written-over when the next measurement was taken).

26. 245 F.R.D. 443 (C.D. Cal. 2007).

27. *See cf.* O'Brien v. O'Brien, 899 So. 2d 1133 (Fla. App. 2005) (determining that information on RAM is not "stored" for purposes of the discovery rules).

For a good discussion of the issues relating to ephemeral data and the potential discovery obligations see Kenneth J. Withers, *"Ephemeral Data" and the Duty to Preserve Discoverable Electronically Stored Information*, 37 U. Balt. L. Rev. 349, 366 (2008) (suggesting that courts should consider four factors in deciding whether ephemeral data should be preserved: (1) whether the data are uniquely relevant to the litigation, (2) how the data are ordinarily treated by the party "in the ordinary course of business," (3) whether preservation imposes excessive costs or burdens relative to the value of the data, and (4) whether technologies exist to preserve the data).

28. As discussed in section 4 of this guide, public sector entities also may have a statutory duty to store certain information.

29. Note that some information generated by Web 2.0 technologies may fall into this category.

30. Flagg v. City of Detroit, 252 F.R.D. 346 (E.D. Mich. 2008).

31. 18 U.S.C. § 2701 *et seq*.

disclosure because the act prohibits those who provide "an electronic communication service to the public" from knowingly disclosing the contents of a communication while in electronic storage by that service. The court rejected that argument, concluding that the relevant text messages were actually within the possession, custody, or control of the city and thus discoverable.[32] The city further argued that many of the text messages sought by the plaintiff were private or personal and thus not relevant and not discoverable.[33] The court rejected this argument in so far as it would lead to a blanket prohibition against discovery. Instead, the court sanctioned a search protocol which required two magistrate judges to review the text messages *in camera* to determine relevancy and then afforded the defendants an opportunity to raise objections to individual messages. This case highlights the challenges posed by organizations using increasingly less formal modes of communication, often across information systems that mix personal information with business or government communications.[34] Organizations, their employees, and their officials must understand that if a litigant has possession, custody, or control[35] over information that is relevant to a dispute it may be discoverable regardless of its form or format or the intention of the individuals who generated or captured the information.[36]

North Carolina Rules of Civil Procedure

Data compilations. The current NCRCP 34 defines document to include "data compilations." North Carolina courts have interpreted this term to include electronic information.[37] It is unclear what, if any, difference there is between the definition of data compilations and ESI, as defined under the federal rules. To date there are not many written opinions addressing the discovery of electronic information in North Carolina's state courts. In one of the few written, albeit unreported, opinions, a North Carolina superior court analyzed the various approaches to dealing with e-discovery and determined that North Carolina state courts "will look to the North Carolina Rules of Civil Procedure for guidance in deciding e-discovery issues and amend those rules as necessary. In applying the Rules, the courts will most likely use the [*Conference of Chief Justices Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information*

---

32. The court did not reach the issue of whether disclosure of the text messages would have violated the act.

33. The city cited *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir. 2008), in which the Ninth Circuit held that a city employee had a reasonable expectation of privacy in the text messages the employee sent over a city-issued pager, pursuant to the city's text-messaging policy. The court held that *Quon* was not applicable to the facts of this case.

34. *See generally* Arteria Property Ltd. v. Universal Funding V.T.O., Inc., 2008 WL 4513696 (D. N.J. Oct. 1, 2008) (holding that there is no reason to treat information posted to a website different than other electronic information for purposes of discovery and imposing sanctions against a party for destroying a website with relevant information after the duty to preserve was triggered).

35. *See* note 15, *supra*, and accompanying text.

36. For a discussion of what information must be preserved by public entities, pursuant to statutory retention requirements, see Section 4.

37. *See, e.g.*, Arndt v. First Union Nat'l Bank, 170 N.C. App. 518, 613 S.E.2d 274 (2005) (holding that trial court did not error in giving spoliation instruction where defendant failed to preserve certain e-mails and profit and loss statements); Commissioner v. Ward, 158 N.C. App. 312, 580 S.E.2d 432 (2003) (affirming trial court's sanctions of party that refused to comply with multiple consent orders involving the examining, inspection, and copying of certain electronic information); Analog Devices, Inc. v. Michalski, 2006 WL 3287382 (N.C. Super. Ct. Nov. 1, 2006) (applying Rule 26 factors to analyze a claim that producing the requested electronic information posed an undue burden or cost and ordering production of the information because of the significant potential for discovery of probative evidence); Bank of Amer. Corp. v. SR Int'l Bus. Ins. Co., Ltd., 2006 WL 3093174 (N.C. Super. Ct. Nov. 1, 2006) (applying Rule 26 factors to analyze a claim by a nonparty that producing the requested electronic information posed an undue burden or cost and holding that the nonparty need not produce the information because the low marginal utility did not justify imposing a heavy burden on a nonparty).

(*Chief Justices' Guidelines*)] . . . ."[38] The *Chief Justices' Guidelines*' definition of discoverable electronic data mirrors that of the federal rules. Thus if other North Carolina courts follow this guidance, there may be no practical difference between what electronic information is discoverable in federal and state courts in this state. (For ease of exposition, both electronically stored information and data compilations will be referred to as ESI.)

How Is ESI Discoverable?

Preserving Potentially Relevant ESI

In order to satisfy its production obligation under both the federal and state rules, a litigant (or potential litigant) is under a common law duty to preserve all potentially relevant documents for possible production once it reasonably anticipates litigation—defined as the point when an entity has actual or constructive knowledge of the likelihood of future litigation ("trigger date").[39] When the duty to preserve is triggered is highly dependent on the facts and circumstances of each case.[40] In most cases the trigger date coincides with the commencement of the litigation. Yet it may occur earlier under certain circumstances, such as when a potential litigant makes a credible threat of filing suit or when a dispute appears to be irreconcilable without resorting to the judicial system.

For example, in a personnel matter the trigger date may arise as early as when an employee reports potentially actionable conduct to a supervisor. On the other hand, the trigger date likely does not arise every time an individual expresses discontent at a public meeting or hearing. The duty to preserve is not triggered by the mere possibility of litigation.[41]

Once the duty to preserve is triggered, an entity "must retain all relevant documents (but not multiple identical copies) in existence at the time [the duty to preserve commences] and any relevant documents created thereafter."[42] This is commonly referred to as a "litigation hold." Pursuant to a litigation hold any previously generated potentially relevant documents must be preserved as they existed on the trigger date. Thus, in order to preserve data that is actively being used, an entity may be required to make a duplicate copy of all sources of potentially relevant information. It also may be obligated to suspend any routine document destruction processes.

Failure to preserve potentially relevant information, including ESI, in and of itself, may result in the imposition of sanctions, even if the actual relevance of the information to the dispute is never proven. In *ACORN v. County of Nassau*,[43] for example, The United States District Court for the Eastern District of New York sanctioned the defendant-county for failing to implement a proper litigation hold until after its motion to dismiss the action was denied. The county attorney had orally communicated the requirement to preserve relevant information to the various depart-

---

38. *Analog Devices*, 2006 WL 3287382 at *12 (N.C. Super. Ct. Nov. 1, 2006).

39. *See* Teague v. Target Corp., 2007 WL 1041191 (W.D.N.C. Apr. 4, 2007) ("The Fourth Circuit states that the duty extends to that period prior to litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation.") (internal quotations omitted).

40. For a good discussion of the duty to preserve and when it is triggered, see *Zubulake v. UBS Warburg*, LLC, 220 F.R.D. 212 (S.D.N.Y. 2003).

41. *See* Toussie v. County of Suffolk, 2007 WL 4565160 (E.D.N.Y. Dec. 21, 2007) ("At times, the duty to preserve arises prior to the filing of a complaint; at the point in time when a defendant first anticipates litigation. But when the defendant is a firm, or, as here, a municipality, a firm or municipal-wide duty to preserve is not imposed simply because one or two employees contemplate the possibility of litigation.").

42. *Zubulake*, 220 F.R.D. 212 (S.D.N.Y. 2003); *see also* Doe v. Norwalk Cmty. Coll., 2007 WL 2066496 (D. Conn. July 16, 2007) (noting that a party needs to act affirmatively to prevent its system from routinely destroying information).

43. 2009 WL 605859 (E.D.N.Y. March 9, 2009).

ments that were affected by the litigation when the complaint was filed, but the attorney did not direct its information technology (IT) personnel to suspend the routine destruction of e-mails and other electronic data, stating that "such a direction would be 'impossible . . . because to do so would entail putting a halt to the entire Countywide [Information Technology] policy of re-using electronic tapes to store data.'" There also was no indication that the county attorney followed up with the departments to ensure that relevant documents actually were being retained, which the court found amounted to gross negligence. The court imposed sanctions on the county, even though there was no indication that the lost information would have provided any additional support to the plaintiff's claims.[44]

The Duty to Preserve, Search, and Retrieve ESI

Who within an organization actually is responsible for preserving and producing the electronic data? The obligation ultimately runs to the entity involved in the suit to ensure compliance with discovery requirements.[45] In the public sector the entity is the city, county, or other government agency or authority. A litigant's counsel, however, often directs and coordinates the discovery process. Specifically, counsel is responsible for informing all relevant personnel within the organization when the duty to preserve arises and what information must be preserved. Counsel must also make reasonable, good faith efforts to ensure compliance with preservation and production requirements.[46] In order to fulfill its obligation, counsel must have reasonable knowledge of its client's information management policies and actual practices.[47] Counsel also must work with an entity's IT professionals and take an active role in the preservation, search, and retrieval process or face potential sanctions from the court for failure to fulfill its duties under the rules. And note that the duty extends to both in-house and outside counsel.[48] In *Phoenix Four, Inc. v. Strategic Resources Corp.*,[49] the United States District Court for the Southern District of New York sanctioned a party and its attorneys when it was discovered that relevant data residing on a partitioned section of the party's computer server had not been located or produced. At a discovery hearing the attorneys informed the court that they had communicated a litigation hold to the party and were assured that all electronic and paper documents had been located and preserved. The attorneys had not, themselves, undertaken a methodical search of the party's information system or followed up with the party about the scope of the party's search. The court found the attorneys' conduct to be deficient and criticized the counsel for failing to interrogate the client fully regarding its information system, concluding that "counsel's obligation is not confined to a

---

44. Note that the sanctions imposed by the court were not as harsh as they likely would have been had the plaintiff been able to demonstrate that the lost information was relevant to the dispute.

45. *Zubulake*, 229 F.R.D. 422 (S.D.N.Y. 2004) ("At the end of the day, [ ] the duty to preserve and produce documents rests on the party.").

46. *See, e.g.*, Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc., 244 F.R.D. 614 (D. Colo. 2007) ("[C]ounsel cannot turn a blind eye to a procedure that he or she should realize will adversely impact [the search for relevant information].").

47. It is particularly important for counsel to understand the actual practices of an organization's employees and officials with respect to data management, which may not adhere to the organization's official policies.

48. Even if an entity relies on outside counsel to handle litigation matters, in-house counsel often play an important role in ensuring that data is preserved once the litigation is reasonably foreseeable. Relevant evidence may be spoliated if an entity awaits direction from outside counsel on its preservation obligations.

49. 2006 WL 1409413 (S.D.N.Y. May 23, 2006); *see also* Qualcomm, Inc. v. Broadcom Corp., 2008 WL 66932 (S.D. Cal. Jan. 7, 2008) (concluding that lawyers "did not make a reasonable inquiry into Qualcomm's discovery search and production and their conduct contributed to the discovery violation" and imposing sanctions); Linnen v. A.H. Robins Co., 1999 WL 462015 (Mass. Super. Ct. June 16, 1999) (sanctioning party because its counsel failed to completely investigate stored computer backup tapes while representing to the court that all relevant computer files had been produced).

request for documents; the duty is to search for sources of information."[50] This is just one example of a growing body of case law admonishing and sanctioning parties and their attorneys for not conducting an appropriate search of their electronic information during the civil discovery process. What steps a party and its counsel must take to ensure proper preservation and production of relevant information, however, will vary based on the nature of the litigation and the type and *sources* of electronic information.[51]

The Form of Production for ESI

Once all relevant information is identified and retrieved, in what form may (or must) it be produced? A common dispute among parties to litigation relates to whether ESI must be produced in its native format (the format in which it was created) or whether it can be converted to another electronic format or printed to hard copy before being produced. A requesting party typically wants electronic data produced in a form that is readable, easy to search, and inclusive of all relevant contextual information. Because a requesting party does not always have full information about another party's information system, however, its requests may not be sufficiently targeted to solicit the information in the desired form. A producing party, on the other hand, generally wants to produce electronic information in a form that limits production costs and burdens and also preserves the integrity of the data and makes it easy to track.

Federal Rules of Civil Procedure. The 2006 amendments do not mandate a specific form for production of ESI. Instead, FRCP 26(f) encourages parties to discuss any issues relating to the form or forms in which it should be produced during the mandatory pretrial meeting (discussed below).[52] A party may stipulate a specific form or forms for the production of ESI in its written FRCP 34 request.[53] The rule recognizes that different forms may be required for different types of ESI and expressly authorizes a party to request different information in different forms. A party does not need to produce identical ESI in more than one form, though.

Objections to Requested Form. The producing party may object to the requested form or forms of electronic information in its written response to the FRCP 34 request. If the producing party objects, or if no form is specified in the FRCP 34 request, the responding party must state the form or forms it intends to use in its written response to the document request. The responding party is obliged to produce the ESI in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable.[54] By definition, ESI is maintained in electronic form, thus the producing party likely does not satisfy the FRCP 34 requirement by preparing the electronic information as printed hard copies.[55] But the form in which ESI is ordinarily maintained does

---

50. *Phoenix Four*, 2006 WL 1409413 at *5.

51. *See, e.g.*, ACORN v. County of Nassau, 2009 WL 605859 (E.D.N.Y. Mar. 9, 2009) (noting that if a party is unable to perform an automated systemwide search for electronic information, an individual electronic search of each potential repository of data (*e.g.*, each computer) likely satisfies a party's discovery obligations). For a helpful discovery checklist to assist counsel in identifying the existence and location of potentially relevant electronically stored information (ESI), see Hon. Shira A. Scheindlin & Jonathan M. Redgrave, *Ch. 22: Discovery of Electronic Information*, *in* Business and Commercial Litigation in Federal Courts (Robert L. Haig ed., 2d ed., rev. ed. 2008).

52. *See* Covad v. Revonet, 254 F.R.D. 147 (D. D.C. 2008) (stating that "[t]he rules now require the parties to confer about the format of production and to specify how a party is to produce electronically stored information").

53. The requesting party may specify hard copies of the ESI as the requested form.

54. *See* PSEG Power New York, Inc. v Alberici Constructors, Inc., 2007 WL 2687670 (N.D.N.Y. Sept. 7, 2007) (holding that the production of e-mails separated from their attachments did not comply with Rule 34's requirement that electronic information be produced as it is kept in the usual course of business or in a reasonably usable form).

55. *See Covad*, 254 F.R.D. 147 (D. D.C. 2008) (noting that a party that converts electronic data to hard copy may be forced to also produce the information in electronic format).

not necessarily require that it be produced in the form in which it was created. If, for example, an entity generated information using a word-processing software, such as Microsoft Word, but ordinarily maintains that information only in portable document format (PDF) or tagged image file format (TIFF) format, it likely can produce the information in the PDF or TIFF format. If, however, the responding party does not produce the ESI in the form in which it is ordinarily maintained, it may not convert it to a different form that makes it more difficult or burdensome for the requesting party to use the information efficiently. According to the committee notes to FRCP 34, "[I]f the responding party ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, the information should not be produced in a form that removes or significantly degrades this feature."[56]

If the requesting party is not satisfied with the form or forms in which the producing party intends to produce the electronic information, FRCP 37(a) requires the parties to attempt to resolve the matter before the requesting party may file a motion to compel production in its preferred form or forms. If a court ultimately must resolve the dispute, it may require the production of ESI in any form, regardless of the form or forms specified by either party.

Metadata. The issue of what form or forms electronic information must be produced is further complicated by the existence of metadata. As discussed above, metadata is the data underlying the electronic information and exists in many different forms to serve a variety of purposes. There are three purposes, in particular, for which a party to litigation may wish to view the metadata associated with an electronic document. First, a party may desire to know who altered an electronic document when and what changes were made. Although probably the most familiar use of metadata, this information is actually relevant in only a small percentage of legal disputes. Further, this type of metadata is often easily manipulated, even unintentionally, and may be unreliable. Second, a party may need to view the metadata underlying the electronic information in order to fully understand the visible data, such as hidden formulas in spreadsheet applications. This metadata actually may be essential to interpreting the underlying information. Third, a party may need certain metadata in order to effectively perform automated searches of electronic information. In general, search queries using metadata can save users from performing more complex filter operations manually.[57]

The 2006 amendments do not specify whether, and under what circumstances, a party is obligated to produce the metadata associated with ESI. FRCP 26 emphasizes the need of the parties to discuss the form or forms of production, including any issues relating to metadata, and resolve any differences without court intervention. In the event that parties do not agree, as stated above, the producing party has the option to produce the ESI either as it is ordinarily maintained or in a form or forms that are reasonably usable.

To date courts have articulated conflicting views over whether the default production forms include metadata.[58] In *Williams v. Sprint/United Management Co.*,[59] the United States District Court for the District of Kansas held that "[b]ased on [] emerging standards, . . . when a party is

---

56. *See, e.g., In re* Classicstar Mare Lease Litig., 2009 WL 260954 (E.D. Ky. Feb. 2, 2009) (requiring defendant to reproduce documents in native format even though the information had previously been produced in TIFF format after plaintiffs successfully argued that the data was much more usable in its native format because it was complex information and extremely reliant on the reporting features within the native software).

57. Under certain circumstances, metadata also may aid in determining the admissibility of ESI. *See, e.g.*, Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534 (D. Md. 2007).

58. Removal of metadata usually requires an affirmative alteration of the ESI—through scrubbing the document or converting the file from its native format.

59. 230 F.R.D. 640 (D. Kan. 2005).

ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to the production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order." Alternatively, in *Wyeth v. Impax Laboratories, Inc.*,[60] the United States District Court for the District of Delaware held that "[e]merging standards of electronic discovery appear to articulate a general presumption against the production of metadata."[61] The differing views articulated by the courts in these two cases likely stemmed from the different nature of the metadata sought in each case. Significantly, *Williams* involved the production of spreadsheets—where the individual tables may have little meaning without access to the underlying formulas in each cell. As the court stated:

> [T]he more interactive the application, the more important the metadata is to understanding the application's output. At one end of the spectrum is a word processing application where the metadata is usually not critical to understanding the substance of the document. The information can be conveyed without the need for the metadata. At the other end of the spectrum is a database application where the database is a completely undifferentiated mass of tables of data. The metadata is the key to showing the relationships between the data; without such metadata, the tables of data would have little meaning.[62]

Whereas, in *Wyeth*, the court concluded that the metadata at issue, including information describing the history, tracking, or management of the electronic documents, was not uniquely relevant to the dispute. The *Wyeth* court left open the possibility that production of metadata may be required under certain circumstances and cautioned that a producing party always should preserve the integrity of the electronic information it produces, including its metadata.

The Sedona Conference Working Group on Electronic Document Retention and Production has published detailed guidance for litigants in interpreting the 2006 amendments and addressing the myriad of issues surrounding the preservation and production of ESI. According to "Principle 12" in its 2007 publication, *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production*:

> Absent party agreement or court order specifying the form or forms of production, production should be made in the form or forms in which the information is ordinarily maintained or in a reasonably usable form, taking into account the need to produce reasonably accessible metadata that will enable the receiving party to have the same ability to access, search, and display the information as the producing party where appropriate or necessary in light of the nature of the information and the needs of the case.[63]

---

60. 248 F.R.D. 169 (D. Del. 2006).

61. The court was following the Default Standard for Discovery of Electronic Documents adopted by local rule in that district which directs parties to produce electronic documents as image files if they cannot agree on a different form for production. *See* Ad Hoc Comm. for Elec. Discovery, U.S. Dist. Court of the Dist. of Delaware, Default Standard for Discovery of Electronic Documents, *available at* www.ded.uscourts.gov/Announce/Policies/Policy01.htm (last visited Feb. 9, 2009).

62. 230 F.R.D. at 647 (D. Kan. 2005).

63. *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production* (2d ed. June 2007), *available at* www.thesedonaconference.org/publications_html (last visited Feb. 21, 2009).

Thus a party should consider the particular type of ESI and its searchability features when determining whether or not the production of metadata is necessary.[64] Beyond that, absent specific local rules in individual districts, the requirements in any given case will vary based on the needs of the requesting party and types of ESI and metadata involved.[65]

North Carolina Rules of Civil Procedure. The North Carolina rules, specifically NCRCP 34, allow a party to request from any other party the production of "documents (including writings, drawings, graphs, charts, photographs, phono-records, and other *data compilations* from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form."[66] The rules do not prescribe a specific form or forms for the production of data compilations. The requesting party should attempt to glean as much information as possible about where and in what form or forms potentially relevant electronic information may reside in the producing party's information system and should tailor its requests accordingly.

Objections to Requested Form. The producing party must respond in writing to any request for the discovery of ESI and state any objections, which presumably include objections to the type or form of requested ESI. If the parties fail to agree on the form or forms of production, the requesting party may move for an order to compel production under NCRCP 37(a). According to the *Chief Justices' Guidelines*, in the absence of agreement among the parties, a court should require that electronic information be produced in the form in which it is ordinarily maintained or in a form that is reasonably usable. Producing the information in a reasonably useable form probably requires that any searchability features not be significantly degraded, thus necessitating the production of at least some metadata. Whether other types of metadata must be produced likely will depend on the facts and circumstances of the case.[67]

---

64. *See In re* Payment Card Interchange Fee & Merch. Discount, 2007 WL 121426 (E.D.N.Y. Jan. 12, 2007) (stating that defendants had "run afoul of the Advisory Committee's proviso that data ordinarily kept in electronically searchable form should not be produced in a form that removes or significantly degrades this feature" where defendants had stripped text-searchable electronic documents of metadata that would not appear in printed form and then converted them back into text searchable electronic documents without that subset of metadata).

65. Note that Proposed 2009 Ethics Opinion 1 of the North Carolina State Bar (Jan. 22, 2009) "rules that a lawyer must use reasonable care to prevent the disclosure of confidential client information hidden in metadata when transmitting an electronic communication and a lawyer who receives an electronic communication from another party or another party's lawyer must refrain from searching for and using confidential information found in the metadata embedded in the document." The opinion, however, specifically exempts the disclosure and searching of metadata pursuant to legal obligation, court order or procedure, or the consent of the other lawyer or party. A copy of the proposed ethics opinion is available at www.ncbar.gov/ethics/propeth.asp (last visited March 20, 2009).

66. A party may also request to inspect or copy designated documents. G.S. 1A-1, Rule 34.

67. The proposed North Carolina amendments would modify the definition of document in Rules 26 and 34 to explicitly include electronically stored information.

Like the 2006 amendments to the federal rules, the proposed North Carolina amendments do not specify a form for the production of ESI. Instead, parties are encouraged to agree amongst themselves about what ESI must be preserved and the media, forms, and procedures for production. (Note that proposed new NCRCP 26(f) authorizes parties to conduct a discovery meeting and formulate a discovery plan that, among other things, specifies "the media, form, format, or procedures by which [ESI] will be produced . . . .") If the parties do not agree on a specific form, the requesting party may specify the form or forms in which the ESI is to be produced. If the producing party objects to a requested form, it must so state in its written response to the Rule 34 request. It also must state the form or forms in which it intends to provide the ESI. The party must produce the ESI in a reasonably usable form or forms. As under the federal rules a party need not produce identical ESI in more than one form.

If the requesting party is not satisfied with the form stated by the producing party, it may file a motion compelling production under new NCRCP 37. Unlike its federal counterpart, NCRCP 37 does not require the parties to attempt to resolve the matter before the requesting party may file the motion.

A potentially important difference between the federal rules and the proposed North Carolina amendments is that new NCRCP 26 would explicitly exempt metadata from the definition of ESI, unless the parties agree otherwise or

Section 3: What Are the Tools for E-Discovery?

Given the scope of the discovery obligation and the potentially significant burden of searching, retrieving, and producing all of the relevant electronic data, is there anything a litigant can do to limit costs? The 2006 amendments offer some guidance and potential relief to federal court litigants. Likewise, North Carolina's federal and state courts have attempted to provide litigants with some direction on walking the fine line between producing all relevant information to a dispute and limiting undue costs and burdens, but there are no magical solutions.

There are three areas in particular where a litigant's strategic employment of the federal and state discovery rules may serve to ameliorate at least some of the costs and burdens. A party may seek to leverage the requirements of several of the rules by fostering collaboration among adversaries with respect to the discovery phase of the litigation. A party also may exploit the rules' prohibition on imposing undue burdens on litigants to limit the amount of discoverable data, or to condition the discovery of the information on cost-sharing among the parties to the litigation. Each of these strategies will be discussed in turn.

Collaboration

A recurrent problem identified in e-discovery cases is that parties do not identify, discuss, and resolve issues related to the preservation and production of ESI early in the litigation process. Often a party does not have sufficient knowledge of its own or the other party's IT systems and the burdens and costs associated with preserving, searching, and producing electronic data until well into the litigation—after problems arise. The various volume, dispersion, formatting, readability, and searchability issues surrounding the discovery of ESI can lead to time-consuming and costly disputes.

One clear theme emerging from the 2006 amendments to the federal rules and various state rules, as well as from the case law, is that litigants are being highly encouraged, and in many cases forced, to collaborate and formulate mutually agreeable approaches to e-discovery. Litigation is, by definition, an adversarial process, and litigants have been slow to embrace the concept of collaboration, let alone adopt it as common practice. Judges, however, are increasingly touting communication, transparency, and mutual cooperation as the most effective means to contain overly broad and overly burdensome discovery obligations. Consequently, they are requiring counsel to work together to identify and fulfill legitimate discovery needs, while avoiding discovery that is too expensive or burdensome in relation to what is at stake in the litigation. Several of the federal rules provide specific guidance to litigants in undertaking this effort.

---

a court orders otherwise upon motion by a party and a showing of good cause. On its face excluding metadata from the definition of ESI appears to resolve an issue that the federal courts have struggled with in interpreting FRCP 34. Because metadata often performs an important function in aiding the searchability of ESI, however, failing to produce metadata in some cases may conflict with a party's obligation to produce the ESI in a reasonably usable form or forms. Recall that the committee notes to the federal amendments state that producing in a reasonably usable form means that the producing party should not remove or degrade the electronic search capability of ESI—which means that the producing party may be restrained from stripping ESI of all metadata. If the proposed North Carolina amendments are interpreted in the same way as the identical language in the federal rules has been interpreted, parties may be forced to produce metadata in some circumstances to preserve the searchability of the ESI.

In fact, a recent district court decision in *Mancia v. Mayflower Textile Services Co.*,[68] serves as an important reminder to litigants and their attorneys that the various federal rules actually mandate a cooperative approach to discovery and that failure to behave accordingly may result in sanctions. In *Mancia*, a discovery dispute arose from a collective action filed by a group of employees for payment of wages under the Fair Labor Standards Act and various state laws. And, in many respects, it was a garden variety discovery dispute—the plaintiffs served extensive discovery requests on the defendants and the defendants responded to a number of these requests with boilerplate objections. The court, however, expressed frustration with the litigants conducting business as usual. In fact, according to the court, both parties actually abused the discovery process by not sufficiently tailoring their discovery requests and, in response, not specifying the grounds for any objections to the requests, as required by the discovery rules. The court admonished that the rules require discovery requests, responses, and objections to be formed after a reasonable inquiry into the factual basis. By signing a discovery disclosure, request, response, or objection, the signatory swears that it is consistent with the rules, not for an improper purpose, not unreasonable, and not unduly burdensome or expensive. The court reminded counsel that the rules impose an affirmative duty to "behave responsibly during discovery, and to ensure that it is conducted in a way that is consistent 'with the spirit and purposes' of the discovery rules . . ." meaning that counsel should consider the cost and the burden of its discovery requests and offer a factual basis for objections. And, the court reminded counsel of its authority to impose sanctions on counsel for violating the rules without justification.

Although not as explicit as the federal rules, the NCRCP, likewise, support litigants in developing mutually agreeable solutions to the problems posed by e-discovery.

The following are four potential mechanisms by which the discovery rules may facilitate collaboration among parties to litigation to limit the costs and burdens commonly associated with e-discovery: (1) the development of discovery plans, (2) agreements on the form of production, (3) the adoption of tiered discovery processes, and (4) the use of clawback provisions to avoid waiver of inadvertently produced privileged or otherwise protected information.

Discovery Plans

Federal Rules of Civil Procedure. One of the most effective mechanisms to control discovery costs and limit disputes is for the parties to mutually develop a discovery plan early in the litigation process. The 2006 amendments require parties to discuss any issues relating to the discovery of ESI during the mandatory pretrial conference, commonly referred to as the "meet and confer."[69]

Pursuant to FRCP 26(f), parties must discuss the preservation of electronic information and develop a proposed discovery plan that, among other things, details any issues relating to the preservation and disclosure of ESI, including the form or forms in which it will be produced. In formulating the plan litigants should attempt to settle on the contours and parameters of each parties' search, preservation, and retrieval obligations in order to contain costs and avoid future disputes.

In order to effectively participate in the meet and confer, counsel must be prepared to discuss the contours of their parties' information systems and identify any potential problems with

68. 253 F.R.D. 354 (D. Md. 2008).

69. With a few exceptions, FRCP 26(f) requires parties to meet at least twenty-one days before a scheduling conference is held or scheduling order is due under FRCP 16. Increasingly, federal courts are interpreting Rule 26(f) as placing a requirement on parties to cooperate. *See, e.g.*, Sec. and Exch. Comm'n v. Collins & Aikman Corp., 2009 WL 94311 (S.D.N.Y. Jan. 13, 2009) (noting that courts view the discovery rules "as a mandate for counsel to act cooperatively") (internal quotations omitted). According to many leading commentators, the 2006 amendments to Rule 26 have impliedly removed the adversarial element from the meet and confer.

preserving and producing electronic information and its potential costs. As discussed above, to properly prepare for these discussions, counsel should make searching inquiries to determine all potential sources of a party's relevant electronic information and any unique costs and burdens of preserving or retrieving the data. Failure to anticipate unique problems and costs associated with the discovery of electronic information early in the process may result in even greater overall costs to a party.

After the FRCP 26(f) meet and confer, parties must submit the proposed discovery plan to the court. FRCP 16 requires the court to issue a scheduling order after receiving the parties' reports under FRCP 26(f) or after consulting with the parties' attorneys and any unrepresented parties at a scheduling conference or by telephone, mail, or other means. FRCP 16 does not require judges to address issues relating to the discovery of ESI in its scheduling order, but the 2006 amendments added "provisions for disclosure or discovery of electronically stored information" and "any agreements the parties reach for asserting claims of privilege or of protection as trial-preparation material after production" to the list of subjects that may be addressed in the order. The rule alerts courts as to the possible need to address ESI-related issues early in the litigation, but it leaves the burden on the parties to raise any relevant issues. A court is authorized under FRCP 16(f), however, to impose sanctions on a party or its attorney if either is substantially unprepared to participate, or does not participate in good faith, in the FRCP 16 conference. Thus parties should be prepared to discuss any e-discovery issues that may be raised by the court.

Courts are beginning to assume a more active role in the pretrial conference process. Several courts have modified their local rules to provide detailed guidance to litigants regarding the discovery of ESI.[70] Other courts have issued comprehensive discovery orders in individual cases. In *O'Bar v. Lowe's Home Centers, Inc.*,[71] the United States District Court for the Western District of North Carolina set forth detailed guidelines governing the discovery of ESI, including the anticipated scope of requests for, and objections to, the production of ESI, the form or forms for production, whether metadata would be requested for some or all ESI, the scope of preservation obligations relating to ESI, and the identification of any ESI that a party determined to be not reasonably accessible because of undue burden or cost.[72] According to the court, "[T]he purpose of the guidelines is to facilitate the just, speedy, and inexpensive conduct of discovery involving ESI in this case, and to promote, whenever possible, the resolution of disputes regarding the discovery of ESI without Court intervention."[73] The court further warned the litigants that "compliance with the guidelines may be considered by [it] in resolving discovery disputes, including whether sanctions should be awarded . . . ."[74]

North Carolina Rules of Civil Procedure. The NCRCP do not go as far as the federal rules in mandating a pretrial conference. Parties involved in state court litigation, though, clearly may discuss issues related to e-discovery and attempt to formulate mutually agreeable solutions. Further, under NCRCP 26(f), a court may direct the parties' attorneys to appear before it for a discovery

70. For example, effective January 1, 2008, the United States District Court for the Western District of North Carolina amended Local Rule 16.1 to specify appropriate topics for consideration at the initial pretrial conference, including the production of ESI. A copy of the local rules is available at www.ediscoverylaw.com/uploads/file/N_C_%20Local%20Rule%2016_1.pdf (last visited Apr. 12, 2009).

71. 2007 WL 1299180 (W.D.N.C. May, 2, 2007).

72. The guidelines were adapted from the United States District Court for the District of Maryland's "Suggested Protocol for Discovery of Electronically Stored Information." The document is available at www.mdd.uscourts.gov/news/news/ESIProtocol.pdf (last visited Feb. 27, 2009).

73. *O'Bar*, 2007 WL 12299180 at *4.

74. *Id*.

conference upon motion of either party that includes, among other things, a proposed discovery plan, proposed limitations on discovery, and a statement that the party's attorney has made reasonable efforts to reach agreement with the opposing party's attorney on the issues set forth in the motion.[75] If either party proposes a discovery plan, both parties and their attorneys must participate in good faith in formulating the plan.[76] Although not specifically required by the rules, parties are well advised to use the discovery conference as an opportunity to discuss any potential issues related to the discovery of ESI—including but not limited to, the scope of preservation, search, and retrieval obligations; the treatment of inadvertently produced privileged materials; and the allocation of costs—and to incorporate their agreements into the discovery plan.[77]

The *Chief Justices' Guidelines* advises parties that intend to seek the production of electronic data to communicate, in clearly delineated categories, the information to be sought early on in the discovery process. Implicit in this guidance is a requirement that counsel be well versed on its party's data storage and management systems and policies. In fact, knowledge of its client's information system may be a prerequisite for counsel to participate in the discovery plan negotiations in good faith. The *Guidelines* also counsels judges to encourage parties, and their attorneys,

---

75. Note that NCRCP 26(f1) prescribes a different discovery conference procedure in medical malpractice cases.

76. After the discovery conference the court enters an order establishing a plan for discovery, including setting a schedule for and identifying any limitations on discovery and, if necessary, allocating discovery expenses between the parties. The order may be amended at any time in the interest of justice.

In the absence of a voluntary agreement, pursuant to NCRCP 16, a court may order the parties to appear before it to discuss, among other things, any "matters as may aid in the disposition of the action," and subsequently may enter an order directing how discovery, including the discovery of electronic information, will proceed. *Chief Justices' Guidelines* recommends that, either before or during Rule 16 conference, judges direct parties to exchange information—such as the names of individuals within the parties' organizations with knowledge of their information technology systems; lists of potential sources of relevant electronic data within the parties' possession, custody, and control; and notices of any known problems reasonably anticipated to arise in connection with compliance with e-discovery requests—that will enable the e-discovery process to move forward expeditiously.

77. The proposed amendment to Rule 26(f) would significantly modify the discovery conference process. Under the new rule either party's attorney, or an unrepresented party, may request a discovery meeting no earlier than forty days after the complaint is filed. The parties must meet within twenty-one days after the request is filed in the county in which the action is pending. The court also may direct the parties to appear before it for a discovery conference any time after the commencement of the litigation.

During the discovery meeting the attorneys and the unrepresented parties are directed to discuss the nature and basis of any claims and defenses and the possibilities for prompt settlement or resolution of the case. The attorneys and the unrepresented parties also must be prepared to discuss a discovery plan and to work together in good faith to formulate the plan.

With respect to ESI, the discovery plan must address issues relating to the preservation of the information and the media, form, format, and procedures by which it will be produced. It also must address, if appropriate, the allocation of discovery costs for preservation, restoration, and production of the ESI and the method for asserting or preserving claims of privilege. Finally, it should detail any limitations proposed to be placed on the discovery of ESI, including, if appropriate, that discovery be conducted in phases or be focused on particular issues. The discovery plan requirements regarding ESI are more detailed than under FRCP 26(f), although both rules leave it to the discretion of the parties and their attorneys to determine the appropriate issues to address given the context of the litigation and the potential types of ESI that may be involved.

If the attorneys and unrepresented parties agree on a discovery plan, they must submit it to the court within fourteen days after the discovery meeting. The parties may request a conference with the court regarding the plan.

If they do not agree on a discovery plan, the parties must submit a joint report to the court describing the parts of the plan they agree upon and stating each party's position on the issues about which they disagree. Upon motion of either party, the parties may appear before the court for a discovery conference at which the court must order the entry of a discovery plan. The order may address the issues raised by the parties and any other issues necessary for the proper management of discovery in the litigation.

to "meet and confer in order to voluntarily come to agreement" on the ESI to be disclosed and the manner and timing of its production.

Testing or Sampling Data

Federal Rules of Civil Procedure. Another tool available to litigants in federal courts is the authority, under FRCP 34, to request to inspect, copy, test, or sample sources of potentially relevant electronic information. The ability to test or sample ESI allows parties to determine the relevance of particular sources of electronic information without incurring significant costs. Parties may agree to a tiered search process—whereby sources of ESI first are tested or sampled and then search requests are refined based on the information (or lack of information) revealed in the test or sample sets.[78] Both the requesting and producing parties have incentives to proceed with a tiered search process. Courts are increasingly rejecting both blanket discovery requests and are similarly skeptical of blanket objections.[79] Following a tiered discovery process allows a requesting party to target initial requests to the most likely sources of relevant ESI, but it preserves the option to supplement (expand) those requests depending on the information actually discovered. A tiered process is most effective, however, when the producing party is able to, and in fact does, share information with the requesting party about the likely sources of relevant electronic information and its ability to search and retrieve the information from those sources before any FRCP 34 requests are made. And, the requesting party must recognize that the ability to test or sample electronic information does not create a routine right of direct access to another party's information system. The party producing the electronic information retains the right, at least as an initial matter, to determine the contours of the search process.[80]

North Carolina Rules of Civil Procedure. The NCRCP do not specifically authorize the testing or sampling of documents, including electronically stored data.[81] However, parties to litigation may agree to a tiered discovery process, or to testing or sampling of some data, during their NCRCP 26(f) discovery conference; the agreement then may be incorporated into the court order establishing the discovery plan and schedule. A court also could order sampling or testing of ESI pursuant to a NCRCP 37 motion to compel production (by the requesting party), or a NCRCP 26 motion for a protective order (by the producing party) in order to aid it in determining the relevancy of the potential data sought and the costs and burdens involved in its production.

---

78. Closely related to testing or sampling particular sources of electronic information is adopting protocols to cull through the data in an efficient manner. Litigants are increasingly employing automated processes to search for potentially responsive electronic information, using keywords, taxonomies, or ontologies in order to comply with discovery obligations within a reasonable amount of time. Of course an automated search has the potential to be both over- and underinclusive. That is, it may produce irrelevant information, while at the same time failing to identify relevant data. Parties should attempt to agree to search protocols up front, perhaps agreeing to a tiered process similar to the one used to sample or test sources of electronic information, to avoid costly discovery disputes.

79. *See, e.g.*, Nicholas v. Wyndham Int'l, Inc., 373 F.3d 537 (4th Cir. 2004) (granting protective order against production of additional e-mails, finding that the discovery requests were cumulative and duplicative, unduly burdensome, and harassing); McDougal-Wilson v. Goodyear Tire & Rubber Co., 232 F.R.D. 246 (E.D.N.C. 2005) (denying motion to compel the production of computer generated employee profiles of all the party's employees in North Carolina from 1995–present, finding that the production would be unduly burdensome and unlikely to lead to the discovery of admissible evidence).

80. Note also that courts may order testing or sampling of data in ruling on a motion to compel production of ESI or a motion for a protective order limiting the production of ESI. *See, e.g.*, Church v. Wachovia Sec., Inc., 2008 WL 281091 (W.D.N.C. Jan. 30, 2008).

81. The proposed North Carolina amendments, likewise, would not explicitly authorize the testing or sampling of ESI.

Clawback Provisions for Privileged Data

The discovery of electronic information further complicates an already burdensome process for litigants—the review of documents for privileged information and attorney work-product (collectively, privileged material).[82] Privilege review is usually one of the most critical and sensitive aspects of the document review process. The volume and dispersion of electronic data, as well as the existence of hidden data, makes the privilege review of ESI more burdensome and costly than that of paper documents. It also increases the likelihood of an inadvertent disclosure of the privileged materials.

Federal Rules of Civil Procedure. Recognizing the increased burden on litigants in searching ESI for privileged information, the federal rules direct parties to discuss any issues relating to potential privilege claims during the meet and confer discovery meeting, including how information that is not disclosed will be tracked and how information that is disclosed will be retrieved. Beyond reclaiming any produced privileged information, the issue of waiver of the privileged status of the information is of great concern to litigants. Production of privileged documents, even inadvertently, may result in waiver of the protected status of the materials. If a waiver occurs, the waiver often is not limited to the pending litigation; in many cases, the privilege is waived for all purposes, including any future litigation. And, under certain circumstances, a waiver may extend to other information that relates to the subject matter of the disclosed information.

Pursuant to FRCP 26, parties are encouraged to agree on a protocol for both reclaiming and protecting the privileged status of any inadvertently produced materials for purposes of the pending litigation. The committee notes to FRCP 26 suggest two different procedures that purport to protect the privileged status of inadvertently produced information while also minimizing the costs of searching and reviewing electronic data for privileged documents. The first involves a clawback agreement. Under such an agreement, if the producing party discovers that it disclosed privileged information, despite its reasonable efforts to identify privileged materials before the production, it notifies the receiving party that the privileged material has been produced inadvertently and requests its return. The parties agree that the inadvertent production will not be considered a waiver of privilege as to that document or its contents or deemed to give rise to a subject-matter waiver. The second suggested procedure is to adopt a quick peek agreement. Pursuant to a quick peek agreement, the producing party provides specified categories of documents or other electronic data for initial examination by another party. The other party then identifies by formal request under FRCP 34 the information it wants produced. The producing party subsequently reviews the requested information and makes any appropriate privilege claims. The parties agree that the initial provision of any privileged materials for examination does not constitute a waiver of the protected status as to that or any other related material.[83]

---

82. "Privilege" is a legal concept that protects litigants from being compelled to disclose confidential communications made between an attorney and his or her client for the purpose of obtaining or providing legal advice or services to the client. The privilege concept applies to both communications an individual makes to an attorney and communications that a client makes with outside and in-house counsel. Similar and related to the attorney–client privilege is the attorney work-product doctrine, which protects against the disclosure of documents and tangible materials prepared by or under the direction of an attorney, in anticipation of litigation. The attorney work-product doctrine allows clients and counsel to share facts and opinions in order to set case strategy without fear of disclosure.

83. If the parties to litigation do not reach agreement on the treatment of inadvertently produced privileged information, FRCP 26(b)(5)(B) prescribes a default protocol for reclaiming the information. If a party has produced information in discovery that it claims is privileged or protected as attorney work-product, the party must notify the receiving party of the claim as soon as possible, stating the basis for the privilege or work-product assertion. After receiving notification, the receiving party must return, sequester, or destroy the information and may not use it or disclose it to third parties until the claim is resolved. The receiving party has the option of submitting the information

Even if parties to litigation adopt protocols to address inadvertently disclosed privileged materials, such as the clawback and quick peek agreements described above, the agreements may provide protection only as between the parties to the agreement and may apply only in the current litigation. An agreement between two or more parties in litigation does not necessarily estop a third party, in a subsequent litigation, from arguing that a waiver has occurred by disclosure of the privileged information in the previous matter.[84] To address this issue and provide greater assurance to litigants, Congress amended the Federal Rules of Evidence (FRE) in 2008 to, among other things, provide that in the event of an inadvertent disclosure of privileged material, no waiver occurs if the privilege-holder took "reasonable steps" both to "prevent disclosure" in the first instance and "to rectify the error" in a timely manner.[85] It limits subject-matter waivers for all disclosed privileged materials (even intentional disclosures), except under certain circumstances.[86] FRE 502 restricts the affect of nonwaiver agreements among parties, such as clawback or quick peek agreements, though. Unless such agreements are incorporated into a court order, they only bind the parties to the agreement.[87] Rule 502 went into effect in September 2008; it is yet to be determined if it will deliver on its promised cost relief to litigants with respect to searching and reviewing ESI for privileged information and attorney work-product.[88]

North Carolina Rules of Civil Procedure. The NCRCP currently do not address the production of privileged material. Litigants, however, may seek a court order adopting a discovery plan that includes a procedure for the treatment of protected material that is inadvertently produced by one

---

directly to the court to decide whether the information is privileged or protected as claimed and, if so, whether a waiver has occurred. A receiving party that has disclosed or provided the information to a nonparty before getting notice must take reasonable steps to obtain the return of the information. The producing party must preserve the information pending the court's ruling on whether the information is privileged or protected and whether any privilege or work-product protection has been waived or forfeited by the production. The goal of this rule is to preserve the status quo until the court can decide the disputed privilege or work-product questions. Simply following the procedures outlined above may not be sufficient to preclude waiver of the protected status of the information produced. Litigants must take reasonable steps to mitigate the production of privileged and work-product information.

For a good discussion of the scope of a litigant's obligation to protect against disclosure of protected information, see *Victor Stanley, Inc. v Creative Pipe, Inc*., 2008 WL 2221841 (D. Md. May 29, 2008) (holding that attorney–client privilege or work-product protected status had been waived for electronic documents that had been produced because the producing party failed to demonstrate that the electronic keyword searches they performed to search for the protected ESI were reasonable). The use of keyword searches to identify privileged information is particularly difficult in reviewing e-mails. Privileged communications may exist in strings of e-mail correspondence but may appear only to some participants in the string depending on the sender's use of the reply and forward commands. *See* Rhoads Indus., Inc. v Bldg. Materials Corp. of Am., 254 F.R.D. (E.D. Pa. 2008).

84. Some courts have held that the privileged status of the materials is not waived with respect to nonparties or in subsequent litigation if the protocol agreements are incorporated into a court order. *See* Hopson v. The Mayor and City Council of Baltimore, 232 F.R.D. 228 (D. Md. 2005).

85. FRE 502(b) also codifies the general practice in most jurisdictions and purports to apply in both subsequent federal and state proceedings.

Note that FRE 502(c) provides that when a disclosure is made in a state proceeding and is not subject to a state-court waiver order, there is no waiver in a subsequent federal proceeding if either (1) there would be no waiver under FRE 502 if the disclosure had been made in a federal proceeding, or (2) there is no waiver under the state law where the disclosure occurred. Thus the federal or state rule that is most protective against waiver applies.

86. FRE 502(a) provides that the waiver extends to undisclosed privileged materials on the "same subject matter" only if "they ought in fairness to be considered together." The rule actually reflects the current practice in most jurisdictions. The rule purports to bar a waiver in both subsequent federal and state proceedings, however.

87. FRE 502(d) provides that federal court nonwaiver orders relating to federal proceedings bind other federal and state courts.

88. *Rhoads Industries*, 254 F.R.D. 216 (E.D. Pa. 2008), is one of the first cases to interpret Rule 502. The opinion highlights some of the challenges that litigants face in attempting to avoid waivers of privileged information.

of the parties.[89] The order will only apply to the parties to the pending litigation. Thus, even if the parties and court agree that production of privileged information does not waive its privileged status in the pending litigation, it may, in fact, waive the privileged status in other litigation or with respect to individuals or entities that are not parties to the pending litigation.[90] And, as under the federal rules, simply because such an agreement is in place does not mean that the parties do not need to take all reasonable steps to protect against disclosure of the protected information. A court may ultimately find that a waiver of the protected status of the information occurred if it determines that a litigant did not sufficiently minimize the risk of disclosure. Several courts in other jurisdictions have employed a multifactor test to determine if a waiver has occurred, considering (1) the reasonableness of the precautions taken to prevent inadvertent disclosure, (2) the number of inadvertent disclosures, (3) the extent of the disclosures, (4) any delay in the measures taken to rectify the disclosure, and (5) overriding interests of justice.[91] This approach is sanctioned by the *Chief Justices' Guidelines*. The North Carolina Rules of Evidence do not have a counterpart to FRE 502.

Limit on Discoverable Data

What if parties to litigation are unable to successfully collaborate and agree on preservation, search, and retrieval protocols? Is there any limit on the scope of production of electronic data imposed by federal or state rules? The answer is maybe. There is a general presumption in civil litigation that all relevant information within the possession, custody, or control of a party is discoverable. Under certain circumstances, however, a litigant either may not be required to produce electronic data or, at least, may be protected from sanctions for failure to preserve or produce the data.

Not Reasonably Accessible Data

One of the over-arching goals of the federal and state discovery rules is to strike a balance between allowing access to information and containing costs. Before the 2006 amendments to the federal rules, litigants could seek a protective order against producing information, including

---

89. It is important that litigants memorialize any agreement in a court order because not all courts have approved nonwaiver agreements between attorneys. *See, e.g.*, Koch Materials Co. v. Shore Slurry Seal, Inc., 208 F.R.D. 109 (D. N.J. 2002) (declining to give effect to agreement between counsel that production of certain documents would not waive privilege protection because such agreements "could lead to sloppy attorney review and improper disclosure which could jeopardize clients' cases").

90. The proposed North Carolina amendments encourage parties to discuss and agree to methods for asserting or preserving claims of privilege or of protection of the information as attorney work-product during the Rule 26(f) discovery meeting. The amendments also mirror the provisions in FRCP 26(b)(5)(A) and (B), with one exception. The default protocol for reclaiming information is expressly limited to inadvertently disclosed privileged or protected information.

91. *See, e.g.*, McCafferty's, Inc. v. Bank of Glen Burnie, 179 F.R.D. 163 (D. Md. 1998) (citing district court cases in Fourth Circuit). The court in *Hopson* v. *The Mayor and City Council of Baltimore*, 232 F.R.D. 228 (D. Md. 2005) also held that the privilege protocols adopted by the parties must be incorporated into a court order to avoid waiver of the protected status, stating:

> [I]t is essential to the success of this approach in avoiding waiver that the production of inadvertently produced privileged electronic data must be at the compulsion of the court, rather than solely by the voluntary act of the producing party, and that the procedures agreed to by the parties and ordered by the court demonstrate that reasonable measures were taken to protect against waiver of privilege and work product protection.

Id. at 240.

ESI, if "the burden or expense of the proposed discovery outweighed its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues."[92] Courts imposed a high threshold in analyzing what constituted an undue burden on a party with respect to the production of paper documents and tangible items and typically erred on the side of allowing discovery, albeit sometimes only conditionally. In early e-discovery cases most courts imposed a similarly high threshold in analyzing claims that the discovery of electronic information was somehow unique and more onerous than the discovery of traditional documents. To the extent that there were greater costs associated with e-discovery, these were deemed to be simply part of the costs of doing business in the digital age.

Federal Rules of Civil Procedure. Following the lead of a seminal opinion out of the Southern District of New York in 2003, *Zubulake v. UBS Warburg, LLC*,[93] at least some courts began to recognize the differences between electronic information and paper documents and how those differences often translated into significantly higher costs and burdens on both the parties and the courts. The drafters of the 2006 amendments sought to encourage courts to consider limiting discovery of electronic information by specifying that a party is not obligated to produce ESI that it identifies as not reasonably accessible because of undue burden or cost.[94] This represents a change from the general presumption of the discoverability of relevant information.[95] The rules do not define what type of ESI is not reasonably accessible. Litigants have focused on the underlying form or format of the information—claiming, for example, that inactive data on backup tapes, legacy data, fragmented or deleted data, and multilayered databases are not reasonably accessible. Whether or not a particular source of ESI is accessible does not necessarily depend on the type of data or the type of media on which it is stored, though. Instead, the determination ultimately depends on whether the costs of retrieving, searching, and producing the data outweigh the value of the ESI to the requesting party. Most ESI can be retrieved, it is just a matter of at what cost. ESI is not considered "not reasonably accessible" simply because it is expensive, only if it poses an undue burden or cost on the producing party.

Upon a motion to compel production, or a motion for a protective order, the producing party bears the burden of showing that the ESI is not reasonably accessible because of undue burden or cost. If it meets that burden, there appears to be a presumption against production.[96] The court

92. FRCP 26(b)(2). Under FRCP 26(b)(2) a party may object to any discovery request, including one for ESI, (1) if the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (2) if the party seeking discovery has had ample opportunity through other discovery to obtain the information sought; or (3) if the burden or expense of the proposed discovery outweighs its likely benefit. Pursuant to a motion to compel production, under FRCP 37(a), or a motion for a protective order, under FRCP 26(c), a court may consider these factors, commonly known as the proportionality factors, to prohibit, limit, or condition the discovery on, among other things, the requesting party bearing all or part of the costs of retrieving the information. When engaging in the cost benefit analysis under factor three, a court may consider (a) the needs of the case, (b) the amount in controversy, (c) the parties' resources, (d) the importance of the issues at stake in the litigation, and (e) the importance of the proposed discovery in resolving the issues.

93. 217 F.R.D. 309 (S.D.N.Y. 2003). The case will be discussed in the subsection, "Cost-Sharing," below.

94. In its response to a Rule 34 request, the producing party should identify by category or type the sources containing potentially responsive ESI that it is not searching or producing.

95. If a party determines that ESI is not reasonably accessible, it does not relieve the party of its common law duty to preserve the information. A party fails to preserve any potentially relevant ESI at its peril because a court may ultimately order production of that ESI. If the party failed to preserve the ESI, it may face sanctions from the court for spoliation.

96. According to the chair of the advisory committee that drafted the 2006 amendments, however, "[T]he rule is not one of presumed non-discoverability, but instead makes the existing proportionality limit more effective in

may, however, order discovery of the ESI if the requesting party demonstrates good cause. In making its determination the court must take into consideration the FRCP 26(b)(2)(C) proportionality factors.[97] The court may order a test or sample production in order to evaluate the likelihood of discovering additional relevant information and weigh its findings against the potential burdens and costs to the producing party.

According to the committee notes to FRCP 26, in most cases discovery from reasonably accessible sources should be sufficient to fully satisfy the requesting party's discovery needs. In fact parties are encouraged to agree to a phased or tiered discovery approach, wherein the requesting party reviews ESI produced from reasonably accessible sources before requesting further production that may be more difficult to retrieve and, consequently, more costly to the producing party. If the requesting party determines that the initial production is not sufficient, the parties will need to appraise the burden and cost of further searches, as balanced against the potential value of the information sought, and consider both whether to incur those burdens and costs and how best to allocate them among the parties. This is among the issues that should be discussed early on in the litigation.

Note that although a litigant may be able to successfully argue that it does not have to produce data that existed in a format that was not reasonably accessible at the time the duty to preserve the information was triggered, FRCP 26 likely does not relieve a party of its burden to preserve subsequently generated information in a reasonably accessible format if possible.[98] In other words a litigant is not going to be able to avoid discovery obligations simply by saving (or converting) its information into a format that is not reasonably accessible.

Note also that, in some cases, preserving, searching, and retrieving ESI from accessible sources may prove equally burdensome and costly to the producing party. It often involves some interruption to a party's current operations. Relying on the proportionality factors in Rule 26(b)(2)(C), a party may move for a protective order against producing ESI even from reasonably accessible sources. In practice, however, courts have been less receptive to arguments that producing potentially relevant information from reasonably accessible sources is unduly burdensome. (Recall that data that is reasonably accessible by definition does not pose an undue burden or cost on the producing party.)

North Carolina Rules of Civil Procedure. The NCRCP do not explicitly authorize parties to refuse to produce ESI that is not reasonably accessible.[99] A litigant may move for a protective

---

a novel area in which the rules can helpfully provide better guidance." *See* Committee on Rules of Practice & Procedure, Judicial Conference of the U.S., *Meeting of June 15-16 Minutes 25*, *available at*: www.uscourts.gov/rules/Minutes/ST_June_2005.pdf (last visited March 1, 2009).

97. FRCP 26. According to the committee notes to FRCP 26, additional appropriate considerations include: (1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessible sources; (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources; (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources; (5) predictions as to the importance and usefulness of the further information; (6) the importance of the issues at stake in the litigation; and (7) the parties' resources. For a good discussion of the application of these factors see *W.E. Aubuchon Co., Inc. v Benefirst, LLC*, 245 F.R.D. 38 (D. Mass. 2007) (holding that ESI was not reasonably accessible but that requesting party had demonstrated good cause for production).

98. *See* Toussie v. County of Suffolk, 2007 WL 4565160 (E.D.N.Y. Dec. 21, 2007).

99. Under the proposed North Carolina amendments the process by which the producing party may object to the production of ESI is very similar to that prescribed by the federal rules. As an initial matter a party always may seek a protective order under Rule 26(c) if it believes that a discovery request is unreasonably cumulative, is sought for an improper purpose, or poses a burden on the producing party that outweighs its likely benefit to the requesting party.

Additionally, under the federal rules a party is not obligated to produce ESI from sources that it identifies as not reasonably accessible because of undue burden or cost. The party must state its objection in its written response to a

order under NCRCP 26 against producing certain information, including data compilations. A court may prohibit, limit, or condition the discovery on specified requirements. NCRCP 26(b)(1) sets forth the same proportionality factors as does its federal rules counterpart, FCRP 26(b)(2)(C). Specifically, the rule directs a court to limit the frequency or extent of discovery if it determines that (1) the discovery sought was unreasonably cumulative or duplicative, or could be obtained from some other source that is more convenient, less burdensome, or less expensive; (2) the party seeking discovery had ample opportunity to obtain the information by discovery in the action; or (3) the burden or expense of the proposed discovery outweighed its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.

North Carolina courts have relied on the third factor to limit the discovery of ESI. In *Analog Devices, Inc. v. Michalski*,[100] the court discussed the application of the Rule 26 proportionality factors to the discovery of electronic data. The case involved allegations of misappropriation of trade secrets, breach of contract, and unfair competition. At issue was the discovery of certain e-mails of the originators of the trade secrets that resided only on the producing party's backup server. The producing party claimed that the production of the e-mails would be expensive and time consuming and, therefore, unduly burdensome. The court surveyed a number of different approaches to determining whether, and under what circumstances, discovery of the e-mails should be compelled. Ultimately, the court concluded that "[a] straightforward application of the basic analytical framework found in Rule 26 should allow courts to . . . reach decisions that safeguard both the interest of justice and the liberal discovery goals of the Rules of Civil Procedure."[101] The court noted, however, that with respect to the production of data that a litigant claims is not reasonably accessible the "overriding concern for judges . . . should be whether or not they are making an outcome-determinative decision." And, the court acknowledged that "[i]n cases where . . . the discovery is stored in a form that is particularly difficult or costly to retrieve, a more searching inquiry into the competing interests of preventing undue burden or expense to the producing party and the importance of the discovery to the requesting party is warranted." The court then applied the third proportionality factor to the facts of the case and granted the requesting party's motion to compel production of the e-mails but ordered that the costs of restoration and recovery be borne equally by both parties.[102]

The *Chief Justices' Guidelines* advises courts to first determine if the information is subject to discovery under the applicable rules and then weigh the benefits to the requesting party against the burden and expense of the discovery to the producing party.[103]

Rule 34 request. The producing party also may seek a protective order under Rule 26(c) or the requesting party may move for an order to compel production under Rule 37(a). The party objecting to the production has the initial burden of demonstrating that the basis for the objection exists. If it meets this burden, the court may nonetheless order discovery if the requesting party shows good cause. In making its determination the court must consider the Rule 26(b)(2) proportionality factors.

100. 2006 WL 3287382 (N.C. Super. Ct. Nov. 1, 2006).

101. The court suggested that it would also refer to *Chief Justices' Guidelines.*

102. In a case decided the same day, *Bank of America Corporation Corp. v. SR International Business Insurance Co., Ltd.*, 2006 WL 3093174 (N.C. Super. Ct. Nov. 1, 2006), the court denied discovery of deleted e-mails contained only on the backup tapes of a nonparty. (The discovery request was pursuant to NCRCP 45.)

103. *Chief Justices' Guidelines* lists the following thirteen factors to aid courts in the cost-benefit analysis: (1) the ease of accessing the requested information; (2) the total cost of production compared to the amount in controversy; (3) the materiality of the information to the requesting party; (4) the availability of the information from other sources; (5) the complexity of the case and the importance of the issues addressed; (6) the need to protect privileged, proprietary, or confidential information, including trade secrets; (7) whether the information or software needed to

Protection from Spoliation Sanctions

What happens if relevant electronic data is deleted or otherwise irretrievable after the duty to preserve it for pending or anticipated litigation is triggered? As discussed above, a litigant may be subject to spoliation sanctions for failure to preserve or produce relevant information. Court-ordered sanctions can vary significantly and are highly dependent on the facts and circumstances of each case.[104] But, a court is not required to award sanctions, and it may be prohibited from imposing sanctions under certain conditions.

Federal Rules of Civil Procedure. FRCP 37(e) states that "[a]bsent exceptional circumstances, a court may not impose sanctions under [the Federal Rules of Civil Procedure] on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system." The committee notes to FRCP 37 state that it only applies to information lost "due to the 'routine operation of an electronic information system'—the ways in which such systems are generally designed, programmed, and implemented to meet the party's technical and business needs." Courts have interpreted this provision to require that data be lost due to some sort of automated, routine system.[105] Further, the good-faith operation of such a system obligates a party to act affirmatively to prevent its information system from destroying or altering information. Thus, the so-called safe harbor provision appears to be very narrow in its application and provides little prospective guidance to litigants.[106]

North Carolina Rules of Civil Procedure. The North Carolina Rules of Civil Procedure do not include a specific safe harbor provision for electronic information lost as a result of the

---

access the requested information is proprietary or constitutes confidential business information; (8) the breadth of the request; (9) the relative ability of each party to control costs and its incentive to do so; (10) the resources of each party compared to the total cost of production; (11) whether the requesting party has offered to pay some or all of the costs of identifying, reviewing, and producing the information; (12) whether the electronically stored information is stored in a way that makes it more costly or burdensome to access than is reasonably warranted by legitimate personal, business, or other non–litigation-related reasons; and (13) whether the responding party has deleted, discarded, or erased electronic information after litigation was commenced or after the responding party was aware that litigation was probable.

104. *See* Teague v. Target Corp., 2007 WL 1041191 (W.D.N.C. Apr. 4, 2007) ("While courts have broad discretion to sanction a party for spoliation, the applicable sanction should be molded to serve the prophylactic, punitive, and remedial rationales underlying the spoliation doctrine.") (internal quotations omitted); *see also* Eckhardt v. Bank of Am. Corp., 2008 WL 1995310 (W.D.N.C. May 6, 2008) (ordering party to pay the costs associated with making its current and former employee deponents available after determining that party did not fully comply with previous court order requiring the party to identify all sources of relevant ESI); Orrell v. Motorcarparts of Am., Inc., 2007 WL 4287750 (W.D.N.C. Dec. 5, 2007) (ordering plaintiff to produce hard drive for forensic examination by defendant after finding that plaintiff did not fully comply with discovery obligations, stating that the plaintiff's burden to preserve evidence was not eliminated due to the alleged crashing of the plaintiff's computer); Warner Bros. Records, Inc. v. Souther, 2006 WL 1549689 (W.D.N.C. June 1, 2006) (ordering defendant to produce computer hard drive at evidentiary hearing and authorizing plaintiff's forensic technician to make a mirror of image of the hard drive in the court's chambers because defendant failed to provide electronic copies of the computer's desktop and registry files in response to a discovery request).

105. *See, e.g.*, Doe v. Norwalk Cmty. Coll., 248 F.R.D. 372 (D. Conn. 2007) (holding that producing party could not take advantage of Rule 37(e)'s good faith exception because it did not have a consistent, routine system in place); *see also* State of Texas v. City of Frisco, 2008 WL 828055 (E.D. Tex. Mar. 27, 2008) (suggesting that Rule 37 addresses the extent of a litigant's duty to preserve information in anticipation of litigation); *In re* Krause, 367 B.R. 740 (D. Kan. 2007). *But see* Escobar v. City of Houston, 2007 WL 2900581 (S.D. Tex. Sept. 29, 2007) (relying on Rule 37 good faith exception to sanctions where there was no duty to preserve the information and the destruction was not done in bad faith).

106. Note also that FRCP 37(e) only applies to sanctions arising under the rules. A court, therefore, retains its inherent authority to impose sanctions even if the provisions of FRCP 37(e) are satisfied.

routine, good faith operation of an information system.[107] The *Chief Justices' Guidelines* suggests that a court should impose sanctions because of the destruction of electronic information only if (1) there was a legal obligation to preserve the information at the time it was destroyed; (2) the destruction of the material was not the result of the routine, good faith operation of an electronic information system; and (3) the destroyed information was subject to production under the applicable state standard for discovery. In North Carolina sanctions for spoliation may be imposed even if relevant evidence is lost or destroyed without intent. A showing of bad faith or even negligence on the part of the spoliating party is not necessary.[108] In *Arndt v. First Union National Bank*,[109] the North Carolina Court of Appeals held that sufficient evidence supported an adverse inference instruction[110] to the jury on spoliation of evidence where certain relevant e-mails and profit and loss statements were not preserved by the defendant at a time that the defendant should have reasonably anticipated litigation.

Cost-Sharing

Even if litigants take advantage of some of the previously discussed tools for reducing the amount of electronic information that needs to be preserved and produced, parties still may face substantial burdens and costs to comply with discovery obligations. Under the American civil discovery system there is a presumption that the producing party pays the costs of production. Although the federal rules encourage parties to discuss the potential for cost-sharing, they do not require courts to shift any of the costs of production to the requesting party. Likewise, the NCRCP do not explicitly address cost-allocation.[111] In early electronic discovery cases, most courts required the producing party to bear the cost of producing electronic evidence, reasoning that producing the data was an ordinary and foreseeable risk of using electronic storage media.[112] As detailed above, however, the costs of retrieving, reviewing, and analyzing electronic evidence, by itself, can be

---

107. The proposed North Carolina amendments would include a safe harbor provision that mirrors that in FRCP 37(e).

108. *See* McLain v. Taco Bell Corp., 137 N.C. App. 179, 527 S.E.2d 712 (2000). Note that federal courts in North Carolina

> have held that three elements should be shown to warrant an adverse inference instruction for spoliation: (1) the party having control over the evidence had an obligation to preserve it when it was destroyed; (2) the destruction or loss was accompanied by a "culpable state of mind;" and (3) the evidence that was destroyed was relevant to the claims or defenses of the party that sought discovery of the spoliated evidence, to the extent that a reasonable fact finder could conclude that the lost evidence would have supported the claims or defenses of the party that sought it.

Teague v. Target Corp., 2007 WL 1041191 (W.D.N.C. Apr. 4, 2007).

109. 170 N.C. App. 518, 613 S.E.2d 274 (2005); *see also* Commissioner v. Ward, 158 N.C. App. 312, 580 S.E.2d 432 (2003) (affirming default judgment sanction against party that repeatedly violated court order to produce information, including electronically stored information).

110. An adverse inference instruction allows a jury to infer that the information that was spoliated would have been adverse to the spoliating party.

111. The proposed North Carolina amendments would encourage courts to consider cost-shifting as a potential condition to authorizing the discovery of ESI that is not reasonably accessible due to undue burden or costs.

112. *See, e.g.*, Linnen v. A.H. Robins Co., 1999 WL 462015 (Mass. Super. Ct. June. 16, 1999) (holding that the costs of restoring electronic data in response to discovery requests is "one of the risks taken on by companies which have made the decision to avail themselves of the computer technology"); *In re* Brand Name Prescription Drugs Antitrust Litig., 1995 WL 360526 (N.D. Ill. Jun. 15, 1995) (denying motion that requesting party bear cost of producing electronic documents, noting that "if a party chooses an electronic storage method, the necessity for a retrieval program or method is an ordinary and foreseeable risk."); Bills v. Kennecott Corp., 108 F.R.D. 459 (D. Utah 1985) (denying motion to shift the costs of the discovery of electronic data because (1) the defendant was in the "most economical position to

substantially greater than traditional paper document productions. Recognizing the often harsh fiscal realities associated with electronic discovery, many courts have followed the lead of the court in *Zubulake*,[113] in which the court formulated a seven-factor analysis to determine if at least some of the costs of producing ESI should be allocated to the requesting party. The seven cost-allocation factors outlined by the court are: (1) the extent to which the request is specifically tailored to discover relevant information; (2) the availability of such information from other sources; (3) the total cost of production as compared to the amount in controversy; (4) the total cost of production as compared to the resources available to each party; (5) the relative ability of each party to control costs and its incentive to do so; (6) the importance of the issues at stake in the litigation; and (7) the relative benefits to the parties of obtaining the information.[114] The court applied varying weights to the different factors, deeming the first two factors most important; the next three factors, addressing cost issues, as slightly less important; and the final factor as the least important. The court noted that the sixth factor rarely will come into play—as it applies only to matters of critical public concern—but has the potential to predominate over the others. The court also suggested that courts first might want to order responding parties to produce test-sets of data to inform the court's assessment whether additional production is appropriate and, if so, who should pay.

Perhaps most importantly, however, the court admonished that cost-shifting should not be considered in every case involving the discovery of electronic data. Rather, the cost-shifting analysis is triggered only when e-discovery imposes an "undue burden or expense" on the responding party, consistent with then FRCP 26(b)(2).[115] According to the court, "[W]hether production of documents is unduly burdensome or expensive turns primarily on whether it is kept in an accessible or inaccessible format . . . ." And, whether electronic data is "accessible" or "inaccessible" depends "largely on the type of media on which the data is stored."[116] This approach toward limiting or conditioning discovery if it is unduly burdensome subsequently was embraced by the 2006 amendments which, as discussed above, provide that a party need not produce ESI that is not reasonably accessible, unless good cause is found.

Given the dynamic and tangled nature of information technology systems, however, the line between accessible and inaccessible data will not always be clear. In fact the line may best be viewed as a continuum—ranging from data stored in a readily usable format (such as hard copy files, active websites, networks, or optical disks or drives), to data that requires extensive manipulation to be retrieved and restored (such as disaster recovery backup tapes, obsolete software applications, and "deleted" network files). For example, data stored on some types of backup

---

call up its own computer stored data," (2) the cost was not excessive, (3) the relative burden in obtaining the data was substantially greater to the requesting party, and (4) the responding party was benefitted to some degree).

113. 217 F.R.D. 309 (S.D.N.Y. 2003). The case involved an employment discrimination claim against the defendant, UBS Warburg. During the litigation the parties battled over a number of discovery issues, including the production of e-mails that were contained on an e-mail system, optical disks, and backup tapes. After reviewing a test-set of the e-mails at issue, the court ordered the defendant to, among other things, produce the e-mails. It required the plaintiff, however, to bear 25 percent of the costs of their production (defined to include only the costs of retrieving the e-mails from the backup tapes, not the costs of review for privilege).

114. Note that the court in *Zubulake* actually modified a cost-allocation test that was adopted a couple of years earlier in *Rowe Entertainment, Inc. v. The William Morris Agency, Inc.,* 205 F.R.D. 421 (S.D.N.Y. 2002). The *Zubulake* court felt that that the *Rowe* test did not comport with the general presumption against cost-shifting except when the production was unduly burdensome.

115. The case was decided before the federal rules were amended.

116. For an application of the *Zubulake* cost-shifting analysis in a case involving a public sector entity, see *Semsroth v. City of Wichita*, 239 F.R.D. 630 (D. Kan. Nov. 15, 2006).

tapes may be easily accessed in a usable format, usually at the stroke of a few keys, whereas data stored on other types of backup tapes may require additional software to decompress and retrieve required files.

The *Chief Justices' Guidelines* sanctions the seven-factor *Zubulake* test and states that

> [o]rdinarily, the shifting of the costs of discovery to the requesting party or the sharing of those costs between the requesting party and the responding party should be considered only when the electronically-stored information sought is not accessible information and when restoration and production of responsive electronically-stored information from a small sample of the requested electronically-stored information would not be sufficient.

Recognizing the difficulty in determining the line between accessible and inaccessible data some courts have required at least some cost-shifting even when the production only involved reasonably accessible ESI, based on the proportionality factors in FRCP 26(b)(2)(C).[117]

The NCRCP contain identical proportionality factors to the federal rules. Thus, arguably, cost-shifting is available in any federal or state case in which discovery is unduly burdensome.

117. *See* 2006 Advisory Committee Note to FRCP 26 ("The limitations of Rule 26(b)(2)(C) apply to all discovery of electronically stored information."). *But see, e.g.*, Peskoff v. Faber, 244 F.R.D. 54 (D.D.C. 2007) (holding that "cost-shifting does not even become a possibility unless there is first a showing of inaccessibility").

Section 4: How Does E-Discovery Differ for Public Sector Litigants?

The difficulties presented by the discovery of electronic information are not unique to public sector entities. But, governments and government agencies may face additional challenges in navigating e-discovery obligations.

Lack of Resources

Public sector entities, for example, often lack the resources (or the political will to expend available resources) to adopt effective electronic data management systems and practices and, consequently, may face even greater hurdles and expenses in retrieving responsive data.

Nevertheless, government entities may not avoid discovery obligations simply because they do not employ sophisticated information technology systems. Consider *Toussie v. County of Suffolk,*[118] a case which involved a civil rights claim relating to the sale of real estate parcels at a county auction. In *Toussie*, the county-defendant initially produced only two e-mails pursuant to a document request. Upon a motion to compel production of additional electronic information, the county first argued that its employees did not routinely communicate through e-mail. The court found this claim disingenuous at best. It ordered the county to search for more e-mails. The county failed to respond to this order and, in response to another motion to compel, the county argued that it lacked the resources to perform the court-ordered search because it did not have an e-mail archival system.[119] Instead, it stored e-mails on backup tapes that were not easily searchable to extract relevant data. The court found this claim unpersuasive, and "expressed [] exasperation with the County's position by noting 'You can't just throw up your hand and say we don't store [e-mails] in an accessible form and then expect everybody to walk away.'" Facing the threat of stiff discovery sanctions, the county ultimately hired an outside vendor to search the backup tapes, which resulted in the production of at least 2,197 additional e-mails, at a significant cost to the county.[120]

---

118. 2007 WL 4565160 (E.D.N.Y. Dec. 21, 2007). Note, however, that at least one court has considered the fact that a party is a governmental entity that receives money only from the public in analyzing whether cost-shifting is warranted for the discovery of electronic information. Semsroth v. City of Wichita, 293 F.R.D. 630 (D. Kan. Nov. 15, 2006) ("However, it should also be considered that as a governmental entity, the City's ability to shoulder significant discovery costs is not comparable to .[.] . investment banking organizations . . . and the source of any such monies comes from public rather than private sources.").

119. An archival system facilitates the retention of e-mails in a searchable format.

120. Additionally, at some point in the process it became clear that potentially relevant data was lost because the county had not taken further steps to implement a litigation hold once the duty to preserve attached. The court found the county to have acted with negligence, if not gross negligence, and it forced the county to pay the plaintiffs' costs of preparing for and appearing at several discovery hearings. The court declined to impose further sanctions on the party because the plaintiffs did not establish that the information that was not produced would have supported their claims.

Public Records Requirements

Public sector entities also often are subject to fairly detailed statutory requirements governing the retention and dissemination of certain public information. These requirements both may aid and complicate a public sector entity's compliance with discovery requirements. In North Carolina, state and local governments and other public entities (collectively, public agencies) must retain certain *public records*, for varying lengths of time, according to disposition schedules established by the North Carolina Department of Cultural Resources.[121] Public records are defined to include "all documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data-processing records, artifacts, or other documentary material, regardless of physical form or characteristics, made or received pursuant to law or ordinance in connection with the transaction of public business . . . ."[122]

Additionally, unless the information qualifies for a statutory exemption, a public agency generally must make its public records available for inspection and examination by any person and must provide copies of the records upon request within a reasonable period of time.[123] A person requesting copies of public records, including electronic public records, "may elect to obtain them in any and all media in which the public agency is capable of providing them."[124] A public agency may charge fees for providing uncertified copies of public records, but the fees may not exceed the *actual costs* to the public agency of making the copies.[125] Actual costs are statutorily limited to "direct, chargeable costs related to the reproduction of a public record as determined by generally accepted accounting principles . . . ." and generally do not include indirect costs or the personnel costs associated with searching for, retrieving, and copying the requested records. A public agency may impose a "special service charge," however, if the public records request requires "extensive use of information technology resources or extensive clerical or supervisory assistance by personnel . . . or if producing the record in the medium requested results in a greater use of information technology resources than that established by the [public entity] for the reproduction of the volume of information requested . . . ."[126]

---

121. *See* G.S. 132-1 and G.S. 132-3. The Department of Cultural Resources' current retention schedules for public records generated by local governments in North Carolina are available at www.records.ncdcr.gov/local/default.htm (last visited May 19, 2009). The retention schedules for public records generated by state agencies in North Carolina are available at www.records.ncdcr.gov/schedules/default.htm (last visited May 19, 2009). And, guidelines for the retention and disposition of e-mails by public sector entities in North Carolina are available at www.records.ncdcr.gov/erecords/Email_8_02.pdf (last visited May 19, 2009). Finally, the North Carolina Government Records Branch's e-mail management policy for state and local government employees is available at www.records.ncdcr.gov/erecords/default.htm#email (last visited July 29, 2009). Note, however, that not all information that is generated or stored by a public agency constitutes a public record, and not all public records must be retained for any period of time.

122. G.S. 132-1. For detailed guidance on public records requirements in North Carolina, see David M. Lawrence, Public Records Law for North Carolina Local Governments (Institute of Government 1997) and David M. Lawrence, 1997-2003 Supplement to Public Records Law for North Carolina Local Governments (Institute of Government 2004).

123. *See* G.S. 132-6; G.S. 132-6.2.

124. G.S. 132-6.2. The statute further provides that "[n]o request of copies of public records in a particular medium shall be denied on the grounds that the custodian has made or prefers to make the public records available in another medium." *Id.*

125. G.S. 132-6.2. A person also may request certified copies of public records. According to the statute, "[t]he fees for certifying copies of public records shall be as provided by law."

126. G.S. 132-6.2. The special charge must be based on the "actual cost incurred for such extensive use of information technology resources or the labor costs of the personnel providing the services, or for a greater use of information technology resources that is actually incurred by the [public entity] or attributable to the [public entity]."

There are several parallels between the obligations imposed under North Carolina's public records laws and those imposed by civil discovery rules for dealing with ESI.[127] Both prohibit the destruction of certain ESI, at least for a period of time. Both require access to or the production of, ESI upon request and, for the most part, in the form requested.[128] Both provide exceptions for certain privileged materials.[129] And, both impose (sometimes large) costs and burdens on public agencies.

Benefits of Public Records Requirements to Public Sector Litigants

Some of the public records requirements actually may aid a public agency in complying with e-discovery requirements.

Overlap among public records and discovery requirements. First, for a unit facing litigation, there is likely to be a good deal of overlap between the two sets of obligations. A significant amount of ESI that may be relevant to a typical civil dispute involving a public agency likely also is subject to statutory retention, at least for a period of time. As such, assuming full compliance with the public records laws, the data already will be preserved.

Organization of public records for search and retrieval. Second, because of the public records requirements, at least theoretically, a public entity must take some steps to organize its public records, including its electronic public records, in a manner that provides for search and retrieval. In fact, with respect to electronic public records, a public agency is prohibited from purchasing, leasing, creating, or otherwise acquiring "any electronic data-processing system for the storage, manipulation, or retrieval of public records unless it first determines that the system will not impair or impede the agency's ability to permit the public inspection and examination, and to provide electronic copies of such records."[130] A public agency further is required to create an index of any computer databases that it compiles or creates, which includes a list of data fields, a description of the format or record layout, information as to the frequency with which the database is updated, a list of any data fields to which public access is restricted, a description of each form in which the database can be copied or reproduced using the agency's computer facilities, and a schedule of fees for the production of copies in each available form.[131] Both of these statutory requirements potentially also would aid a public agency in complying with discovery requests for at least some of its ESI.

Employees and officials accustomed to saving and producing information. Third, because of the public records requirements, public employees and officials are accustomed to dealing with regulations relating to the retention of, and access to, certain information. Complying with a litigation hold and discovery production requirement, thus, may not be as foreign to them as to their private sector counterparts, who often generate, organize, and dispose of information at will.

---

127. Much of what is discussed in this section applies to both electronic records and paper records. Electronic information further complicates a public agencyís compliance with both public records laws and civil discovery requirements. For that reason, this section focuses on the relationship between electronic public records and ESI subject to civil discovery.

128. G.S. 132-6.2 provides that "[p]ersons requesting copies of public records may elect to obtain them in any and all media in which the public agency is capable of providing them. No request for copies of public records in a particular medium shall be denied on the grounds that the custodian has made or prefers to make the public records available in another medium."

129. Although, the exception under the public records laws is limited. *See* G.S. 132-1.1.

130. G.S. 132-6.1. Electronic data-processing system is defined to include "computer hardware, computer software, or computer programs or any combination thereof, regardless of kind or origin."

131. G.S. 132-6.1.

Disposition schedules aid in data management. Fourth, although the disposition schedules for public records prescribed by the Department of Cultural Resources do not require actual disposition of the public records once the retention period has passed, they potentially provide a useful data management guide for public agencies. Private sector entities frequently are advised to adopt and ensure compliance with stringent electronic document deletion policies as the best way to manage information and control costs in the event that they subsequently face litigation.[132] Common wisdom suggests that the lower the volume of ESI, the lower the costs of its preservation, search, and retrieval. The disposition schedules, if carefully followed, potentially serve the same purpose for public sector entities.

Burdens of Public Records Requirements on Public Sector Litigants

Despite their potential benefits to public sector litigants in complying with civil discovery obligations, the public records laws also present a number of complicating factors. In fact, the interrelation between the public records laws and civil discovery obligations may be analyzed as two sides of the same coin—the same public records requirements that (at least potentially) aid a public sector entity's compliance with its discovery obligations also may hinder its compliance.

Public records and discovery requirements not completely coextensive. First, statutory public records requirements and the duties to preserve and produce information pursuant to civil discovery rules are not always coextensive. And the potential for confusion by and among public sector employees, officials, and (even) attorneys as to the different preservation and production requirements should not be understated.

There may be electronic information that is relevant to a current or anticipated lawsuit but that does not constitute a "public record" under the state's public records laws. For example, in order to constitute a public record, information must be "made or received pursuant to law or ordinance in connection with the transaction of public business." A personal e-mail or other ESI generated by an employee for personal use only (personal ESI) is not a public record, even if it is created and stored on a government-owned computer.[133] Thus personal ESI is not required to be retained or produced pursuant to the public records laws. Personal ESI, however, may be discoverable if it is relevant to a litigation involving the public entity, such as a sexual harassment claim by an employee or a claim involving other inappropriate or illegal behavior. If it is relevant to pending, or reasonably anticipated, litigation, the ESI must be preserved pursuant to the public agency's discovery obligations.

Likewise, there are many statutory exemptions to the general supposition that all records held by a public agency are open to public access. Examples include personnel records, trade secrets, local tax records, personal medical information, public enterprise billing information, and student records.[134] Any ESI that constitutes a statutorily exempted record is not required to be disclosed, and in some cases it may not be disclosed, pursuant to a public records request. If relevant to a

---

132. *See* Arthur Andersen, LLP v. United States, 544 U.S. 696 (2005) (noting that there is nothing wrong with having a policy that requires the destruction of documents, as long as it does not occur at a time when a legal preservation duty has arisen). Of course, potentially relevant data never should be deleted during pending litigation or when litigation is reasonably anticipated.

133. *See* North Carolina Department of Cultural Resources, *Email as a Public Record in North Carolina: Guidelines for Its Retention and Disposition,* p.3, *at* www.records.ncdcr.gov/erecords/Email_9_02.pdf (last visited June 29, 2009).

134. This list is not exhaustive. For a detailed list and explanation of the statutory exemptions see David M. Lawrence, Public Records Law for North Carolina Local Governments (Institute of Government 1997) and David M. Lawrence, 1997-2003 Supplement to Public Records Law for North Carolina Local Governments (Institute of Government 2004).

pending litigation, in most cases it may be required to be disclosed pursuant to a valid discovery request.[135]

Further, under the public records laws a public agency does not have a duty to create a record that does not otherwise exist.[136] Under the civil discovery laws, however, a public agency may have to compile ESI in a manner in which it is not normally maintained in order to translate it into a reasonably usable format.

Finally, not all public records must be saved indefinitely, or even at all.[137] Public employees or officials must retain ESI, including e-mails, according to the disposition schedule of the record series to which the subject and content of the ESI relates. The disposition schedules vary significantly depending on the underlying information—a public agency may destroy some ESI as soon as its useful value expires, whereas it may be required to retain other ESI for a certain period of time or even permanently. Again, however, if the ESI is subject to a litigation hold, because it is relevant to the dispute, it typically must be preserved until the final disposition of the dispute through litigation or otherwise.

Lack of compliance with public records requirements. Second, the public record laws and document retention policies are only as good as the level at which a public agency's officials and employees comply with them. As stated above, a public agency may not have the resources to adopt an efficient data management system to handle its public records. Because of the nature of electronic information, and its ease of storage, a public record may be kept in electronic format (even inadvertently) long after it could have been disposed according to the records retention schedule, which adds to the volume of information within the possession, custody, or control of the public agency. This accumulation of data potentially negates, or at least significantly diminishes, any benefit to the public agency from the detailed disposition schedules.

Public records requirements add to total volume of information. Third, even if a public agency complies perfectly with the disposition schedules, the public records laws impose a burden on public sector entities to retain information that its employees and officials might otherwise destroy. Public agencies often do not have the same freedom to routinely delete electronic data in order to better manage digital information as do their private sector counterparts. Thus the public records retention requirements, themselves, add to the total volume of electronic information that is within the possession, custody, or control of a public agency. Furthermore, even if an electronic record is "disposed of" for purposes of the public records laws, it may still be discoverable. Recall that deleted electronic data may still reside within the recesses of a computer, until it is overwritten by automatic computer processes. A person likely does not have a right to request to examine, or to request a copy of, deleted electronic data, even if it technically exists in some form. The deleted data may very well be subject to discovery, though.

Spoliation sanctions. Fourth, a public agency may have more difficulty avoiding spoliation sanctions in the event that information that is relevant to a civil lawsuit was lost or destroyed if that information was also subject to a statutory preservation obligation. It would be hard to argue under FRCP 37, for example, that deletion of electronic information was pursuant to a routine, good-faith operation of an electronic information system if that information was subject

135. As described in Section 2, under certain circumstances a litigant may seek a protective order to prevent or limit disclosure of certain information. Whether or not a protective order is warranted is dependent on the facts and circumstances of a particular case. Additionally, some information generated or stored by a public agency is shielded from discovery under federal or state law.

136. *See* G.S. 132-6.2(e).

137. Different types of records are subject to different retention schedules and not all records generated by a public sector entity must be retained at all.

to statutory retention. For many of the reasons that electronic information differs from paper documents—particularly its volume and dispersion—full compliance with statutory public records retention requirements for electronic information is often difficult, though. It is made more complicated by the mobility of both electronic information-generating platforms and public employees. For example, many public sector entities allow, and even encourage, some form of telecommuting—whether through an official program or simply as a means to allow employees to accomplish more work. Often, however, the entities lack an effective mechanism to capture and store all data that is generated off-site. There are statutory penalties for failing to comply with record retention requirements,[138] but the threat of potentially large discovery sanctions should provide an added incentive to public agencies to routinely comply with all public records retention requirements.

It is important to note, however, that a violation of statutory record retention requirements will not *automatically* result in spoliation sanctions. Sanctions follow only from a discovery violation. In *Sarmiento v. Montclair State University*,[139] an unsuccessful job candidate filed an employment discrimination claim against the university and sought sanctions because the university failed to retain the selection committee's notes that related to the decision not to hire—a violation of federal regulations. The court held that "[a]lthough a regulation may supply the duty to preserve records, a party seeking to benefit from an inference of spoliation must still make out the other usual elements" of that claim. The court found that in this case the duty to preserve for purposes of litigation had not attached because at the time the notes were destroyed, litigation was not reasonably foreseeable.

Circumventing discovery rules. Finally, because of the right of access to public records generally, a litigant may be able to obtain information, including ESI, from a state or local government or other public agency that it otherwise would not have a right to obtain pursuant to the federal or state civil discovery rules. Under G.S. 132-6 a custodian of public records must "permit any record in the custodian's custody to be inspected and examined at reasonable times and under reasonable supervision by any person" and must "as promptly as possible, furnish copies [of the requested record] upon payment of any fees as may be prescribed by law." Thus a litigant may be able to obtain, through a public records request, ESI that constitutes a public record but that is not relevant to the claims or defenses of any party (discovery standard under the FRCP) or to the subject matter involved in the pending action (discovery standard under the NCRCP).[140] Why, though, would a litigant want access to this information? Although the information requested may not relate to the underlying litigation, its discovery may serve to embarrass or harass the public sector litigant or its employees or officials.[141] A person requesting to inspect, examine, or obtain

138. *See* G.S. 132-3.

139. 513 F. Supp. 2d 72 (D. N.J. 2007).

140. *See* McCormick v. Hanson Aggregates Southeast, Inc., 164 N.C. App. 459, 596 S.E.2d 431 (2004). Note that in *Sheila v. Moon*, 125 N.C. App. 607, 481 S.E.2d 363 (1997), the North Carolina Court of Appeals stated, albeit in dicta, that "it would be illogical to allow plaintiff to circumvent the rules of discovery in a civil context through the use of the Public Records Act." The *McCormick* court, however, indicated that *Sheila* involved a unique circumstance, whereby a plaintiff had asked for and was denied discovery under the public records laws and the civil discovery rules and then sought "a second bite at the apple."

141. Note, however, that under Proposed 2009 Ethics Opinion 1 of the North Carolina State Bar, discussed in note 65 *supra*, a lawyer who reviews ESI produced pursuant to a public records request, as opposed to produced pursuant to a discovery request, likely may not search for or use any confidential information embedded in the metadata associated with the ESI.

copies of a public record is not required to "disclose the purpose or motive for the request."[142] It also potentially poses an added cost or burden on the public sector litigant. Consequently, it places additional pressures on a public agency to settle the litigation.

142. G.S. 132-6. A special provision applies, however, to requests for copies of geographical information systems databases and data files developed and operated by counties and cities. "As a condition of furnishing an electronic copy, whether on magnetic tape, magnetic disk, compact disk, or photo-optical device, a county or city may require that the person obtaining the copy agree in writing that the copy will not be resold or otherwise used for trade or commercial purposes." G.S. 132-10.

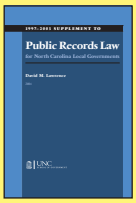
Conclusion

The management of electronic information, generally, has become increasingly complex. That complexity is no more apparent than when an organization must cull through vast amounts of electronic information to find, preserve, and retrieve potentially relevant data pursuant to civil discovery obligations. Although largely ignored by organizations until they face actual litigation, the burdens of complying with e-discovery requirements can be onerous and the costs exorbitant.

Further complicating the process is the fact that some court rules, including those that apply in North Carolina federal courts, have been amended to specifically address e-discovery, whereas others, including those that apply in North Carolina state courts, have not. Additionally, as technology constantly changes, litigants are presented with ever new challenges in applying the rules, even the amended rules, to the discovery of ESI. In many cases, however, strategic use of the rules by litigants will serve to contain at least some of the costs and burdens of litigating in the digital age.

Kara A. Millonzi is Assistant Professor of Public Law and Government at the School of Government. She specializes in municipal and county finance law, special assessments, utility finance law, solid waste finance law, and public school finance law.

OTHER SCHOOL OF GOVERNMENT PUBLICATIONS



Public Records Law for North Carolina Local Governments
1997 book and 2003 cumulative supplement
David M. Lawrence
A new edition of this book is forthcoming in 2010.

Open Meetings and Local Governments in North Carolina: Some Questions and Answers
Seventh edition, 2008
David M. Lawrence

County and Municipal Government in North Carolina
2007
Edited by David M. Lawrence

***Digital Government Innovation Bulletin #2004/02*, "How Public is Too Public? Property Records Availability on North Carolina County Government Web Sites"**
June 2004
Henrietta H. Presler
www.sog.unc.edu/pubs/electronicversions/pdfs/dgib0402.pdf

***Digital Government Innovation Bulletin #2004/01*, "Ensuring Services Availability: Seven Steps to Continuity of Government Operations"**
February 2004
Thomas Foss
www.sog.unc.edu/pubs/electronicversions/pdfs/dgib0401.pdf

***Digital Government Innovation Bulletin #2003/01*, "The Move Toward Online Government Services"**
July 2003
Mary-Maureen Brown
www.sog.unc.edu/pubs/electronicversions/pdfs/dgib0301.pdf

Order School of Government publications online: www.sog.unc.edu
Contact the Sales Office: sales@sog.unc.edu or 919.966.4119

2009.16
978-1-56011-631-8