

SOMEONE’S WATCHING: PROTECTING PRIVILEGE ON BOTH SIDES OF THE TABLE DURING ELECTRONIC DISCOVERY

*Christopher N. George**

I. INTRODUCTION

Discovery is a critical part of successful litigation. Cases are shaped by the parties’ available documents and aspects of trial preparation such as depositions and interrogatories. Electronic discovery currently is gaining importance in litigation. Through electronic discovery, a discovering party now has the ability to search computer files for keywords, dates, names, and other criteria.

Litigation cases involving patents and other technology are prime candidates for the use of electronic discovery due to the sophistication of the parties, the high stakes and litigation costs involved, and the likelihood that many documents produced in tangible form originate from electronic files, such as word processing documents or spreadsheets. Non-privileged e-mails and software codes are also frequent targets of discovery requests.

Electronic documents (“e-documents”) can be produced via printed production, electronic production (e.g., on compact disc), or on-site inspection. In many cases, the large volume of data precludes printed production. Because neither party may want to bear the expense of production, the producing party may prefer an on-site inspection to lower costs because this method reduces the amount of time and resources to produce the documents.

Much discussion recently has arisen regarding the waiver of privilege from inadvertent disclosure when producing e-documents.¹

* J.D., *cum laude*, University of Illinois College of Law, 2002. Mr. George is an associate with McAndrews, Held & Malloy, a full-service intellectual property law firm in Chicago. He welcomes any feedback via e-mail at cgeorge@mhmlaw.com.

1. See, e.g., John T. Hundley, “Inadvertent Waiver” of Evidentiary Privileges: Can Reformulating the Issue Lead to More Sensible Decisions?, S. ILL. U. L.J. 263, 263 (1995); David J.

One part of the debate over electronic discovery centers on protecting privileged attorney–client communications and work product from accidental production during on-site inspection of e-documents, such as e-mails.² Exposure of electronic evidence most definitely affects the integrity of the discovery process. There is also the possibility of spoliation of the documents by electronic manipulation or deletion. However, the debate has not yet addressed the issue of inadvertent waivers when the party that is making documents available for inspection monitors computer activity as the opposing party inspects its electronic files. For example, if the producing party is monitoring only lightly and does not notice that the opposing party saw a privileged e-document, has it made an inadvertent waiver even though it was ignorant of the mistake?

Often overlooked are the issues of privilege that are intertwined in electronic searches and its strategies, search terms used, and documents of interest identified in the search. Instead, courts generally have focused on the issue of maintaining and preserving electronic evidence, while ignoring the related issue of monitoring someone’s inspection of electronic evidence. Perhaps this oversight occurs because many attorneys, clients, and judges are not aware of the relative ease with which commands and keystrokes typed at a computer can be recorded or monitored by software running in the background.³

This Essay discusses the similarities and differences between traditional and electronic discovery, and also reviews the privileges protecting attorney–client communication and attorney work product. The Essay then provides some suggestions for both practitioners and courts designed to protect the privileges and rights of both parties involved in discovery, particularly in document production and inspection. For example, diligent use of protective orders and highly confidential “attorneys’ eyes only” exchanges of electronic discovery can protect the confidentiality of the producing party and preserve the discovering party’s freedom to conduct discovery and develop a strategy for the litigation. Hopefully a discussion of the possibilities and ramifications will raise awareness of potential pitfalls and obligations introduced by electronic discovery practice.

Stanoch, “Finders . . . Weepers?” *Clarifying a Pennsylvania Lawyer’s Obligations to Return Inadvertent Disclosures, Even After New ABA Rule 4.4(B)*, 75 TEMP. L. REV. 657, 659–61 (2002).

2. See, e.g., Carl Pacini et al., *Accountants, Attorney–Client Privilege, and the Kavel Rule: Waiver Through Inadvertent Disclosure via Electronic Communication*, 28 DEL. J. CORP. L. 893, 893–902 (2003); The Sedona Conference Working Group on Electronic Document Retention and Production, *The (2004) Sedona Principles: Best Practices, Recommendations and Principles for Addressing Electronic Document Production*, 5 SEDONA CONF. J. 151, 162–63 (2004); Ken M. Zeidner, *Inadvertent Disclosure and the Attorney–Client Privilege: Looking to the Work-Product Doctrine for Guidance*, 22 CARDOZO L. REV. 1315, 1318–22 (2002).

3. See, e.g., Eltima Software’s Powered Keylogger, at <http://www.mykeylogger.com/keystroke-logger/powered-keylogger/> (last visited Feb. 9, 2005); Google Directory, Monitoring, at http://directory.google.com/Top/Computers/Security/Products_and_Tools/Monitoring/ (last visited Feb. 9, 2005); Keylogger.org, at <http://www.keylogger.org/> (last visited Feb. 9, 2005).

II. THE RIGHT TO DISCOVERY AND INSPECTION OF “DOCUMENTS AND THINGS”

Traditional discovery of documents and other tangible materials during litigation has given rise to a vast array of case law and statutes at both the federal and state levels. Electronic discovery and the right to inspect e-documents introduce issues that are not present in traditional paper-based discovery. It is now much easier to monitor and record a discovering party's activities via computers than it is through labor-intensive on-site paper discovery. In addition, the default configurations of computer systems can be designed to track a command or even keystroke histories.⁴ In such a situation, a party's search strategies, search terms, and the identified documents themselves are laid bare for the opposing party to view. Thus, the protections provided by the work product doctrine and attorney–client privilege can be circumvented.

A. Traditional Discovery

Rule 26 of the Federal Rules of Civil Procedure provides methods for obtaining discovery, including “production of documents or things or permission to enter upon land or other property under Rule 34 or 45(a)(1)(C), for inspection and other purposes.”⁵ Additionally, Rule 26(c) provides for protective orders “which justice requires to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense.”⁶ Courts may make an order in cases in which: (1) “the discovery may be had only on specified terms and conditions”; (2) “discovery [should] be conducted with no one present except persons designated by the court”; and (3) “a trade secret or other confidential research, development, or commercial information [should] not be revealed or be revealed only in a designated way.”⁷

Rule 34 of the Federal Rules of Civil Procedure provides a party in a lawsuit with the right to inspect “documents and things.”⁸ Since 1970, the courts and Congress have interpreted “documents and things” to

4. Information Technology Systems and Services, Stanford University, UNIX Command Summary, at <http://unix-docs.stanford.edu/unixcomm.html> (last modified Oct. 5, 2004).

5. FED. R. CIV. P. 26(a)(5).

6. FED. R. CIV. P. 26(c).

7. FED. R. CIV. P. 26(c)(2), (5), (7).

8. FED. R. CIV. P. 34.

include “data compilations.”⁹ Rule 34 allows a party to request production of data compilations and other documents or to request entry upon land for inspection of documents and things within the scope of Rule 26(b).¹⁰ Rule 34 gives a party the right to inspect and copy, test, or sample documents and things, including data compilations.¹¹

B. Electronic Discovery

As discussed above, Rules 26 and 34 provide the right to inspect documents and things, including e-documents and data. Electronic data include materials such as saved documents (e.g., word processing or database documents), backup or archive files, e-mail messages, and deleted or residual data.¹² The right to inspect extends to electronic data on site.¹³ However, issues about this type of inspection still remain regarding confidentiality, privacy, and access to trade secrets by the opposing party.

An increasing number of federal district and appellate courts have made decisions regarding demands for electronic discovery, forms of production, and the burden of costs associated with the production. Courts have ordered physical production of e-documents, electronic production of e-documents, and on-site access to the producing party’s computers for examination of the e-documents.¹⁴ In these decisions, courts have often performed a cost-shifting analysis to determine which side should bear the financial burden for production.¹⁵ Although the producing party traditionally is ordered to bear costs, the current

9. FED. R. CIV. P. 34(a) advisory committee notes. The committee’s notes explain: The inclusive description of “documents” is revised to accord with changing technology. It makes clear that Rule 34 applies to electronic 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. In many instances, this means that respondent will have to supply a print-out of computer data Similarly, if the discovering party needs to check the electronic source itself, the court may protect respondent with respect to preservation of his records, confidentiality of nondiscoverable matters, and costs.

Id.

10. FED. R. CIV. P. 34(a).

11. *Id.*

12. *See Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 316–17, 318–20 (S.D.N.Y. 2003).

13. FED. R. CIV. P. 34(a).

14. *See, e.g., Zubulake*, 217 F.R.D. at 324; *see also infra* notes 19 and 23.

15. In *Zubulake*, the court examined the cost-shifting analysis for electronic discovery. *Zubulake*, 217 F.R.D. at 316. The court examined the eight-factor cost-shifting analysis of *Rowe Entm’t, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421, 429 (S.D.N.Y. 2002), and formulated a new seven-factor test:

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, compared to the amount in controversy;
4. The total cost of production, 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 issue at stake in the litigation; and
7. The relative benefits to the parties of obtaining the information.

Zubulake, 217 F.R.D. at 322.

solution for balancing the broad scope of discovery with cost implications for both parties is to shift costs to the requesting party.¹⁶

On-site access to the producing party's computer system is often the least expensive but most intrusive option. Additionally, on-site inspection could allow the discovering party to access software tools and other resources such as special software debugging or translation programs used by the producing party to view certain e-documents, such as software source code. By using the producing party's tools to inspect e-documents while on site, the discovering party can reduce or eliminate the need to purchase expensive software tools for itself. Courts have begun to allow such on-site inspection, but frequently shift costs to the discovering party in such instances.¹⁷

Producing parties are often reluctant to allow a competitor or its representatives to access an internal computer network. Such hesitation stems from the parties' desire to protect trade secrets and other confidential information vital to business that often reside on a company's computers. Because of this fact, courts have emphasized the importance of proper safeguards or restrictions when a discovering party is accessing a producing party's computer system.¹⁸

Some courts have even allowed parties to access files located on personal or home computers, in addition to the company's computers, if such computers had been used for business purposes.¹⁹ In *Simon Property Group v. mySimon, Inc.*, the court appointed an expert to retrieve the desired data from the home computers of the defendant's main executives, rather than allowing the plaintiff to personally examine the defendant's personal computers.²⁰ In *Playboy Enterprises v. Welles*, the court weighed the benefit and burden of electronic discovery according to Federal Rule of Civil Procedure 26(c) in allowing retrieval of a "mirror image" of the defendant's hard drive pursuant to a protective order.²¹ Such discovery was obtained at the plaintiff's expense.²² Other courts have given the producing party such options as downloading and producing data electronically, loaning necessary

16. *Id.* at 316 (discussing the desire for courts to balance the broad scope of discovery in Fed. R. Civ. P. 26(b)(1) with the cost-consciousness of Fed. R. Civ. P. 26(b)(2)).

17. *Id.* at 320.

18. See *Bills v. Kennecott Corp.*, 108 F.R.D. 459, 462 (C.D. Utah 1985) (stating that responding parties are hesitant to "open up their computer banks for inspection pursuant to discovery requests" due in part to the "lack of expertise on the part of parties and their lawyers in computer technology and data processing"); *Strasser v. Yalamanchi*, 669 So. 2d 1142, 1145 (Fla. Dist. Ct. App. 1996) (finding a likelihood of irreparable harm in allowing plaintiff unrestricted on-site access to defendant's entire computer system without proper access restrictions and defined parameters of time and scope).

19. See *Simon Prop. Group v. mySimon, Inc.*, 194 F.R.D. 639, 640-43 (S.D. Ind. 2000) (granting plaintiff's motion to produce electronic versions of documents and make certain home computers available for inspection); *Playboy Enters. v. Welles*, 60 F. Supp. 2d 1050, 1053-55 (S.D. Cal. 1999) (holding that plaintiff could have access to defendant's personal hard drive because defendant used her personal computer for both business and personal communications).

20. *Simon Prop. Group*, 194 F.R.D. at 641; see also *Playboy Enters.*, 60 F. Supp. 2d at 1055.

21. *Playboy Enters.*, 60 F. Supp. 2d at 1054.

22. *Id.*

software to the opposing party for discovery, or providing on-site access for inspection of the producing party's computers.²³

III. THE PROTECTED PRIVILEGES

Privileges have been defined primarily by common law to prevent a party's use of certain evidence in order to protect the other party's interest or relationship of outstanding importance.²⁴ Two commonly cited privileges are the attorney-client privilege and the work product doctrine. While both privileges likely are to be relied upon in most civil cases, the scope of each varies, as illustrated below.

A. Attorney-Client Privilege

Federal courts and the common law recognize a privilege against disclosing confidential communications between lawyer and client.²⁵ Generally, the privilege also extends to experts employed to assist counsel in providing legal services, but not to an expert hired to testify at trial.²⁶ Documents, including e-documents, exchanged between the lawyer and the client are also covered by the privilege when created to provide legal services.²⁷ However, only the communications, not the underlying factual circumstances, are protected from discovery.²⁸

B. Work Product Doctrine

The work product doctrine in civil litigation protects materials prepared for anticipated or current litigation.²⁹ Federal Rule of Civil Procedure 26(b)(3) provides that a party may only obtain "discovery of documents and tangible things . . . prepared in anticipation of litigation or for trial" by an attorney or agent of an opposing party upon a showing that the party seeking discovery has "substantial need of the materials in the preparation of the party's case and that the party is unable without undue hardship to obtain the substantial equivalent of the materials by other means."³⁰ The work product doctrine instructs the court to protect

23. See *Sattar v. Motorola, Inc.*, 138 F.3d 1164, 1171 (7th Cir. 1998). The court required the producing party, which had initially produced the information on inaccessible tapes, to: (1) download the data onto computer disks or a hard drive, (2) loan the other party a copy of the necessary software, or (3) allow the other party on-site access to its own system. *Id.*

24. Federal Rule of Evidence 501 provides that "the privilege of a witness . . . shall be governed by the principles of the common law as they may be interpreted by the courts of the United States in the light of reason and experience." FED. R. EVID. 501 and Report of House Committee on the Judiciary (No. 93-650).

25. FED. R. EVID. 501 Report of House Committee on the Judiciary.

26. 6 JAMES WM. MOORE ET AL., MOORE'S FEDERAL PRACTICE § 26.80[1][a], [2] (3d ed. 1999).

27. RESTATEMENT (THIRD) OF LAW GOVERNING LAWYERS § 87(f) (1998).

28. 6 MOORE ET AL., *supra* note 26, § 26.49[1].

29. See, e.g., FED. R. CIV. P. 26(b)(3) advisory committee notes; *Hickman v. Taylor*, 329 U.S. 495, 509-11 (1947).

30. FED. R. CIV. P. 26(b)(3).

against disclosure of the “mental impressions, conclusions, opinions, or legal theories of an attorney or other representative of a party concerning the litigation.”³¹ Search terms and search strategies used in electronic inspection of documents could reveal the mental impressions and legal theories used by a party and, therefore, may also be protected.

IV. VIOLATIONS OF THOSE PRIVILEGES

As discussed previously, electronic discovery has been legitimized through statutes and case law as an extension of traditional paper-based discovery. Thus, parties have the right to inspect e-documents to develop their legal strategies and theories of a case. However, allowing opposing counsel access to a party's facilities to inspect e-documents introduces complexities not encountered in traditional document review. For example, due to the relative ease of recording commands and keystrokes entered at a keyboard, “electronic eavesdropping” has become a new issue.

A. *Related Case Law*

A lawsuit involving electronic keystroke or command monitoring by an opposing party during discovery has yet to generate any published opinions. However, two analogous lines of case law involving traditional discovery practices may provide a useful comparison.

In the first scenario, the opposing counsel of a party who secretly recorded witness conversations requested that those recordings be made discoverable.³² The counsel who made the recordings argued that they were privileged because of the work product doctrine.³³ The court ruled that the recordings were not protected by privilege because the work product doctrine does not protect the unethical conduct of attorneys.³⁴ In this line of cases, sanctions were seldom requested and rarely imposed, probably because the disclosure of the recordings themselves was an adequate remedy.

In the second scenario, one counsel intentionally attempted to view privileged information of the opposing counsel.³⁵ This attempt to improperly view privileged information was met with discipline and dismissal of the lawsuit by the court.³⁶ In this line of cases, the sanctions

31. *Id.*; see also 6 MOORE ET AL., *supra* note 26, § 26.70[2][c].

32. See *Parrott v. Wilson*, 707 F.2d 1262, 1271 (11th Cir. 1983); see also *Ward v. Maritz, Inc.*, 156 F.R.D. 592, 599 (D.N.J. 1994); *Bogan v. Northwestern Mut. Life Ins. Co.*, 144 F.R.D. 51, 56 (S.D.N.Y. 1992); *Moody v. Internal Revenue Service*, 654 F.2d 795, 800 (D.C. Cir. 1981).

33. *Parrot*, 707 F.2d at 1271.

34. *Id.* at 1272.

35. See *Perna v. Elec. Data Sys. Corp.*, 916 F. Supp. 388 (D.N.J. 1995).

36. See *Perna*, 916 F. Supp. at 400–03 (holding that deliberate acts to gain unauthorized access to documents warrants dismissal, irrespective of whether the wrongfully viewed documents were privileged); *Lipin v. Am. Nat'l Red Cross*, No. 93 Civ. 1334, No. 92 Civ. 4455, 1996 U.S. Dist. LEXIS

depended on factors such as the egregiousness of the breach, the effect of the breach on the case, and the deterrence value of the possible sanctions.³⁷ Arguably, secretly recording keystrokes while an opposing attorney is investigating discoverable e-documents is analogous to improperly viewing or stealing privileged information of the opposing counsel because it reveals clues as to his or her strategy.

B. *Electronic Eavesdropping*

Electronic “eavesdropping” can become an issue when, for example, producing parties electronically monitor the searches done on their computers by the party seeking discovery during on-site inspections. The Electronic Communications Privacy Act (“ECPA”) includes protection for electronic communications, in addition to traditional wire or oral communications.³⁸ The ECPA prohibits “intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication.”³⁹ Violators of this provision shall be subject to fines and/or imprisonment.⁴⁰ In addition, the ECPA provides that “[n]o otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.”⁴¹ The significance of electronic eavesdropping or monitoring will be discussed further in the Analysis section.

C. *Keystroke and Command Logging*

Courts are currently struggling with the balance between protecting the private rights of individuals and allowing the government to use invasive modern search technology—including devices that record keystrokes—during criminal investigations of potential felons.⁴² *United States v. Scarfo* was the first case to take on this issue after the FBI used a keystroke-logging system, installed per a valid warrant, to secretly record the password for encrypted files of a suspected loan shark.⁴³ Although the loan shark’s motion to suppress the evidence collected via keystroke logging was denied, the district court noted, “[W]e must be ever vigilant against the evisceration of Constitutional rights at the hands of modern

396, at *25, 26 (S.D.N.Y. Jan. 17, 1996) (stealing the other party’s clearly marked privileged documents resulted in a dismissal); *Furnish v. Merlo*, No. 93-1052-AS, 1994 U.S. Dist LEXIS 8455, at *28 (D. Or. June 8, 1994) (removal of privileged documents from opposing counsel warrants an *in camera* review to determine the appropriate remedy).

37. *Perna*, 916 F. Supp. at 398.

38. Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2522 (2000).

39. *Id.* § 2511(1)(a).

40. *Id.* § 2511(4)(a).

41. *Id.* § 2517(4).

42. *United States v. Scarfo*, 180 F. Supp. 2d 572, 574–76 (D.N.J. 2001).

43. *See id.* at 574.

technology.”⁴⁴ While the government can rely on national security concerns to justify keystroke monitoring in some cases under the 1980 Classified Information Procedures Act⁴⁵ or the ECPA,⁴⁶ these justifications typically are not relevant in a lawsuit between private parties.

Keystroke-logging tools and other activity-monitoring software are readily available in the marketplace and can be programmed by skilled system administrators.⁴⁷ Logging and history software can be used with multiple operating systems. Some operating systems, such as UNIX, have built-in commands that allow a user to retrieve a log of recently executed commands.⁴⁸ With all the current technology, commands executed on a computer, words or commands typed within an application or document, and other user activity can be monitored by software installed by the producing party on a computer being used by the party seeking electronic discovery.

V. ANALYSIS

How can opposing parties keep their privileged materials and strategies from being revealed during on-site inspection of e-documents? For the producing party, encryption and password protection are examples of techniques that can be used to protect privileged e-mail and other confidential e-documents unrelated to discovery requests in the current litigation. For the party seeking discovery, however, such safeguards cannot protect the search commands and keystrokes executed during an on-site inspection. Therefore, other steps must be taken to address the privilege concerns of both the discovering party and the producing party.

The American Bar Association has stated that “attorneys should not ‘record any conversation whether by tapes or other electronic device . . . without the consent or prior knowledge of all parties to the conversation’ because such conduct is deceitful.”⁴⁹ Additionally, the Model Rules of Professional Conduct prohibit “dishonesty, fraud, deceit, or misrepresentation” and “conduct that is prejudicial to the administration of justice.”⁵⁰ Secretly recording opposing counsel’s keystrokes, and thereby “endeavoring to foreclose a person’s choice to speak ‘on the record’ without actually providing the person with information to intelligently exercise that choice, is therefore inherently deceitful

44. *Id.* at 583. Note that the district court proceeded to point out, “[I]t is likewise true that modern-day criminals have also embraced technological advances and used them to further their felonious purposes.” *Id.*

45. Classified Information Procedures Act, 18 U.S.C. app. III §§ 1–15 (2000).

46. 18 U.S.C. §§ 2510–2521 (2000).

47. *See, e.g.*, sources cited *supra* note 3.

48. *See supra* note 4.

49. ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 337 (1974).

50. MODEL RULES OF PROF’L CONDUCT R. 8.4(c)–(d) (2003).

because the practice obtains information through trickery.”⁵¹ Additionally, federal and state wiretapping statutes prohibit unlawful interception of wire, electronic, or oral communications.⁵² Selection and compilation of documents by counsel in preparation for pretrial discovery has been protected by the work product privilege.⁵³ The undisclosed access and use by opposing counsel of that work product should not be permitted by the courts.⁵⁴

The primary argument to justify withholding access to e-documents and for electronically monitoring the opposing party’s on-site activities is usually the sensitivity of the e-documents. However, every party has information that is confidential and sensitive, and discovery would never proceed if a party were allowed to completely withhold relevant information based on its sensitivity.⁵⁵ “[T]here is no absolute privilege for trade secrets and similar confidential information.”⁵⁶ Consider the particular sensitivity of computer software codes, which could pertain to business practices of the party beyond the scope of the current litigation. A producing party may object to e-discovery of its software code and will have the burden to show that such code is a trade secret and that disclosure of it would be harmful.⁵⁷ If disclosure of the trade secret is relevant and necessary to the action, it nonetheless should be disclosed.⁵⁸ Such relevancy is “construed more broadly during discovery than at trial.”⁵⁹

Monitoring or logging of keystrokes at a computer allows a producing party to essentially view privileged attorney communications by the reviewing party, often those from collaboration with the opposing party’s agent or expert who is consulting during discovery. Keystrokes and executed commands allow the monitoring party to become privy to the search strategies, keywords, and important documents identified by the opposing party. Because review of the keystroke or command log can provide extensive insight into the strategy and analysis of the opposing party, it should be prevented as a violation of attorney–client or work product privilege.

51. *Anderson v. Hale*, 202 F.R.D. 548, 556 (N.D. Ill. 2001).

52. *See, e.g.*, Electronic Communications Privacy Act, 18 U.S.C. § 2510 (2000); Illinois Eavesdropping Statute, 720 ILL. COMP. STAT. 5/14-1 to -9 (West 2000); *see also supra* Section IV.B.

53. *Sporck v. Peil*, 759 F.2d 312, 316 (3d Cir. 1985).

54. *See Perna v. Elec. Data Sys. Corp.*, 916 F. Supp. 388, 400 (D.N.J. 1995) (condemning unauthorized access to opposing counsel’s documents).

55. *See Atkins v. S. Cent. Bell Tel. Co.*, 744 F.2d 1133, 1136 (5th Cir. 1984). “Confidential information is produced in lawsuits all the time. Should the District Court deem it necessary, a protective order may be used to safeguard the confidentiality of [the information].” *Id.*

56. *Centurion Indus. Inc. v. Warren Steurer & Assocs.*, 665 F.2d 323, 325 (10th Cir. 1981) (quoting 8 CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 2043 (2d ed. 1994)).

57. *Id.* at 325.

58. *Id.* at 325–26.

59. *Id.* at 326; *see also* 8 WRIGHT & MILLER, *supra* note 56, § 2008.

VI. CONCLUSION

While a reviewing party has the right to request and inspect documents and evidence while protecting its own work product, a producing party has the right to protect its own work product as well as confidential information unrelated to the pending litigation. Parties may confer and ask the court to enter a protective order to safeguard the confidentiality of their materials. A court may also provide a remedy for a breach of the protective order, including sanctions, declaratory judgment, or dismissal of the lawsuit.⁶⁰

For on-site inspections of e-documents of the producing party's own computer system, the existence of the work product doctrine, attorney-client privilege, and possible protective orders should satisfactorily protect confidential information. Keystroke logging or otherwise recording a discovering party's activities is like electronic eavesdropping and violates the party's right to inspect. Limits may be placed on electronic discovery due to the burden of maintaining and producing electronic data, but the limits should not facilitate monitoring or eavesdropping. Counsel's ethical and professional obligations, as well as sanctions threatened by the court under a protective order, should provide the proper incentive for a reviewing party to avoid viewing content that it is not entitled to inspect. Furthermore, in response to an e-document request, the computer system administrator or other agent of the producing party may duplicate the relevant documents and copy them to a secure location within the system. In other words, the reviewing party will be able to view the documents in an "electronic area" apart from the regular system that the opponent uses and relies upon in business.

As an alternative to on-site inspection, the producing party could use "electronic production," where the e-documents are provided by disk (e.g., a mirror image of a hard drive or copy of a requested database or software code) to the requesting party pursuant to a protective order. Electronic production of the documents eases the burden on the producing party because an electronic copy or forwarding of files would eliminate the costs of printing the documents. Electronic production also alleviates the producing party's concern that the discovering party may view areas of the producing party's computer system that are privileged or unrelated to the lawsuit. Furthermore, by providing a separate electronic copy of the documents to opposing counsel, he or she may review the documents without being unnecessarily constrained by the schedule of the producing party and without imposing his schedule on the producing party.

In conclusion, courts and attorneys should carefully consider the wording of protective orders and agreements surrounding examination of

60. See FED. R. CIV. P. 26(c), 37(b)(2).

e-documents prior to the commencement of discovery in litigation. Allowing production of e-documents by disk, imaging a drive, or providing access to duplicate files in a restricted area of a party's computer system should help protect the analysis and inspection efforts of the discovering party, as well as secure against unwanted intrusion by the discovering party. Protective orders must include significant penalties to make them a viable threat against dissemination of the produced data. Allowing the return of inadvertently produced privileged materials without automatically declaring the mistake a waiver of privilege may also help to protect the confidentiality of the producing party. Parties and the courts must be aware of all the issues surrounding electronic discovery and the clear potential for abuse during the discovery process because electronic discovery is becoming increasingly prevalent in modern litigation.