'Discovery' in the United States

Melinda F. Levitt

1st November 2011

INTRODUCTION

Perhaps one of the most controversial - and disdained - aspects of the legal system in the United States is the very broad and extensive concept of 'discovery' in civil lawsuits. In short, the U.S. system permits parties to a civil lawsuit, most commonly through their lawyers, to self-conduct, without the immediate supervision of a judge, the direct collection of information and documents from an opposing party - with the opposing party being required to respond to interrogatories, requests for documents, and requests for admissions. For persons or businesses who are not a party to the lawsuit - that is, they are neither a plaintiff nor defendant - the same result can be achieved by way of subpoena, which is a type of court order, but one issued by the attorneys and not judges, and pursuant to which the non-party must provide requested documents. Both parties and non-parties are also subject to being called to 'testify' at a deposition, which is conducted entirely by lawyers without the participation of a judge. Failure to respond properly to discovery requests, or failure to appear and testify meaningfully at a deposition, subjects the non-complying party to court

About The Author

Melinda F. Levitt is a partner with Foley & Lardner LLP, where she is a member of the firm's Antitrust, Privacy, Security & Information Management and International Practices. Melinda's practice focuses on complex commercial litigation, including the areas of antitrust, securities, intellectual property and class action defense work in matters pending before federal and state courts, as well as various federal agencies.
Melinda has developed particular experience in complex electronic discovery and obtaining discovery from companies abroad. She co-authored an article titled "California's E-discovery Rules: US and Non-US Impact" which was published in Data Protection Law & Policy (September 2009) and in E-Commerce Law & Policy (August 2009), as well as an article exploring remote email privacy issues, which was published in E-Commerce Law Reports (October 2009).

mlevitt@foley.com

sanctions, including monetary fines, a requirement to pay the opposing party's attorneys' fees, or evidentiary sanctions that serve to limit a party's ability to pursue or defend against a law suit. Put plainly, the discovery system in the United States must be taken very seriously and cannot be ignored.

Prior to the advent of the mass electronic data and communications era, the U.S. discovery process was onerous enough - requiring a party (or a subpoenaed non-party) to go through the tedious process of locating, collecting and providing (known as 'producing') 'all' documents for a defined period of time in the producing party's possession on the broad topics set forth in the other side's document requests. When the world communicated by way of the written word on paper, this process, while demanding, was manageable given that the volume of paper documents retained and archived by most people or companies was relatively limited. In the electronic age, where the volume of written communications via email, text messages, 'tweets', etc. has skyrocketed to levels previously unimaginable - and where such 'documents' are regularly retained for long-periods of time, or are recoverable from computer system 'back up tapes,' document archives, individual hard-drives, and system-wide, multi-user, dynamic databases, the demands of complying with discovery requests have substantially increased and the financial costs have risen dramatically. Moreover, for those concerned with issues of data control and management, as well as privacy considerations, the challenges today can be extraordinarily difficult. Thus, 'e-discovery' has become the most controversial aspect of discovery under the U.S. system, with lawyers and judges alike grappling on how to adapt rules originally designed for the world of paper to the new and constantly evolving electronic age.

THE BASIC LEGAL FRAMEWORK

The rules governing discovery in the United States, in the federal courts, are set forth in the Federal Rules of Civil Procedure - a compilation of procedural rules that are adopted by the U.S. Congress. Each of the individual states have discovery rules and systems that are very similar to the federal rules and, thus, the federal rules and the judicial opinions

interpreting them serve as a general guidepost for discovery issues under both the federal and state legal systems.

1. The Scope of Discovery is Very Broad

The Federal Rules of Civil Procedure contain twelve rules specifically addressed to discovery practices. Rule 26(b) explains that the scope is broad, stating that 'Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claims or defenses . . . . Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.' Fed. R. Civ. P. 26(b)(1) (emphasis added). This language has been interpreted by countless judges to permit and approve extremely broad requests for information and documents. Typical examples may be:

All documents, for the period January 1, 2007- April 17, 2011, referring or relating to prices, pricing plans, pricing policies, pricing trends, pricing conditions, competitive prices, and price studies, whether or not commissioned by the company, relating to the sale of widgets: a) in the United States; b) in North America; and c) all other non-North American foreign countries.

All documents, discussing, communicating or otherwise referring to the Company's decision in 2008 to modify its design of widgets, including the reasons therefore, any drawings or technical designs associated with that decision, all testing of any modified designs and all meetings concerning modifications approved or rejected by the Company's management.

All documents relating to any injuries allegedly suffered and sustained while utilizing a widget manufactured by Company X, including all medical records, all photographs, all records of treatments received, including physical therapy or similar types of therapies, and all documents regarding devises purchased arising from any such injuries

(such as wheelchairs, walkers, mobile scooters, etc.)

While the latter request may be more manageable given it is directed at an individual, the first two sweep very broadly and reach to every email, memorandum (and every draft), every Excel spreadsheet, every PowerPoint and every other type of 'document' throughout the company that has been retained either in hard copy paper or electronically. As discussed below, although there are means by which either the parties can negotiate limitation or the courts can intervene to limit overly broad requests, depending on the suit, it is possible that millions of electronic records may need to be collected and provided to the opposing party.

2. Depositions, Interrogatories and Document Requests

The three typical types of discovery requests are addressed by Rules 30, 33 and 34.

a. Depositions

Rule 30 sets forth the rules relating to the taking of a deposition, which is conducted under oath - i.e., the same or very similar oath administered in court whereby the deponent/witness swears under penalty of perjury to tell the truth. The deponent is then questioned by the opposing counsel and, except in limited situations, is required to answer all questions posed - and even if the deponent's attorney (who also is present) lodges objections on the record to the questions being asked, the deposition continues and the deponent is required to respond. The questions and answers are transcribed by a court reporter who administered the oath. In addition, it has become very common today for depositions to be videotaped such that there is both a written transcript and a video of the deposition, the latter of which allows for the tone of the responses to be captured and the demeanor of the witness to be recorded. Rule 30 initially limits each party to 10 deposition, with no one deposition to exceed 7 hours or one day; however, exceptions are regularly made for complex cases.

Rule 30(b)(6) allows for a deposition to be directed at a business entity (e.g., a corporation or partnership) or a government agency, where the requesting party seeks a representative from the business (or government) who can testify knowledgeably about and bind the company on the topics set forth in the deposition notice. For each such topic, the business must designate an officer, director or managing

person (or anyone else as long as that person consents to testify) who will testify about the requested subjects and, if necessary, produce multiple people to speak on different topics. Thus, while a particular designated deponent may not be able to respond thoroughly to all topics, the company is obligated to designate and prepare someone from the company to address each of the listed topics. Failure to do so can result in court ordered sanctions against the non-complying business.

b. Interrogatories

Rule 33 deals with written interrogatories, which are a series of written questions with the receiving party required to provide full and complete answers. As with all discovery, the subject matters of the interrogatories may be very broad in terms of subject matter and scope. Moreover, under Rule 26(e), a party is required to 'seasonably' amend or update those responses to the extent that further investigation or discovery reveals additional responsive information. Written objections may be made - and usually are made - to interrogatories. Nonetheless, an obligation remains to respond to the best of the person's or business's ability and such responses are usually made with the prefatory qualifying language 'Without waiving these objections, Company X responds that it first developed the design for its advanced XE model widget in 2006, with the following people contributing to that design effort . . . .' Interrogatory answers are required to be signed by the responding party and, essentially, certified as to their truthfulness.

In lieu of providing a complete written response to each interrogatory, Rule 33 permits the responding party to respond by producing documents where a review of those documents will provide a response 'and the burden of deriving or ascertaining the answer will be substantially the same for either party.' Fed. R. Civ. P. 30(d).

c. Requests for the Production of Documents

As indicated above, the most difficult and controversial aspect of U.S. discovery today relates to requests for the production of documents under Rule 34. Under this rule, the requesting party serves on the opposing party a series of 'requests' on a wide range of topics relating to the law suit for which documents 'relating' thereto are required to be produced. In 2006, the Federal Rules specifically were amended to recognize that the term 'document' includes 'electronically stored information' - known as 'ESI.' This change was made in recognition of the fact that individuals and businesses had moved away from recording information on paper, and instead had moved to an electronic means of

communication, as well as electronic systems for document storage, archiving and retrieval.

The term 'ESI' is not given a precise definition in the Federal Rules.

The wide variety of computer systems currently in use, and the rapidity of technological change, counsel against a limiting or precise definition of electronically stored information. . . . Rule 34(a)(1) is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments.
Fed. R. Civ. P. 34 advisory committee's note to 2006 amendments.

The concept of 'documents' and 'ESI' under Rule 34 is broad enough to include non-written language means of communications. Hence, document requests can require the production of voice-mail messages that have been retained - or future retained messages. Electronically stored photographs also are regarded as 'documents' - as are essentially any type of record created and retained electronically.

Rule 34 also requires that ESI be produced in the form in which it is usually ordinarily maintained or in a reasonably usable form. Thus, while in the early years of electronic communications, parties would locate and literally print out to 'hard copy' paper the emails from a person's computer, the norm today is to produce electronic documents in electronic form - with sufficient metadata provided such that the receiving party can sort the documents by date, author, recipients, etc. Likewise, ESI is most commonly produced with the documents having been 'Tiffed' and 'OCRed' - meaning that they are in a 'tagged image file format' such that they appear to the reader in a format similar to the format of the original document and have been subjected to an optical character recognition software program such that the entire text of the document is 'word searchable.' Receiving the documents in an electronic, word searchable format allows the receiving party to search through an entire collection of electronic documents - which often number into the hundreds of thousands or even millions of pages - to locate, for example, those documents containing only certain words or phrases or documents prepared or received by certain persons within a specific date range.

More recently, there has been a movement to push for the production of documents in 'native' format - i.e., an exact, dynamic copy of the 'live' document as it exists on the original computer system where it was located. The desire for native production has made some headway in terms of electronic spreadsheets and other types of complex electronic documents that are dynamic in their original forms, such as PowerPoint presentations, where there can be certain levels of animation or other advanced visual features. Because Tiffed images are static and not dynamic, a Tiffed image of an electronic document does not allow the document to be manipulated, which means that, for example, the reader cannot 'drill down' to examine particular data cells or rearrange the data. The production of native format documents, however, raises various concerns because by providing a native, 'live' document, the reader can literally change the document - inadvertently or intentionally - thereby raising questions about what information was contained in the true original versus data that might have been altered by the reader. See, e.g., In re Netbank, Inc. Securities Litigation, 259 F.R.D. 656, 681 (N.D. Ge. 2009) (granting request for native format production despite hypothetical possibilities of alteration of documents and other problems associated with native production versus Tiff images).

d. Sanctions and Special Issues

Rule 37 grants the courts authority to sanction a party or a non-party for failures associated with discovery. Such failures can include inadequate responses to interrogatories or document requests, failure to appear at a deposition, or failure otherwise to cooperate in discovery. In the case of ESI, Rule 37 provides a 'safe harbor' provision, which states that sanctions may not be imposed, absent exceptional circumstances, for failure to provide electronically stored information 'lost as a result of the routine, good-faith operation of an electronic information system.'

1. The Duty to Preserve and Sanctions for Spoliation

Although Rule 37's 'safe harbor' for ESI provides some comfort, in reality courts have very high expectations in terms of parties' abilities to avoid the loss of ESI information and have sanctioned parties, either under

Rule 37 or the court's inherent authority, for failing to meet those expectations. Specifically, litigants in the United States have an obligation to preserve documents, including ESI materials, and as one very influential judge has explained, 'once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold.'' Zubulake v. UBS Warburg, 220 F.R.D. 212, 218 (S.D.N.Y 2003) (seminal opinion) (emphasis added).

In short, based on numerous court decisions that have emerged over the last few years, once a person or a business begins to plan to file a lawsuit, or a person or business reasonably expects to be named as a defendant in a future lawsuit, an immediate obligation arises to suspend normal procedures and practices relating to the routine destruction of documents and ESI and to 'preserve' documentation likely to be relevant to the lawsuit. The same obligations arise when a subpoena is served on a non-party. In such situations, it is expected that a 'litigation hold' notice will be sent to, at a minimum, the employees of the portion(s) of a business that is involved in the subject matters of the lawsuit. The notice typically informs the employees that until further notice they are to cease deleting or altering documents that relate to the topics of the lawsuit (or the subpoena). Moreover, a company's IT department must become involved to ensure, for example, that routine document purge protocols are suspended, that sufficient electronic storage space is available to employees so that they can both cease deleting emails and other documents and continue to work on their computers into the foreseeable future; and, that, if necessary, at least some level of computer 'back-up' tapes are preserved so that deleted information may be recovered. Likewise, a company's IT department often is requested to take and retain 'snap shots' of back-up tapes and databases in order to preserve the information that existed as of the date of the snap-shot so that a 'base line' reference point of data and information exists in the event that information is lost or deleted in the future.

The exact contours of any preservation obligation and the steps necessary to meet those obligations will depend on the nature of the case, the involved entities' computer systems, and the ability of counsel for both sides to negotiate acceptable parameters. That said, the entire

issue of preservation - and the 'spoliation' of documents that were not preserved but should have been - has resulted in numerous court decisions over the last three or so years, with substantial monetary sanctions issued for intentional or grossly negligent failures to preserve documents properly. See, e.g., Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497 (D. Md. 2010) (imposing more than $1 million in attorneys' fees and costs for willful spoliation); Kevin Keithly v. The Home Store.com, Inc., 2008 WL 3833384 (N.D. Cal. 2008) (sanctions of $650,000 for discovery abuses and spoliation of documents). Other courts have emphasized that the severest of sanctions should not be imposed where the destruction of documents was negligent, but not willful and/or the prejudice to the opposing party was not sufficiently great. Rimkus Consulting Group v. Cammarata, 688 F. Supp.2d (S.D. Tex. 2010) (detailed analysis).

In addition to - or in lieu of - monetary sanctions, courts may award evidentiary sanctions, including adverse jury instructions where, for example, the jury is informed about the destruction of documents and is instructed to presume that the documents destroyed would have supported the other side's case, or where the jury is instructed to presume certain facts as true even though no documentary evidence is presented to support such a conclusion. See e.g., E.I. Du Pont de Nemours and Co. v. Kolon Industries, 2011 WL 296682 (E.D. Va. July 21, 2011). Similarly, a judge may order that the party that destroyed documents will not be permitted to present evidence on certain topics to counter the other party's evidence. Moreover, for the most egregious of situations, i.e., where the spoliation was undertaken in bad faith and/or in a deliberate manner to deprive the other side of important information relevant to the law suit, and where the other side was substantively prejudiced by the loss of the information, the judge may order the severest of sanction whereby the case is either dismissed (if the spoliator is the plaintiff) or award judgment to the other party. See e.g., Micron Technology v. Rambus, 2011 WL 1815975 (Fed. Cir. May 13, 2011) (reversing trial court's decision to enter judgment in Micron's favor for Rambus's spoliation in order for trial court to examine degree of bad faith and prejudice in more detail). See also generally Pension Comm. Of Univ. of Montreal Pension Plan v. Banc of Am. Sec. LLC, 685

F. Supp.2d 456 (S.D.N.Y 2010) (seminal decision discussing preservation obligations, spoliation and sanctions considerations).

2. Protection of Attorney-Client Communications and Attorney Work Product Materials

Under the U.S. legal system, a privilege is granted to confidential communications between an attorney and the client, as well as the attorney's work performed on behalf of a client in anticipation of and during the course of litigation. These privileges - i.e., the attorney-client privilege and the work product doctrine - when asserted mean that such privileged or protected documents need not be produced in discovery, even if they address issues relevant to the litigation. Likewise, a person being deposed or a witness at trial need not testify about confidential communications with that person's (or that business's) attorney relating to the litigation. However, the general rule is that if the privileged/protected communication is given or revealed to a third-party, the privileged status is deemed waived and the information may be used in the pending litigation (or otherwise). Moreover, in the case of the attorney-client privilege, waiver of a single document or piece of information often results in what is as known as 'subject matter waiver' - that is, all other documents or information relating to the same topic as the initial communication deemed waived also are no longer considered privileged and must be provided in discovery.

While determining the exact contours of the attorney-client privilege or documents protected under the attorney work-product doctrine can be difficult enough (and is a subject beyond the scope of this Practice Note), one of the biggest challenges facing litigants in the United States today is locating and withholding privileged documents from large-scale electronic document productions undertaken pursuant to Rule 34. Because of the fear of potential waiver, in particular on a 'subject matter' basis, parties' counsel involved in litigation find themselves expending extraordinary amounts of time and effort - at their client's expense - in searching for and locating documents entitled to privileged protection.

Recognizing the challenges, burdens and 'fear factor' associated with reviewing thousands or millions of pages of electronic documents for privileged communications, in 2008, Federal Rule of Evidence 502 was amended such that an inadvertent disclosure of a privileged communication will not result in waiver if reasonable steps had been undertaken to prevent disclosure and the producing party takes reasonable steps to rectify the error. Fed. R. Evid. 502(b). One such typical 'reasonable step' is to send to the opposing party notice of the inadvertent production promptly after its discovery and a request to 'claw-back' the inadvertently produced documents. Under Rule of Civil Procedure 26(b)(5)(B), upon receipt of such a notice, the receiving party must promptly return, sequester or destroy the documents and any copies thereof and, if the receiving party disputes whether the documents are privileged, must promptly make an application to the court for a decision. Rule 502 also allows for the parties to enter into 'claw-back' agreements and seek for the court to recognize such an agreement by way of an order.

Since the adoption of the new rule, the issue has become what constitutes reasonable steps to prevent disclosure or to rectify the error, with some courts setting very high bars. See, e.g., Mt. Hawley Insurance Co. v. Felman Production, 271 F.R.D. 125 ((S.D.W. Va. 2010) (numerous and sophisticated steps taken pre-production to identify privileged documents among very large collection of documents; court determined that such steps were inadequate and found waiver of privilege). Other courts are more forgiving. See, e.g., Kandel v. Brothers Int'l Corp., 683 F. Supp.2d 1076 (C.D. Cal. 2010).

3. Non-Privileged Confidentiality and Privacy Concerns

Because the U.S. discovery system requires the production of documents and information to an adversary, including very typically information about a company's day-to-day operations, its financial performance, its long-term strategic planning, its product development goals, its human relations records, and other such matters, business parties to litigation are anxious to ensure that such information is not widely disseminated or used to their competitive disadvantage. The same concerns arise

when an individual is required to provide information and documents about, for example, his or her medical history, finances, property, etc.

To address these circumstances, Federal Rule of Civil Procedure 26(c)(1) allows for the issuance of a Protective Order by the court, whereby '[t]he court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression or undue burden or expense.' The Protective Order may entirely forbid that the discovery take place, may limit the permitted topics to certain subjects or may limit dissemination of the information to the parties and their attorneys only (as opposed to allowing the wide dissemination of the information to, for example, the press - as is otherwise permitted). Indeed, in the case of highly sensitive business or personal information, a Protective Order may provide that certain information may only be seen on an 'Attorneys Eyes Only' basis, meaning that while the parties' lawyers may see the documents, the parties themselves may not have access to them or be told of their contents during the discovery phase of the litigation.

In light of the sensitivity - or potential sensitivity - of information exchanged in discovery, as well as the high volume of ESI documents exchanged, courts often have standard protective orders and parties regularly seek such an order from the court as part of the discovery process.

Documents that are protected as confidential under a protective order are filed 'under seal' with the court, to the extent that they are used to support a pretrial motion seeking a determination by the court on a particular issue. However, it should be understood that merely because a party declares a document, or some aspect of the information in the document, to be confidential, the other party can challenge that designation and seek to have the document 'unsealed.' Moreover, because there is a very strong presumption of the public's right of access to judicial proceedings, once a case moves to the trial stage, documentary exhibits - even those marked 'confidential' during discovery - will become part of the open, public record, with exceptions made for only the most sensitive of materials such as a true trade secret whereby, for example, a business's technology has not been disclosed through a

patent or some other means.

On the issue of personal privacy, as a general matter, individuals using a company issued computer or other electronic communication devise have limited privacy rights to personal emails or documents on those systems. Although U.S. courts have found some exceptions to exist, the general view is that when the computer is owned by the company, and the company clearly has notified employees that it retains the right to review and examine all communications made on its systems, the individual should not expect there to be a protected privacy zone around that person's personal emails or documents. See, e.g., In re Reserve Fund Sec. & Deriviative Litig., 2011 WL 2039758, 09-MD 2011, 09-Civ-4346 (S.D.N.Y May 23, 2011) (emails between husband and wife exchanged from husband's employer's computer not entitled to protection); Holmes v. Petrovich Dev. Co., 109 Cal. App. 4th 1047 (Cal. App. Jan. 13, 2011) (communications with employee's attorney sent over employer's computer system not privileged).

One new area relating to privacy concerns relates to information posted by an individual on social networking sites such as Facebook. A few recent cases have ordered a party to produce (or otherwise provide to the opposing party) full access to the private portions of the party's Facebook and/or MySpace pages, reasoning that a self-declared 'privacy' designation did not shield that information from discovery. See, e.g., McMillen v. Hummingbird Speedway, Inc., 2010 Pa. Dist. & Cnty. Dec. LEXIS 270 (Jefferson Co. Com. Pl. 2010); Romano v. Steelcare, Inc., 907 N.Y.S.2d 650 (Suffolk Co. 2010).

ADDITIONAL STATUTORY PROVISIONS ON ELECTRONIC COMMUNICATIONS

In addition to the Rules of Civil Procedure, there are federal statutes that implicate the ability of other parties or the government to obtain electronic documents that exist or are stored on an internet service provider's ('ISP') system. Unfortunately, the existing statutory scheme dates back to 1986, when the concept of mass electronic communications was in its infancy. However, based on recent legal

decisions, as well as significant developments in communications norms and options, there are efforts underway in the U.S. Congress to amend the existing statutes to bring them into line with the significant developments in electronic communications over the last 25 years.

In 1986, the U.S. Congress adopted the Electronic Communications Privacy Act, which has several parts, including the Stored Communications Act ('SCA') (18 U.S.C. §§ 2701-12) and the Wiretap Act (18 U.S.C. §§ 2510-22). Under the Wiretap Act, a document is in 'electronic storage' where it is held on a temporary basis incidental to subsequent electronic transmission (i.e., the addressee of the email) or where it is stored for purposes of backup protection. 18 U.S.C. §2510(17).

Under the SCA, a party may not seek, pursuant to a subpoena, to obtain from an ISP (such as Microsoft) a person's electronic communications where the ISP merely holds that information in 'electronic storage' for back-up purposes and is not the primary repository of the communication. See Theofel v. Farney-Jones, 359 F.3d 1066 (9th Cir. 2004) (subpoena issued in civil litigation to other party's ISP provider unlawful under the SCA). Rather, in such a case, the party must seek the information directly from the person (or the business).

As to the government, under the SCA, it must obtain a search warrant issued by judge if it wishes to obtain from an ISP the contents of a wire or electronic communication that is in electronic storage for one-hundred and eighty days or less. In such cases, it is not required for the government to give the subscriber notice of this effort. If the communication is older than 180 days, the government need only proceed by way of an administrative subpoena to require the ISP to produce the subscriber's communications; however, in such a case, the subscriber is to be given advance notice. Similarly, a warrant is not necessary where the government is seeking to obtain from an ISP any electronic communication that is held or maintained on a remote computing service 'solely for the purpose of providing storage or computer processing services to [the] subscriber.' Moreover, at least one U.S. court has found that remote, web-based ISP services such a

hotmail.com or gmail.com account do not merely serve as a 'storage' repository for purposes of back-up, but act essentially as the primary repository of electronic communications - meaning that such web-based email accounts fall outside of the definition of 'electronic storage' found in the Wiretap Act and that the government need not obtain a search warrant to obtain access to these materials and may proceed simply by way of a subpoena. United States v. Weaver, 2011 WL 2163478 (C.D. Ill. July 15, 2009); but see Jennings v. Jennings 697 S.E.2d 671 (S.C. App. 2010).

The future impact of these decisions has been called into question by an important recent decision of the United States Court of Appeals for the Sixth Circuit. In the case of United States v. Warshak, 2010 WL 5071766 (6th Cir. Dec. 14, 2010), the court specifically held that people legitimately have an expectation of privacy in their email communications, even if stored on an ISP's system, and that the Fourth Amendment to the U.S. Constitution, which protects against unreasonable 'search and seizure' by the government, precludes the government from obtaining a person's email by way of a subpoena on the ISP and that 'the government may not compel a commercial ISP to turn over the content's of a subscriber's emails without first obtaining a warrant based on probable cause.' Id. at *14.

In summary, in light of recent legislation efforts to amend the SCA and related statutes, and the Sixth Circuit's Warshak decision, the legal landscape concerning electronic communications, and the privacy rights afforded to such communications is likely to change in the near future.