WARD AND SMITH, P.A.
ATTORNEYS AT LAW

iHeadache: The Incorporation Of Metadata Into Discovery In Litigation And Its Impact On You

Written By **Allen N. Trask, III** (ant@wardandsmith.com)
January 8, 2013

An Electronic Twist on a Traditional System

It is no secret that we live in an increasingly electronic world. Whether we are checking email on our smartphones, firing up our satellite-powered GPS for a road trip, tweeting our latest 140-character update to the social media world, or videoconferencing over VOIP systems, seemingly every move we make involves electronics. And although we have an adaptable legal system designed to be flexible enough to follow societal change, the law is a relative latecomer to the electronic party. Lawyers are notoriously old-fashioned and certainly shoulder their fair share of the blame for the slow-to-market acclimation of the law to this new digital world. But perhaps even more importantly, the very laws and rules that govern the practice of law have struggled to adapt to and incorporate the numerous facets of the digital age.

The Way Things Were

Storing records in the past was a relatively straightforward process, ruled by the fact that records were a tangible item. These tangible records were simply kept in paper form in hard files. The image of shelves upon shelves stacked with rows of brown accordion files containing pages and pages of white paper is a familiar, if not nostalgic, memory. The process for destroying a document was similarly simple. If a document needed to be destroyed, the process involved little more than a pair of scissors, a fireplace, or, for the very fancy, a shredder. This all seems painfully simple in hindsight, but remembering these warm details of the past just serves to highlight their contrast with the present and future of file storage and destruction.

The Way Things Are

As society and more and more individuals and businesses move to a "paperless" world, file management quickly is changing wholesale due, in large part, to the explosion in the amount of stored material. No longer does a contract simply consist of the paper on which it is written. Now that very same contract consists, at a minimum, of a word processing document, complete with layers upon layers of often unknown electronic information such as creation date, author, tracked changes, comments regarding various versions by various readers and reviewers, original kilobyte size, file storage location, and file path data, just to name a few. And to make matters even more complicated, this example stops short of mentioning other electronic files so often associated with electronic documents, such as emails, which themselves are laden with the same or similar additional electronic data. All of this data is stored somewhere, often on a hard-wired system like a server, in online repositories, or in some other type of system. No matter where the data is stored, the amount is staggering. This creates potential problems both for storing the data and for destroying it. The simple deletion of an electronic file itself does little to address the veritable mountain of data associated with that file.

As a result, the storage and destruction policies and rules of the past are not always relevant to the new and improved electronic file creation and storage environment in which we live. In the past decade, legislatures and court systems around the country, including here in North Carolina, have begun addressing these issues by implementing changes to the rules that govern the legal system. These systematic changes have a very real, and in some situations immediate, impact on North Carolina individuals and businesses.

One of the most important areas impacted is litigation and is centered on the "discovery" process. While litigation certainly, and thankfully, does not affect every individual and business, it is better, and often cheaper, to be prepared for it than to be caught unaware. The purposes of this article are to explain how the legal system has changed for litigants, to highlight some of the potential pitfalls associated with the attempts to adapt the legal system to the digital age (including "metadata," what it is, why it is important, and how it impacts the North Carolina resident and business owner), and to explore the potential ramifications of the failure to consider the implications on day-to-day recordkeeping policies and actions.

From Discovery to eDiscovery

Good Intentions

Discovery is nothing more than a formal, structured exchange of documents and information between and among parties in litigation. The law requires parties in litigation to disclose their records, documents, information, and testimony to opposing parties prior to a trial. The original intent of broad discovery requirements is easily understood: the encouragement of pre-trial resolution of litigation matters and the discouragement of ambush, "gotcha" gamesmanship at trial which tended to elevate theatrics over truth-finding.

The idea was that if parties are forced to exchange all of the facts about a case before a trial, then the legal position of the parties should be clearer to all and resolution should be more forthcoming. For example, if a party is forced to disclose a document that shows that party's improper behavior, that party may be far more inclined to resolve litigation over that behavior. In that case, everyone benefits from a cost perspective.

The Law of Unintended Consequences

Unfortunately, the effort to foster full and complete disclosure has resulted in the exponential increase in the scope, complexity, and costs of litigation. Broad discovery has created an environment where attorneys are expected to turn over every possible stone, not only in their initial investigations of cases, but also throughout the litigation process. To complicate matters further, there are significant and appropriate professional obligations that require such thoroughness. As a result, discovery has become tedious, time-consuming, and generally excessive in breadth and is lamented by clients, attorneys, and judges alike. Indeed, since the vast majority of civil cases are resolved before trial, discovery is often the single most expensive phase of litigation. It is important to remember that this fact had been recognized as an unfortunate consequence prior to the rise in the prevalence of electronic records. The rise in the volume of electronic records has served only to exacerbate this problem and to give rise to a host of other problems.

The Rules

While each state and the federal courts have different rules governing their discovery processes, discovery in North Carolina court cases is governed by the North Carolina Rules of Civil Procedure. At the heart of all discovery is the definition of "discoverable information." The scope of what information must be disclosed has been relatively broad since the inception of discovery. Discoverable information typically includes things such as relevant records and documents and the names and addresses of persons with knowledge, or who might have knowledge, of the allegations and facts of the case and who might be able to give testimony about case

events. Prior to recent changes, this definition of discoverable information in the North Carolina Rules of Civil Procedure did not directly address electronic data and, therefore, electronic data was not at the forefront of the discovery process.

Effective October 1, 2011, however, the definition of "discoverable information" was amended in North Carolina to include "electronically stored information" ("ESI"). At first glance, one would think that this is a reasonable addition to discovery designed to keep the process relevant in the information age. If a paper document must be disclosed in discovery, then it would seem to make perfect sense that the electronic file from which that document was printed also should be disclosed.

But the definition of ESI does not stop with just the electronic document or file. Remember all of those layers of electronic data associated with every file? The North Carolina General Assembly certainly did, and it took the definition of ESI one step further by including "reasonably accessible *metadata*."

At the risk of losing you by using a new "term of electronic art" to remember (yes, file "metadata" right up there with "the cloud," "tweet," "vlog," and whatever new term hits the " web" tomorrow), metadata is a term with which all North Carolina residents and business owners should become familiar. Metadata is not only something that litigants may have to address in litigation, but it also is something that all individuals and businesses should begin to manage in the regular course of their day-to-day activities. You are free to do much more to limit the amount of discovery that you can be compelled to disgorge before you have a hint of a lawsuit than you can after you should have noticed the "hint."

Wait, What is Metadata and Why Should I Care?

Although a more complete definition of metadata follows, the short and sweet of it is that metadata is an oft-hidden trail of electronic information that leads to or from an electronic file. The North Carolina General Assembly's addition of metadata to the scope of discoverable information means that litigants have, with some limitations, a means now to acquire this metadata. However, with the right planning and preparation, you and your business may be able to avoid potential litigation-related problems created by this trail of information.

The Tall Task of Defining Metadata

Trying to find a specific, simple, and concrete definition for metadata is tantamount to trying to define pornography. IT professionals may know metadata when they see it (or maybe not), but what about the rest of us? There certainly is a collective concept, at least in the technological community, about what metadata is, but even a brief survey of the term returns a multitude of different definitions applicable to different situations. The most commonly accepted general definition appears to be that metadata is "data about data." More specifically, metadata is electronic information that either is created automatically as part of the electronic process or is input manually by the user or creator of the electronic information.

Metadata generally consists of three types:

- Descriptive – Descriptive metadata describes things such as the subjects the record is about, the party to whom the record pertains, or the record's creator;
- Structural (or system) – Structural metadata is the more technical form of metadata and includes such things as data about format, styling, processing, encryption, and authentication; and,
- Administrative – Administrative metadata pertains to data such as ownership, access rights and restrictions, usage history, and even copyrights.

Regardless of the type or kind of metadata, the common theme, and the most important thing to remember,

is that all metadata provides *searchable information* related to the electronic item at issue. This searchable information often allows people or software to locate electronic records or other items in a database and to learn more about the electronic file.

A very simple and routine example is where an online record storage program requires the creator of a record to disclose the creator's identity before a record is created. Obviously, that identification can be used later to search for and locate that record. A slightly more complex example involves searchable information created and stored about the history of a record, such as the date and time of modifications to, or access of, a record and the identity of the person who made the modification or accessed the record (or at least the user whose computer was used to modify or access the record). In addition, a record can be located based on the date it was created or its particular location in the database, each of which is an item of metadata that may be created and attached to the record electronically or automatically without any direct input from the user.

While plenty of metadata is simply a byproduct of the electronic process, several types of metadata provide numerous and clear benefits to the end user. Electronic data systems are more easily and efficiently organized for the benefit of all users, companies are able to track employee efficiency by checking the creation and modification history of a particular file, and there is an additional avenue for full or partial recovery of "unsaved" or "crashed" electronic files, just to name a few.

Metadata Minefield

Unfortunately, and as is often the case, the good comes with the bad. Like so many other things in life, there are unintended consequences that accompany metadata. Taking together the "turn over every stone" approach to discovery and the fact that metadata is now discoverable by opposing litigants, it is impossible for one to ever imagine all of the complications that may be associated with the discovery of data that we often do not even know exists. Things such as author history, formatting history, fonts, templates, hidden text, comments, graphics, hyperlinks, and even personal information all are now items that may be inadvertently disclosed by parties in litigation. To understand this "metadata minefield," it is prudent to take a look at the actual changes to the law in North Carolina.

The North Carolina General Assembly's full amendment of the ESI definition defines "electronically stored information" to include "reasonably accessible metadata that will enable the discovering party to have the ability to access such information as the date sent, date received, author, and recipients." The General Assembly also included a qualifier which states that "[t]he phrase does not include other metadata unless the parties agree otherwise or the court [so] order[s.]" This definition is amorphous at best. Instead of defining specific types of metadata to be included in discovery, the General Assembly points only to metadata that will lead to certain types of information. This leaves significant room for interpretation, with the result being that at least some attorneys almost certainly will issue broad requests in an attempt to capture all "reasonably accessible metadata" as defined in the amendment.

In the case of email, the effect of the amendment on discoverable information is relatively obvious. Frankly, all of the referenced information, metadata or not, is right there on the printed email for everyone to see. However, in the case of an electronic file that has not been sent or received, the issue becomes more complicated. For instance, it would seem that a party may request, using the "author" portion of the new ESI definition, that the producing party hand over the metadata associated with the creation of internal records and documents that have never been emailed or otherwise disclosed. This may or may not have relevance to the matter at hand in litigation.

Another example of unintended consequences involves one of the most common and beneficial forms of metadata: track changes. This is an incredibly useful feature that appears in nearly all word processing

programs and is a regular part of drafting and revising documents. Track changes provide an easy, legible way to "red-line" documents and the changes can be saved to capture the cumulative benefit. By the same token, the *problem* is that each entry, revision, and comment is stored somewhere in the document or database. Simply turning off the "track changes" feature and "cleaning up" the document by accepting or rejecting changes are often not enough to remove the track changes history from the document. So metadata not only keeps track of each and every time that a particular document has been modified or even viewed, and by whom, but it also stores the actual changes themselves. Horror stories abound about users amending documents in track changes and turning the feature off before saving and sending, only to have the recipient open the document and use the document's metadata to see all the changes made. Sometimes this is intended; other times, it is not. Even if the track changes are not disclosed unintentionally, those very track changes may be sought by an opposing party in litigation.

These are just a very few examples of the many lingering questions and a portent of questions to come surrounding the inclusion of metadata, and ESI generally, in discovery. These types of questions will have to be worked out as the new rules are applied by the trial courts and interpreted by the appellate courts. Regardless, the time for individuals and businesses to take notice of and address this issue is now. Even though the specifics of the rules have not been finalized, and attorneys have not made full use of the new rules in litigation, there is no reason why individuals and businesses cannot and should not take a proactive approach now.

Steps to Take Now

Enormous amounts of information are input into, and generated by, electronic systems each day. To require that an individual or business be able to produce each piece of that information would be utterly unreasonable. Nevertheless, and outside of the fact that the information may have to be disclosed to an opposing party, there are two primary areas of concern:

- Court-imposed sanctions for failure to provide ESI; and,
- Consequences associated with "spoiling the evidence."

Luckily for individuals and business owners, and in tandem with the amendment to the definition of discoverable information, the rule pertaining to sanctions for failure to comply with discovery requests was also amended to account for the normal day-to-day use of electronic systems. Specifically, this amendment states that:

> Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of routine, good-faith operation of an electronic information system.

This additional amendment appears to offer individuals and businesses not only a way to manage metadata, but also a way to avoid issues with the doctrine of "Spoliation of Evidence." Moreover, since the definition of ESI includes "reasonably accessible metadata," this amendment appears to apply to metadata as well. The inference here is that a court will not punish computer users for things done in the ordinary course of their business.

This amendment will have a yet unknown effect on the doctrine of "Spoliation of Evidence." In North Carolina, there is no "tort" for destroying, or "spoiling," evidence. However, if a party can show that another party has "spoiled" evidence, then that party is entitled to an evidentiary inference and a jury instruction that the evidence destroyed would have injured the case of the party who destroyed the evidence. In other words, if a party is shown to have destroyed evidence, then the presumption is that the evidence destroyed would have

hurt that party's position in the lawsuit at hand. This doctrine can apply to either individuals or businesses when document retention policies have not been followed.

A party can avoid the consequences of destroying evidence by offering a fair, frank, and satisfactory reason for not being able to produce it. Thus, the amendment above seems to offer an out on spoliation of ESI, so long as the ESI (including metadata) was destroyed as the result of a routine, good-faith operation of an electronic information system (read: not clicking the delete button in the "uh, oh" moment just after receiving a summons).

Although nothing is certain at this stage, this companion amendment may give individuals and businesses the ability to customize their electronic programs and data storage and file management policies and procedures in ways that may minimize the storage of potentially harmful metadata. Programs that store less metadata can be purchased, developed, and implemented. Archiving practices can be adopted that address the storage of metadata. These steps should be evaluated with input from both IT personnel and attorneys who can provide advice as to the electronic and legal benefits and drawbacks. For example, it is already common for businesses to use programs that cleanse metadata from documents prior to sending via email. But while that may be good general practice, it could pose potential problems if the cleansing goes deeper than just the document sent.

In any event, taking a proactive approach in advance of litigation, or even the threat of litigation, will ease the potential future hassle and expense of discovery and the possible negative ramifications of the disclosure of certain information should litigation ever ensue.

Conclusion

The reach of the addition of ESI to the litigation discovery process extends far beyond the scope of this article. But it would be folly to overlook the potential pitfalls tied to the discovery of metadata hidden in our electronic systems. While no one looks forward to litigation, all individuals and business owners must plan for just that possibility and the tedious process of discovery; it is simply an unfortunate reality of modern-day life.

As is often the case, proper planning before litigation occurs can save significant costs and stress if it ever does occur. Attorneys will always have various tools to fight the production of information in discovery, but it would be wise to take action to protect you or your business long before those tools ever enter the picture.

--