6-1-2005

V. The Impact of Electronic Discovery on Privilege and the Applicability of the Electronic Communications Privacy Act

Sasha K. Danna

Recommended Citation
Available at: https://digitalcommons.lmu.edu/llr/vol38/iss4/5

This Developments in the Law is brought to you for free and open access by the Law Reviews at Digital Commons @ Loyola Marymount University and Loyola Law School. It has been accepted for inclusion in Loyola of Los Angeles Law Review by an authorized administrator of Digital Commons@Loyola Marymount University and Loyola Law School. For more information, please contact digitalcommons@lmu.edu.
V. THE IMPACT OF ELECTRONIC DISCOVERY ON PRIVILEGE AND THE APPLICABILITY OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT.*

Electronic discovery raises a range of issues in the area of privilege law that have challenged courts and litigants alike. When a propounding party seeks to obtain large volumes of electronic data in discovery, one of the biggest concerns for the producing party is the protection of privileged communications. This Part addresses a number of problems that a litigant must resolve in developing a discovery plan that safeguards the integrity of privilege claims. Part V.A. sets out the legal framework applicable to privilege claims and examines how it has been applied in the context of electronic discovery. Section V.B. discusses the types of privilege claims that litigants have raised in electronic discovery, focusing particularly on the attorney-client privilege and the work product doctrine. Part V.C. identifies the threat that the unique characteristics of electronic data pose to privilege protection and summarizes the traditional and innovative approaches proposed by litigants and courts to avoid waivers of privilege. Part V.D. analyzes the impact that electronic discovery may have on the five factors applied by a majority of courts to determine the effect of an inadvertent disclosure of privileged communications.

Finally, this Part addresses the applicability of the Electronic Communications Privacy Act (ECPA) to electronic discovery. Part V.E. discusses the different interpretations of the ECPA and the extent to which the privacy of litigants is protected under each. It also hypothesizes how the ECPA may influence litigants in their use of emerging electronic discovery tools.

*Sasha K. Danna: J.D. Candidate, May 2006, Loyola Law School; B.A., Art History and Italian Language and Literature, Smith College, June 1998. I wish to thank the staff of the Loyola of Los Angeles Law Review, particularly the Developments Editors, for their hard work and guidance. I would also like to thank my parents for their love and support and my siblings for their wit. I dedicate this Part to my husband, Giacomo Gallai.
A. Legal Framework for Privilege in Electronic Discovery


Although the Federal Rules of Civil Procedure (FRCP) were created before the advent of electronic data systems, they nonetheless provide an adequate framework within which to resolve many of the issues that arise in the context of electronic discovery. Generally, the FRCP contemplate broad discovery; however, the discovery that a civil litigant is permitted to seek is subject to some limitations. In fact, FRCP 26(b)(1) restricts a party's right to obtain discovery to "any matter, not privileged, which is relevant to the claim or defense of the party." This language provides for the categorical exemption from discovery of matters that do not meet the applicable

1. See Williams v. Owens-Illinois, Inc., 665 F.2d 918, 933 (9th Cir. 1982) ("[D]iscovery requests relating to the computer... should be processed under methods consistent with the approach taken to discovery of other types of information."); Medtronic Sofamor Danek, Inc. v. Michelson, 56 Fed. R. Serv. 3d (West) 1159, 1161 (W.D. Tenn. 2003) (setting out the scope of discovery as governed by FED. R. CIV. P. 26(b)(1), the limitations of discovery as governed by FRCP 26(b)(2)(i)-(iii) and asserting that "[e]lectronic information, if relevant, generally is discoverable under these same guidelines."); Jones v. Goord, No. 95 CIV. 8026, 2002 WL 1007614, at *6 (S.D.N.Y. May 16, 2002) ("The [FRCP] albeit for the most part drafted in an earlier era, deal perfectly well with the problems occasioned by discovery of electronic 'documents'."); Indiana Coal Council v. Hodel, 118 F.R.D. 264, 266 n.3 (D.D.C. 1988) ("That a computer system is at issue here does not require application of different discovery principles."); see also Cornel Research Found., Inc. v. Hewlett Packard Co., 223 F.R.D. 55, 73 (N.D.N.Y. 2003) ("Rule 34 permits discovery of electronically or digitally stored information."); Anti-Monopoly, Inc. v. Hasbro, Inc., No. 94CIV.2120, 1995 WL 649934, at *1-2 (S.D.N.Y. Nov. 3, 1995) (noting the application of Rule 34 to computerized data); Daewoo Elecs. Co. v. United States, 650 F.Supp. 1003, 1006 (Ct. Int'l Trade 1986) ("[I]nformation which is stored, used, or transmitted in new forms should be available through discovery ...."); FED. R. CIV. P. 34 advisory committee's note.

2. Jones, 2002 WL 1007614, at *1. The court in Jones commenced its opinion by stating that "[b]road discovery is a cornerstone of the litigation process contemplated by the Federal Rules of Civil Procedure." Id. However, the court acknowledges that discovery is limited by the principles of relevance and privilege. Id. at *6; see also Medtronic, 56 Fed. R. Serv. 3d (West) at 1161 (considering a request for production of electronic data and noting that "discovery does have 'ultimate and necessary boundaries'")

standards of relevance, as well as those matters deemed to be privileged, even if they do satisfy the relevance requirement.⁴

Because the FRCP do not expressly enumerate the privileges entitled to protection under federal law, FRCP 26(b)(1) depends for its meaning on Federal Rule of Evidence (FRE) 501, which provides that "the privilege of a witness, person, government, State or political subdivision thereof 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."⁵ This rule has been construed to warrant the preservation of privileges existing at common law, while at the same time providing the courts with some degree of discretion to recognize new privileges.⁶ Nonetheless, courts will only recognize a new privilege where it would advance fundamental public policy objectives which override the presumption in favor of discoverability.⁷ Once a party asserts a privilege that is

⁴ In addition to the categorical limitations on discovery created by Rule 26(b)(1), the Federal Rules also endow federal courts with broad discretion to limit discovery under the following circumstances:

(i) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit taking into account the needs of the case, the amount in controversy, the parties’ resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.

⁵ FED. R. EVID. 501; see Von Bulow v. Von Bulow, 811 F.2d 136, 141 (2d Cir. 1987) (indicating that "[t]he principles by which a federal court determines whether material sought [under Rule 26(b)(1)] is privileged are set forth in Fed. R. Evid. 501").


⁷ See Jaffe, 518 U.S. at 9 (cautioning that "[e]xceptions from the general rule disfavoring testimonial privileges may be justified . . . by a 'public good transcending the normally predominant principle of utilizing all rational means
contested by an opposing party, federal courts apply these two rules to determine whether the matter sought to be discovered falls within a federally recognized privilege, and, if so, to hold that such matter is immunized from discovery.\textsuperscript{8}

A party claiming a privilege as to a paper or electronic document has the initial burden of establishing that the matter sought to be protected does in fact qualify as privileged.\textsuperscript{9} Under the FRCP, a party is empowered to protect his or her evidentiary privilege and is allowed to "withhold[] information otherwise discoverable under [the] rules" by claiming that it is privileged or subject to protection as trial preparation material.\textsuperscript{10} In doing so however, "the party shall make the claim expressly and shall describe the nature of the documents, communications, or things not produced or disclosed in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the applicability of the privilege or protection."\textsuperscript{11}

2. Legal Framework Applied

While many courts have long operated under the assumption that the FRCP apply to the discovery of electronic media, fewer have

\textsuperscript{8} See Cornell Research Found., Inc. v. Hewlett Packard Co., 223 F.R.D. 55, 59 (N.D.N.Y. 2003) ("Rule 34 permits discovery of electronically or digitally stored information provided, of course, that it meets the relevance test articulated in the rules governing pretrial discovery and there is no other proper basis [such as privilege] for denying or restricting the discovery sought.").

\textsuperscript{9} See Streamline Capital, L.L.C. v. Hartford Cas. Ins. Co., No. 02 Civ.8123 PKC MHD, 2005 WL 66898, at *1 (S.D.N.Y. Jan. 11, 2005) (assessing whether e-mail messages were privileged, the court noted that "the party invoking the privilege bears the burden of proving each element of the factual basis for that privilege claim and must do so by competent evidence"); Long v. Anderson Univ., 204 F.R.D. 129, 134 (S.D. Ind. 2001) (clarifying in a dispute over the discoverability of an e-mail that defendants, "[a]s the parties seeking to establish the privilege, . . . bear the burden of demonstrating that all of the requirements for invoking the attorney-client privilege have been met").

\textsuperscript{10} FED. R. CIV. P. 26(b)(5).

\textsuperscript{11} Id.
specifically announced this principle.\textsuperscript{12} In addition to expressly declaring that the FRCP govern electronic discovery, \textit{Jones v. Goord}\textsuperscript{13} represents one of the first cases to systematically apply FRCP 26 and FRE 501 to a privilege dispute over electronic data.\textsuperscript{14} In \textit{Jones}, the court addressed a discovery dispute involving electronic media in a class action suit filed by prison inmates against the New York Department of Correctional Services, contesting the conditions of confinement.\textsuperscript{15} After producing over 700,000 pages of documents, the defendant opposed the plaintiff's motion to compel production of the defendant's electronic database.\textsuperscript{16} The defendant claimed that the database contained prison personnel and inmate files that were subject to a qualified, if not full privilege, based on prison security concerns.\textsuperscript{17} The defendant further argued that the confidentiality of the electronic files could not be adequately safeguarded by any existing or conceivable protective order.\textsuperscript{18}

In deciding whether to grant the protective order, the court first cited FRCP 26(b)(1) for the proposition that irrelevant or privileged

\textsuperscript{12} The United States Supreme Court applied the FRCP to a discovery request for electronic data as early as 1978. See Oppenheimer Fund Inc. v. Sanders, 437 U.S. 340, 362 (1978); see also Playboy Entm't., Inc. v. Wells, 60 F. Supp. 2d 1050, 1053 (S.D. Cal. 1999) ("Defendant has cited no cases finding that electronically stored data is exempt from discovery."); Anti-Monopoly, Inc. v. Hasbro, Inc., No. 94CIV.2120, 1995 WL 649934, at *2 (S.D.N.Y. Nov. 3, 1995) ("[T]oday it is black letter law that computerized data is discoverable if relevant."); Ind. Coal Council v. Hodel, 118 F.R.D. 264, 266 (D.D.C. 1988) (indicating that requests to discover electronic information should be treated the same as other discovery requests); Daewoo Elecs. Co. v. United States, 650 F. Supp. 1003, 1004 (Ct. Int'l Trade 1986) (commenting that the discovery dispute before the court "is a good example of how the development of new technology for using, storing and transmitting information allows parties to test the rules of... discovery"); see also Medtronic Sofamor Danek, Inc. v. Michelson, 56 Fed. R. Serv. 3d (West) 1159, 1161 (W.D. Tenn. 2003) (considering as a threshold matter that the parties did not dispute that the electronic data requested by defendant satisfied the relevance requirements imposed by Rule 26(b)(1)); Cornel Research Found., 223 F.R.D. at 73 (describing the applicability of FRCP 34 to electronically stored information).

\textsuperscript{13} No. 95 CIV. 8026, 2002 WL 1007614, at *1 (S.D.N.Y. May 16, 2002).

\textsuperscript{14} See \textit{id.} at *5--*10.

\textsuperscript{15} \textit{id.} at *1.

\textsuperscript{16} \textit{id.} at *3--*4.

\textsuperscript{17} \textit{id.} at *4.

\textsuperscript{18} \textit{id.} at *5.
matters are not discoverable. The court then relied on FRCP 26(c)(1) to establish that the trial judge has broad discretion to tailor discovery narrowly to protect a party from undue burden or expense. These two rules formed the framework that the court asserted “applies to requests for electronic or computer-based information just as it applies to more traditional materials.”

The court then applied the framework to the defendant’s objections. After assuming that a substantial part of the information contained in the database was relevant, the court addressed the defendant’s privilege claim. In accordance with FRE 501, the court consulted federal common law to evaluate the merits of the defendant’s claim that prison personnel and inmate files are privileged and protected against discovery for security purposes. In the absence of precedent supporting the existence of a privilege for prison personnel and inmate files, the court rejected the defendant’s privilege claim. Although the court declined to decide whether it should recognize a privilege for prison personnel and inmate files, it noted that privileges “are not lightly created... for they are in derogation of the search for truth.” Nonetheless, the court did acknowledge the possibility that some of the information on the database may have fallen within the “more traditional” privileges. The court ultimately avoided making “broad legal proclamations about privilege” by denying the motion to compel pursuant to Rule 26(b)(2) because the burden of the electronic discovery significantly outweighed the likely benefits for resolving the case.

Jones essentially proposes that, where possible, courts should seek to evade a litigant’s request to recognize a new privilege on grounds of undue burden rather than engaging in a privilege analysis. Considering that production of documents can be
extremely time consuming and expensive particularly in the context of electronic discovery, discovery requests seeking electronic data are more likely to be unduly burdensome than those seeking paper documents. Where electronic rather than traditional discovery is concerned, courts may have more success in deflecting issues of privilege creation by focusing principally on whether motions to compel can be denied as unduly burdensome. Only in instances where the benefits of electronic discovery outweigh the burden should a court consider whether the motives for creating a particular privilege justify shielding the electronic data from disclosure.


Jones demonstrates that the FRCP and the FRE, particularly FRCP 26 and FRE 501, provide an adequate framework for the judicial resolution of privilege claims arising in electronic discovery after the privileged document has been identified. In electronic and traditional discovery alike, after segregating privileged documents from non-privileged ones, parties usually assert privileges by timely submitting a privilege log in accordance with FRCP 26(b)(5). Failure to satisfy the requirements of this rule can result in grave consequences for the privilege holder. However, where privilege discoverability by balancing the benefit and burden of the discovery request. 

Id.

29. See infra note 161 and accompanying text.

30. See supra note 10 and accompanying text; see also Banks v. Office of Senate Sergeant-at-Arms, 222 F.R.D. 7, 21 (D.D.C. 2004) ("[P]rivilege logs have become the universal means of claiming a privilege when a party claims that certain documents are privileged from discovery . . . ."); Medtronic Sofamor Danek, Inc. v. Michelson, 56 Fed. R. Serv. 3d (West) 1159, 1172, 1175 (W.D. Tenn. 2003) (instructing the plaintiff to review his electronic databases for privileged information and provide the defendant with a privilege log).

31. See Felham Enters. (Cayman) Ltd. v. Certain Underwriters at Lloyd’s, No. 02-3588 c/w 04-624, 2004 U.S. Dist. LEXIS 20983, at *9–*10 (E.D. La. Oct. 19, 2004). In Felham, the plaintiff propounded discovery of “all electronic files, paperless files, computer files, [and] computer work station files” pertaining to the claim. Id. at *3. The defendant’s privilege log was untimely, overbroad, and did not adequately describe the contents of the privileged documents, thus denying the plaintiff an opportunity to contest the claim. Id. at *9–*10. Based primarily on these circumstances, the court held that the defendant had waived any claim of privilege to the electronic data requested. Id. at *10; see also SEC v. Beacon Hill Asset Mgmt., 02 Civ. 8855 (LAK) (HBP), 2004 U.S. Dist LEXIS 15031, at *42–*43 (S.D.N.Y. Aug. 3,
logs fail to convey the merit of a claim of privilege and the privilege is contested, courts will usually make a determination based on an in camera review of disputed documents rather than deeming that the privilege has been waived. In most cases, compliance with FRCP 25(b)(5) poses no particular challenges once privileged materials have been identified.

It is usually before privilege claims are asserted and disputed, however, that electronic discovery complicates matters for litigants. For parties whose privileged documents are seeded among masses of stored electronic data, the main concern and challenge is identifying

---

2004). Here, the defendant asserted that an electronically stored contact list was privileged three weeks after the deadline for producing privilege logs. Id. at *42. Defendant claimed the delay was due to the fact that the "list did not exist" until it was printed out. Id. The court rejected this claim as frivolous, stating that "[t]he fact that data has not been printed out does not mean that the document does not exist." Id. at *43. Failure to include the contact list in the privilege index constituted a waiver of any privilege claim. Id.

32. Some courts frequently resort to in camera reviews, finding that privilege logs are generally insufficient to prove the existence of a privilege. See, e.g., Banks, 222 F.R.D. at 21 (ordering the production of documents for in camera review after stating, "I have reviewed the privilege log and find, as I invariably do, it is useless"). But see Navigant Consulting, Inc. v. Wilkinson, 220 F.R.D. 467, 473-74 (N.D. Tex. 2004) ([A] privilege log and an in camera review of documents may assist the court in conducting its [privileged] analysis. . . . [However], "resort to an in camera review is appropriate only after the burdened party has submitted detailed affidavits and other evidence to the extent possible." (citation omitted)).

33. But see United States v. Stewart, 287 F. Supp. 2d 461 (S.D.N.Y. 2003). In Stewart, Defendant listed an e-mail originally sent to her attorney on the privilege log, but failed to identify the forwarded version of the message sent to her daughter on the log. Id. at 436. Despite Defendant’s disclosure of the e-mail to opposing counsel, the court ultimately held the e-mail was protected under the work product doctrine. Id. at 469. Nonetheless, Defendant had to withstand judicial review before surviving the claim of privilege.

34. See Jones v. Goord, No. 95 CIV. 8026, 2002 WL 1007614, at *6 (S.D.N.Y. May 16, 2002) ([T]he first step in [any discovery analysis] is deciding whether requested material . . . is relevant and not privileged."). However, deciding how to make this determination may be very difficult in practice particularly where electronic discovery is concerned. See Medtronic, 56 Fed. R. Serv. 3d (West) at 1160 (noting that the parties had not been able to agree on a protocol for production, the court recognized that as an initial matter, "[p]roducing electronic data requires . . . several steps: (1) designing and applying a search program to identify potentially relevant electronic files; (2) reviewing the resulting files for relevance; (3) reviewing the resulting files for privilege; (4) deciding whether the files should be produced in electronic or printed form, and (5) actual production").
and protecting the privileged material from disclosure. Difficulties arise particularly in electronic discovery with regard to discerning which documents out of many qualify as privileged, and therefore can and must be withheld to prevent waiver. Perhaps the greatest question left unresolved by the FRCP in the context of both traditional and electronic discovery concerns the inadvertent production of privileged materials. Whether such a circumstance constitutes a waiver of privilege, and what parties can do to avoid such waiver are important matters on which the Federal Rules remain

35. See Medtronic, 56 Fed. R. Serv. 3d (West) at 1168. The court emphasized that the physical production of the electronic data was not the issue. Id. The real challenge was presented by “[t]he production of . . . data in a format [Plaintiff] can use, and in a way that accommodates [Defendant’s] privilege concerns . . . .” Id.; see also Ken Withers, Two Tiers and a Safe Harbor: Federal Rulemakers Grapple with E-Discovery, FED. LAW., Sept. 2004, at 35, available at http://www.kenwithers.com/articles/index.html (last updated Oct. 19, 2004). During the period of public commentary following the issuance of the proposed amendments by the Advisory Committee on Rules of Practice and Procedure dated May 17, 2004, nearly all commentators expressed recognition of the burden of conducting privilege review in response to electronic discovery requests. Id. at 23.

36. See Ciba-Geigy Corp. v. Sandoz Ltd., 916 F. Supp 404, 410 (D.N.J. 1996). In Ciba-Geigy Corp., Defendants inadvertently produced a privileged document from an electronic database after failing to identify it. Id. Finding that the disclosure constituted a waiver, the court warned that “the inadvertent production of a privileged document is a specter that haunts every document intensive case.” Id.; see also Cheney v. United States Dist. Ct., 124 S. Ct. 2576, 2597 (2004) (Ginsburg, J., dissenting). The Court validated the government’s objection to an overly broad discovery order on the basis that it imposed an unconstitutional burden which violated the separation of powers doctrine. Id. at 2588. The government lamented the burden imposed by the federal district court’s discovery order, explaining that each box of potentially responsive documents:

requires one or two attorney days to review and prepare a rough privilege log. Following that review, privilege logs must be finalized. Further, once . . . responsive e-mails are identified, printed, and numbered . . . privilege review and logging process [will] be equally, if not more time-consuming, due to the expected quantity of individual e-mails.

Id. at 2598.

37. See Kenneth J. Withers, Forward to MICHELE C.S. LANGE & KRISTIN M. NIMSGER, ELECTRONIC EVIDENCE AND DISCOVERY: WHAT EVERY LAWYER SHOULD KNOW, at iv (ABA ed., 2004) (“Since 2000, the case law has exploded, and the cases deal with a number of complicated questions, including . . . the effect of inadvertent production of privileged electronic communications.”).
The resolution of such questions on a case-by-case basis has challenged courts and litigants to devise discovery plans that prevent inadvertent disclosure in the first place. The following two sections will identify the privileges most frequently at issue in


[w]hen a party produces information without intending to waive a claim of privilege it may, within a reasonably time, notify any party that received the information of its claim of privilege. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies. The producing party must comply with Rule 26(b)(5)(A) with regard to the information and preserve it pending a ruling by the court.

Id. at 7.

Notably, the language of the rule still preserves the court’s discretion to find that inadvertent production of a document results in a waiver of any privilege that previously attached. Many commentators have suggested that this ambiguity could be settled at once by amending the FRCP to contain a clear abrogation of the common law rule applied in some jurisdictions that inadvertent disclosure of privileged information may constitute a waiver. See Withers, supra note 35, at 11. However, such a modification of the FRCP would probably exceed the delegation of the Rules Enabling Act, 28 U.S.C. § 2072, which provides for the prescription of procedural and evidentiary rules as long as they do not alter any substantive right. Id. Furthermore, under 28 U.S.C. § 2074(b), the United States Supreme Court is barred from adopting a rule that alters a privilege without Congressional approval. See Gregory P. Joseph, Proposed Electronic Discovery Amendments to the Federal Rules of Civil Procedure 1 (2005) at http://www.uscourts.gov/rules/e-delivery/04-CV-066.pdf.

39. See Ciba-Geigy Corp., 916 F. Supp. at 410–411 ("One line of cases holds that the inadvertent disclosure of a privileged document vitiates the privilege and constitutes a waiver... At the other end of the spectrum lies a line of cases which espouse the 'no waiver' rule... The [majority] approach takes the middle of the road, and focuses upon the reasonableness of the steps taken to preserve the confidentiality of privileged documents." (citations omitted)).

40. See Medtronic Safomor Danek, Inc. v. Michelson, 56 Fed. R. Serv. 3d (West) 1159, 1168 (W.D. Tenn. 2003) (noting that one of the court’s main concerns was devising an electronic discovery plan that enabled plaintiff to respond to a request for large volumes of data, while at the same time preventing disclosure of privileged documents).
electronic discovery, discuss the adequacy of traditional methods of privilege protection, and analyze parties' and courts' innovative approaches to privilege protection.

B. Privileges Most Frequently Implicated in Electronic Discovery

It is well established that electronic communications are no less deserving of privileged status than verbal or paper communications. At the same time, the mere fact that information is retained in an electronic form does not warrant its protection from disclosure. The important question is whether there are any differences between privileged information contained in paper-based documents and that stored in electronic form that would justify greater judicial leniency towards the latter.

41. According to the American Bar Association (ABA), "a lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating [the confidentiality provisions of] the Model Rules of Professional Conduct," as long as the client consents to that mode of communication. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999). In addition, the ABA has found that e-mail messages "pose no greater risk of interception or disclosure than other modes of communication commonly relied upon as having a reasonable expectation of privacy," and "[t]he level of legal protection accorded e-mail transmissions... supports the reasonableness of an expectation of privacy..." Id.

Courts and state legislatures, such as California and New York, support the proposition that electronic communications are worthy of privilege. See City of Reno v. Reno Police Protective Assoc., 59 P.3d 1212, 1218 (Nev. 2002). The court indicates that the electronic format of the communication does not preclude a finding of privilege. Instead, "[c]ourts have generally looked to the content and recipients of [an] e-mail to determine if the e-mail is protected... [A] document transmitted by e-mail is protected by the attorney-client privilege as long as the requirements of the privilege are met." Id.; see also CAL. EVID. CODE § 952 (West 1995) ("A communication between a client and his or her lawyer is not deemed lacking in confidentiality solely because the communication is transmitted by... electronic means between the client and his or her lawyer."); N.Y. C.P.L.R. 4548 (McKinney 1998) ("No communication privileged under this article shall lose its privileged character for the sole reason that it is communicated by electronic means or because persons necessary for delivery or facilitation of such electronic communication may have access to the content of the communication.").

42. See Holland v. GMAC Mortgage Corp., No. 03-2666-CM, 2004 WL 1534179 (D. Kan. June 30, 2004) (stating that the "mere fact that a document is a computer record or an electronic document does not warrant protection from disclosure" and rejecting a request for a protective order that would designate as confidential all computer records).
Federal courts recognize a number of privileges, including but not limited to the attorney-client privilege, the psychotherapist-patient privilege, the spousal privileges, the priest-penitent privilege, and the privilege accorded to state secrets. In addition, under the work product doctrine, federal courts also protect the confidentiality of materials prepared by the parties in anticipation of litigation. The privileges asserted most commonly by parties during discovery are the attorney-client privilege and the work product privilege. Consequently, privileges other than those protecting attorney-client communications and work product are less likely to be implicated in the context of electronic discovery.

For example, there is no case law to date dealing with the spousal privileges, the psychotherapist-patient privilege, or the priest-penitent privilege in the context of electronic discovery. The reason for this may be that these types of privilege holders do not rely on electronic communications to convey important information to the extent that in-house counsel and corporate officers do. On the other hand, it could be that privilege claims based on electronic communications between these types of groups are simply not as frequently contested. The remainder of this section will focus on the electronic discovery cases involving the attorney-client privilege and the work product doctrine.

1. The Attorney-Client Privilege

The purpose of the attorney-client privilege is to "encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice." Furthermore, effective "advocacy

---

43. See generally MURL A. LARKIN, FEDERAL TESTIMONIAL PRIVILEGES (1982–2002) (setting out the privileges recognized by federal courts and extensively referencing case law on the subject).
47. Upjohn Co., 449 U.S. at 389; see also Women's InterArt Ctr. v. N.Y.C. Econ. Dev., 223 F.R.D. 156, 159 (S.D.N.Y. 2004) (setting out the elements of the attorney-client privilege and explaining its purpose in the context of
serves public ends and... depends on the lawyer's being fully informed by the client." Courts resolving disputes involving the attorney-client privilege apply the same tests to electronic communications as would be applied to traditional paper documents.

\[a. \text{E-mail}\]

One way in which clients increasingly communicate with their attorneys is through e-mail. It is particularly in litigation involving

electronic discovery).


49. Long v. Anderson Univ., 204 F.R.D. 129, 134 (S.D. Ind. 2001) (considering whether an e-mail communication was privileged under the attorney-client privilege, the court turned to the general standard adopted by the Seventh Circuit: "(1) where legal advise was sought; (2) from a professional legal advisor in his capacity as such; (3) the communications relating to that purpose; (4) made in confidence; (5) by the client; (6) are at his instance permanently protected; (7) from disclosure by himself or by the legal advisor; (8) except the protection be waived") (citing 9 WIGMORE, EVIDENCE § 2292 (McNaughton rev. 1961)). Other circuits have applied the same standard in the context of electronic discovery. See, e.g., Uniroyal Chem. Co., Inc. v. Syngenta Crop Protection, 224 F.R.D. 53 (D. Conn. 2004); United States v. B.D.O. Seidman, LLP, No. 02 C 4822, 2004 WL 1470034 (N.D. Ill. June 29, 2004); Cornell Research Found. Inc. v. Hewlett Packard Co., 223 F.R.D. 55 (N.D.N.Y. 2003); United States v. Stewart, 287 F. Supp. 2d 461 (S.D.N.Y. 2003); Naquin v. UNOCAL Corp., 53 Fed. R. Serv. 3d (West) 1079 (E.D. La. 2002); Lewis v. UNUM Corp. Severance Plan, 203 F.R.D. 615 (D. Kan. 2001); see also Visa U.S.A., Inc. v. First Data Corp., No. C-02-1786JSW(EMC), 2004 WL 1878209 (N.D. Cal. Aug. 23, 2004). In analyzing whether corporate e-mail messages were privileged, the court in *Visa U.S.A., Inc.* applied a standard newly adopted by the Ninth Circuit. *Id.* at *4. Under previous Ninth Circuit precedent, "the protection of the [attorney-client] privilege applie[d] only if the primary or predominant purpose of the attorney-client consultations [was] to seek legal advice or assistance." *Id.* at *3 (internal quotation omitted). The court found that the messages were not privileged under the newer more protective test which takes into consideration "the totality of the circumstances and affords protection when...[a] document [is] created because of anticipated litigation, and would not have been created in substantially similar form but for [that] prospect." *Id.* at *3-*4 (quoting *In re Grand Jury Subpoena*, 357 F.3d 900, 908 (9th Cir. 2004)).

50. Discovery disputes involving e-mail messages between attorneys and private individuals seemingly arise much less frequently than those involving e-mail messages between attorneys and corporate clients. In fact, there is a scarcity of case law dealing with assertions by individuals of the attorney-client privilege with respect to e-mail messages sent to counsel. *See Stewart*, 287 F. Supp. at 463 (responding to her attorney's ongoing requests for factual
corporations, however, that parties have occasion to resist discovery of e-mail messages pursuant to the attorney-client privilege.\textsuperscript{51} This seems to be due to two relatively recent developments—corporate dependence on electronic communications for efficient functioning and the increased role of in-house and outside counsel in the corporate decision-making process.\textsuperscript{52} Courts have recognized that e-mail messages addressed to in-house counsel by corporate officers, employees and other corporate legal representatives frequently contain information regarding both legal and business matters.\textsuperscript{53} As a result, courts exercise heightened caution when making privilege determinations regarding e-mail messages sent by, addressed to, or

\begin{quote}
information pertinent to her securities fraud defense, defendant prepared an e-mail memorializing the circumstances of her sale of stock); Turner v. Brave River Solutions, No. Civ. 02-148 D, 2003 WL 21418540, at *1 (D.N.H. June 18, 2003) (acknowledging that the plaintiff, a private individual, asserted the attorney-client privilege as to an e-mail sent to him by his attorney which was inadvertently produced to defendant). \textit{But see} Nicholas v. Wyndham Intern., Inc., 224 F.R.D. 370, 371 (D.V.I. 2004). Plaintiffs sued a resort and its employee who they claimed had inappropriate sexual contact with their son. \textit{Id.} at 370. Plaintiffs exchanged e-mail communications with the Assistant Attorney General of the Virgin Islands on the subject of defendant-employee’s criminal prosecution. \textit{Id.} at 371. The court found that the e-mail messages were not subject to the attorney-client privilege because they were not communications between plaintiffs and their attorney. \textit{Id.} at 372 n.4.


\textsuperscript{52} See United States v. Segal, No. 02-CR-112, 2004 WL 830428, at *3 (N.D. Ill. Apr. 16, 2004) ("One challenge to our privilege analysis is that the expanded role of the corporate general counsel has blurred the line between business and legal advice... Additionally the rise of e-mail as the primary mode of corporate communications permits the broad dissemination and near-complete documentation of corporate communications.").

\textsuperscript{53} See Bell Microproducts, Inc. v. Relational Funding Corp., No. 02 C 329, 2002 WL 31133195, at *1 (N.D. Ill. Sept. 25, 2002) ("[A]s is often signaled by such legal titles as [Vice President and General Counsel], a lawyer employed as house counsel sometimes wears his or her lawyer’s hat but also sometimes wears a businessman’s or businesswoman’s hat—or on occasion he or she may don both simultaneously.").
forwarded to in-house counsel.\textsuperscript{54} In fact, courts have regarded with particular skepticism claims that e-mail messages are subject to the attorney-client privilege because they have either been copied or forwarded to in-house counsel.\textsuperscript{55}

An e-mail message is only privileged to the extent that it contains legal advice or client confidences, regardless of whether the communication was sent by or addressed to a privilege claimant's attorney.\textsuperscript{56} Litigants that seek to pass off non-privileged

\begin{itemize}
\item \textsuperscript{54} See Segal, 2004 WL 830428, at *3 (noting the difficulty of making privilege determinations in situations where e-mail messages are transmitted between a corporate officer and general counsel); Teleplus, Inc., 2003 WL 23282491, at *3 ("E-mail documents [transmitted between in-house counsel and corporate employees] are of particular complexity when determining whether they should be privileged.").
\item \textsuperscript{55} See United States ex rel. Fields v. Sherman Health Sys., No. 01 C 2495, 2004 WL 905934, at *3 (N.D. Ill. Apr. 28, 2004). Defendant's employee sent an e-mail to another employee and to defendant's attorney. \textit{Id.} The e-mail disclosed contents of a discussion with a non-lawyer. \textit{Id.} The fact that the e-mail was copied to defendant's attorney did not make the communication privileged. \textit{Id.; see also In re Gabapentin Patent Litig., 214 F.R.D. 178, 186 (D.N.J. 2003) ("Forwarding an e-mail ... to an attorney does not transform it into the attorney's work product... Neither can it be said that communications between clients, unrelated to legal issues or advice, fall under the attorney client privilege... Cc'ing numerous people who are ancillary to the discussion, one of whom happens to be an attorney, or forwarding an e-mail several times until it reaches an attorney does not amount to 'attorney client communication.'"); Mac-Ray Corp. v. Ricotta, No. 03-CV-523S(F), 2004 WL 1368857, at *2 (W.D.N.Y. June 16, 2004). One of plaintiff's senior executives sent an e-mail to two employees in the human resources department with a copy to plaintiff's in-house counsel. \textit{Id.} The e-mail recited the facts of defendant's resignation and as such did not seek legal advice or assistance. \textit{Id.}
\item \textsuperscript{56} See Women's InterArt Ctr., Inc. v. N.Y.C. Econ. Dev., 223 F.R.D. 156 (S.D.N.Y. 2004). In its privilege inquiry, the court focused on the content of an e-mail and an attached draft letter, as well as on the identity of the sender and recipient. \textit{Id.} at 161. The court reasoned that "'[s]uch documents retain their privilege if 'they were prepared for the purpose of obtaining legal advice and/or contain information a client considered but decided not to include in the final version ... ,' or if it is demonstrated that a confidential communication was removed from the final document." \textit{Id.; Visa U.S.A., Inc., 2004 WL 1878209.} Visa asserted the attorney-client privilege as to several e-mail messages that contained embedded messages that had either been authored or received by Visa's in-house counsel. \textit{Id.} at *10. The court rejected the claim, noting that the messages were not prepared because of a legal purpose. \textit{Id.; see also, Bell, 2002 WL 31133195, at *2 (claiming that non confidential e-mail messages were privileged merely because an attorney was one of multiple recipients); B.F.G. of Ill., Inc. v. Ameritech Corp., No. 99 C 4604, 2001 WL
communications as privileged "by routing them through an attorney" are seldom successful in prevailing on a privilege claim once challenged:  

[This] is not of course how privilege (or for that matter work product) operates... [T]he mere presence of a lawyer’s name at the top or bottom of a document is not the bell that causes the dog named Privilege to salivate. What is entitled to protection is really limited to the communication of confidences from client to lawyer, whether any such confidences (or sometimes the fact that confidences have been communicated) [are] disclosed in a client-authored document or lawyer-authored response.  

There are two important reasons why such a “full boar” and undifferentiating approach is harmful to the adjudicative process and will therefore not be tolerated. First, “[a] particular problem with this scenario is that there is no way that the party seeking the documents can detect... improper use merely from the description on the privilege log.” Second, parties who characterize as privileged re-routed electronic communications pose a serious threat to the efficient and just resolution of legal conflicts. Thus,

[u]nless in-house counsel and litigation counsel are

58. See Women’s InterArt Ctr., 223 F.R.D. at 161. The court determined that a draft letter sent between non-lawyers and attached to e-mail correspondence addressed to counsel did not qualify as privileged. Id. However, the court did recognize that the e-mail itself was privileged. Id.; see also Bell, 2002 WL 31133195, at *2 (ordering the defendant to produce e-mail messages sent to or from its in-house counsel acting in a business capacity rather than in a legal capacity); B.F.G. of Ill., Inc., 2001 WL 1414468, at *6 (identifying two e-mail messages sent to corporate counsel through an intermediary as having been wrongfully withheld as privileged).
60. Id.
61. See B.F.G. of Ill., Inc., 2001 WL 1414468, at *6 (“[C]onsistent with decisions of other federal courts, [the court in this case would] not tolerate the use of in-house counsel to give a veneer of privilege to otherwise non-privileged business communications.”).
62. Id.
63. See id.
scrupulous in their assertion of privilege, the courts will be asked to review all documents in which an in-house attorney’s involvement is the basis for assertion of privilege or work product. That would impose an unbearable burden on the courts and other litigants.\(^{64}\)

Courts may impose a particular burden on corporations to demonstrate that allegedly privileged e-mail messages are not merely business related communications.\(^{65}\) An unsupported claim that an e-mail message is privileged may cause the court to scrutinize corporations’ internal electronic communications practices to determine whether they function to deliberately mislead opposing counsel and the court.\(^{66}\)

Corporations that employ deceptive e-mail

---

64. *Id.* at *7. Over 500 allegedly privileged documents were submitted to the judge for in camera review. *Id.* at *5. *See also* Banks v. Office of Senate Sergeant-At-Arms, 222 F.R.D. 7, 21 (D.D.C. 2004) (ordering that 400 documents claimed to be privileged be submitted to the court for an in camera review).

65. *See B.F.G. of Ill., Inc.*, 2001 WL 1414468, at *6. In the context of a privilege dispute over e-mail messages, the court stated that in circumstances where corporate counsel works with a business team, “there is a particular burden on that corporation to demonstrate why communications deserves protection and are not merely business documents.” *Id.; see also* Visa U.S.A., Inc. v. First Data Corp., No. C-02-1786JSW(EMC), 2004 WL 1878209, at *10 (N.D. Cal. Aug. 23, 2004) (“The involvement of in-house counsel alone [in e-mail communications] is not enough for the attorney-client privilege to be applicable. Because in-house counsel is often extensively involved in the business matters of the company... [c]ourts have not been willing to presume that the services provided were of a legal, as opposed to a business, nature.”).

66. *See* Bell Microproducts, Inc. v. Relational Funding Corp., No. 02 C 329, 2002 WL 31133195, at *1 (N.D. Ill. Sept. 25, 2002). The court criticized defendant’s General Counsel for giving the following instructions to fellow employees: “[U]nless instructed otherwise, any written correspondence you author, whether by letter, memo, Excel spreadsheet, e-mail, etc., should be directed to my attention (at least as one of the recipients) to assure that the attorney-client privilege is retained.” *Id.; see also* B.F.G. of Ill., Inc., 2001 WL 1414468, at *6 (N.D. Ill. Nov. 13, 2001). The court in *B.F.G. of Illinois, Inc.* noted that the defendant “was sophisticated in its efforts to shield its communications.” *Id.* at *6. The first e-mail claimed to be privileged announced a “final business decision.” *Id.* It did not seek legal advice as defendant had asserted, but merely instructed counsel to “approve from a legal perspective... and... forward to” other people on counsel’s business team. *Id.* The second e-mail merely forwarded a previous e-mail sent to in-house counsel by a corporate employee. *Id.* at *7. The forwarded e-mail explained that another specified corporate employee had asked for comments on a purely business matter. *Id.* When forwarding the message to the specified employee,
practices intended to link in-house counsel to non-privileged communications in order to complicate privilege determinations may be ordered to pay the costs incurred by the opposing party due to such determinations. By imposing such sanctions, courts generally seek to deter litigants from "us[ing] in-house counsel to apply a veneer of privilege to non-privileged business communications." 

The above discussion indicates that e-mail facilitates communication about both protected legal matters and non-legal matters between in-house counsel and corporate officers and employees. While it has always been possible for litigants to assert scurrilous privilege claims as to non-privileged paper documents addressed to counsel, such abusive tactics may have become more pervasive with the emergence of electronic technology. The copying and forwarding functions unique to e-mail communications provide an effortless means of concealing "smoking guns" by veiling them behind a "smoke screen" of privilege. Even if e-mail messages are not forwarded to attorneys for the purpose of creating a false premise for a privilege claim, the temptation to withhold non-privileged e-mail messages directed to or sent by corporate counsel has grown with the overall increase in communications running to or from corporate counsel due to e-mail.

the in-house counsel did not add any commentary whatsoever.  ld. 67. 1d. After determining that defendant's privilege log deceptively characterized communications regarding business matters as privileged documents, the court ordered that defendant pay the costs plaintiff incurred in preparing the motion to compel. ld. But see Bell, 2002 WL 31133195, at *1. Despite a strong indication that defendant adopted deceptive internal e-mailing practices, the court only chastised the defendant for relying on the flimsy claim that the mere receipt of e-mail shelters communications otherwise unworthy of the attorney-client privilege. ld.

69. See 1 PAUL R. RICE, ATTORNEY-CLIENT PRIVILEGE IN THE UNITED STATES § 7:2, at 24 (2d ed. 1999) (noting generally that businesses may try to "immunize internal [business] communications from discovery by placing legal counsel in strategic corporate positions and funneling documents through counsel").

70. In fact, many of the cases addressing the attorney-client privilege asserted as to e-mail messages involve unpersuasive claims. See cases cited supra notes 55–56.
71. See B.F.G. of Ill., Inc., 2001 WL 1414468, at *4 ("[I]n-house counsel and litigation counsel" have "an important professional responsibility . . . to police the anticipatable desire of corporations to shield as much as possible from their adversaries in litigation.").
Nonetheless, the deeply entrenched precedent of construing privileges narrowly\(^7\) encourages courts to peer behind the curtain of privilege to ascertain the true nature of the e-mail at issue.\(^7\) Additionally, courts’ power to impose sanctions on unscrupulous litigants, although infrequently wielded, constitutes an important potential deterrent of the manipulation of electronic communications to abuse the attorney-client privilege.\(^7\)

\(b.\) **Voice mail**

Voice mail has been described as the “next frontier in electronic discovery.”\(^7\) Forecasts that voice mail will emerge as an abundant and potent source of discovery are based on cutting edge technological developments in information technology that will improve voice mail retention\(^7\) and simplify searches of the medium.\(^7\)

---

72. See Lewis v. UNUM Corp. Severance Plan, 203 F.R.D. 615, 618 (D. Kan. 2001) (noting that the attorney-client privilege “is to be extended no more broadly than necessary to effectuate its purpose”).

73. In this respect, the power to require parties to submit contested electronic communications to the court for in camera inspection is indispensable to the truth seeking function of the adversarial system.


76. See Madden et al., *supra* note 75. United Message Systems (UMS) have evolved to the point where digitized e-mail and voice mail systems are rapidly converging. *Id.* This has improved the capacity for retention of voice mails. *Id.* Voice mail systems may have the capacity to retain all voice mail messages. *See* Bennett, *supra* note 75. But see Alexander v. F.B.I., 186 F.R.D. 148, 153 (D.D.C. 1999) (describing the retention capacity of the voice mail system in place at the White House as late as 1998 and indicating that unopened voice mail was erased after only ten days while opened voice mail was erased after only fifteen days).

77. Voice mail has always been a problematic target for discovery considering that it is not searchable and, therefore, must be screened aurally. *See* Madden et al., *supra* note 75. However, several UMS providers appear to be developing technologies that will permit text searches of voice recordings. *Id.* Such capabilities “will enable litigation teams to quickly review voice files for privilege and keep out what is not necessary (and possibly damaging to the
Currently, federal case law addressing discovery disputes over electronically stored voice mail is extremely scant.\(^7\)8 “However, there is nothing in theory and little in substance to distinguish these forms of communication from e-mail ... for the purposes of discovery.”\(^7\)9 Several courts have indicated that discoverable electronically stored data includes voice mail.\(^8\)0 Moreover, other courts have issued rulings based on the same implicit premise.\(^8\)1 Courts have employed the same procedures for determining whether voice mail is privileged as they would in analyzing other types of communications.\(^8\)2 Insofar as voice mail satisfies the elements of applicable privileges, it will receive protection comparable to that accorded to other types of privileged communications.\(^8\)3

\(^7\)8. As recently as December 1999, Kenneth Withers stated that “[v]oice mail is only mentioned occasionally in the literature, and there are no instances cited in which it has actually been disclosed in discovery.” Kenneth J. Withers, Is Digital Different? Electronic Disclosure and Discovery in Civil Litigation, (Dec. 30, 1999), at http://www.kenwithers.com/articles/bileta/elecdisc.htm (last updated Oct. 19, 2004).

\(^7\)9. Id.


\(^8\)1. See Bayer Corp. v. Roche Molecular Sys., Inc., 72 F. Supp. 2d 1111, 1121 (N.D. Cal. 1999) (ordering an employee of defendant to “transcribe or otherwise preserve all voicemails that he receives ... and they too must be produced [to plaintiff for in preparation for his deposition]”); see also Lewis v. UNUM Corp. Severance Plan, 203 F.R.D. 615, 617 (D. Kan. 2001) (reviewing in camera transcriptions of voice mails claimed to be privileged).

\(^8\)2. See Lewis, 203 F.R.D. at 617. The plaintiff sought to compel discovery of a voice mail sent by one of defendant’s company representatives to defendant’s in-house counsel. Id. To determine whether the voice mail was protected by the attorney-client privilege, the court reviewed a transcript of the voice mail in camera. Id.; see also Coastline Terminals of Conn., Inc. v. U.S. Steel Corp., 221 F.R.D. 14, 17–18 (D. Kan. 2001) (reviewing in camera a transcript of an allegedly privileged voice mail).

\(^8\)3. See Lewis, 203 F.R.D. at 621–622 (determining that a voice mail sent by defendant’s company representative to defendant’s in-house counsel “relat[ed] to legal advice sought by a client and thus [was] protected by the attorney-client privilege”); see also Coastline Terminals of Conn., 221 F.R.D.
c. Expectation of confidentiality

It has been observed that e-mail and voice mail engender communications that are less formal than a written letter.\textsuperscript{84} E-mail messages are often infused with a frankness that is a common characteristic of instantaneous communication by phone or in person.\textsuperscript{85} This is in part due to an overestimation of the confidentiality associated with e-mail messages.\textsuperscript{86} The unguarded nature of many e-mail communications renders such evidence an extremely persuasive at trial.\textsuperscript{87} Furthermore, because e-mail and

\textsuperscript{84} See Kenneth J. Withers, \textit{Self-Deleting E-mail: A Self-Delusion}, http://www.kenwithers.com/articles/index.html ("[D]espite a decade of high-profile e-mail gaffs... people churned out embarrassing and self-incriminating electronic messages at a dizzying rate... .'[T]he real lesson corporate America is taking away from the Microsoft antitrust trial is that old e-mail can be a mine field of legal liability, not to mention a source of public embarrassment.") (quoting Amy Harmon, \textit{Corporate Delete Keys Busy as E-mail Turns up in Court}, NEW YORK TIMES, Nov. 11, 1998, at A1); Stephen D. Williger & Robin M. Wilson, \textit{Negotiating the Minefields of Electronic Discovery}, 10 RICH. J.L. & TECH. 52, 27 (2004), at http://law.richmond.edu/jolt/v10i5/article52.pdf ("Employees need to be educated to be mindful of the contents of all electronic documents—especially, but not exclusively, e-mail, text messaging, and other seemingly 'informal' means of communication.").

\textsuperscript{85} See Mark D. Robins, \textit{Computers and the Discovery of Evidence—A New Dimension to Civil Procedure}, 17 J. MARSHALL J. COMPUTER & INFO. L. 411, 416 (1999) ("Because users do not expect the information entered into many of these formats ever to be put in hard copy, this information is likely to be less guarded and, therefore, more revealing and potentially damaging. Perhaps the best example of this phenomenon is the notoriously relaxed attitude of e-mail users whose spontaneity appears to be inspired by an instantaneous and seemingly private form of communication in which the presence of the interlocutor is not felt."); Madden et al., \textit{supra} note 75 ("Voice-mail has traditionally been the most personalized and candid form of communication in business.").

\textsuperscript{86} See Withers, \textit{supra} note 37. Perhaps this frankness is due to the false perception by electronic technology users that electronic evidence is not "'real' because the evidence was never reduced to paper form, nor is it even susceptible to being printed out." \textit{Id.} at iv.

\textsuperscript{87} See, \textit{e.g.}, Owens v. Morgan Stanley & Co., No. 96 Civ. 9747 DLC, 1997 WL 793004 (S.D.N.Y. Dec. 23, 1997) (addressing the racist comment
voice mail facilitate the candid exchange of information, they have the potential to significantly enhance the quality of legal representation by increasing the amount of information available to an attorney. For the above reasons, privileged electronic communications require at least the same degree of protection as is afforded to paper based documents. Any comparative reduction in protection of electronic communication will undercut the utility of e-mail and voice mail as effective communicative tools for potential litigants.

On the other hand, there is an argument that electronic communications create a lower expectation of confidentiality than communications made in person, by phone or by traditional mail.88 “Private, or internal, e-mail systems ... do not create the potential for inadvertent waiver of the attorney-client privilege through the disclosure of confidential information because, by their private nature, the communications never [have to] leave the building and ... never [have to] actually [be] disclosed.”89 In contrast, “[p]ublic e-mail systems using the Internet ... invoke a host of concerns over the confidentiality and security of e-mail communications between attorney and client.”90 Such concerns have led to a debate over whether attorneys should use encryption

that was sent through company e-mail system and gave rise to employment discrimination lawsuit); Strauss v. Microsoft Corp., 68 Fair Empl. Prac. Cas. (BNA) 1576 (S.D.N.Y. 1995), 91 Civ. 5928 SWK, 1995 WL 326492 (S.D.N.Y. June 1, 1995) (finding inappropriate e-mail messages sent by supervisor were probative evidence in retaliatory discharge case); Siemens Solar Indus. v. Atl. Richfield Co., No. 93 Civ. 1126 LAP, 1994 WL 86368 (S.D.N.Y. Mar. 16, 1994) (finding defendant’s e-mail contradicted theory of its defense); see also Madden et al., supra note 75 (“Even with the proliferation of e-mail and other electronic documents, voice mail continues to have a greater impact on juries and judges.”); Bennett, supra note 75 (“Voicemail evidence is powerful. Even beyond e-mail, where informal, often ill-considered messages can produce damning admission, the actual sound of an oral message can literally make or break a case.”).

88. See Mathew J. Boettcher & Eric G. Tucciarone, Concerns Over Attorney-Client Communication Through E-Mail: Is the Sky Really Falling?, 2002 L. REV. MICH. STATE UNIV. DETROIT C. LAW 127, 128 (Spring 2002) (commenting that “attorneys and judges alike have not been so quick to afford e-mail communications the same level of respect and protection” that they would give to more traditional means of communications).

89. Id. at 130.

90. Id.
programs to prevent privileged communications from being denied protection either because of a finding that the requisite confidentiality was lacking or because of waiver. Considering that many corporations employing in-house counsel operate internal e-mail systems, the reduced confidentiality of e-mail messages would appear to affect private individuals more than corporations. Nonetheless, several court opinions addressing the expectation of privacy in e-mail messages sent via the Internet have indicated that e-mail communications are sufficiently secure to preserve the attorney-client privilege.\(^9\)

Attorneys should, however, adhere to clients’ preferences with respect to means of communicating sensitive information.\(^2\)

2. The Work Product Doctrine

The work product doctrine shields from discovery material “prepared in anticipation of litigation or for trial”\(^3\) by or for a party or its representative, including but not limited to that party’s attorney.\(^4\) Generally, the goal of the work product doctrine is to

91. See United States v. Maxwell, 45 M.J. 406, 418 (1996) (“The [e-mail] sender enjoys a reasonable expectation that the initial transmission will not be intercepted by the police. The fact that an unauthorized ‘hacker’ might intercept an e-mail message does not diminish the legitimate expectation of privacy in any way.”).

92. See ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999) (“A lawyer should consult with the client and follow her instructions, however, as to the mode of transmitting highly sensitive information relating to the client’s representation.”).

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

94. See Portis v. City of Chicago, No. 02 C 3139, 2004 WL 1535854, at *2 (N.D. Ill. July 7, 2004) (announcing the definition of and principles behind the work product doctrine in the context of plaintiff’s opposition to defendant’s motion to compel production of a database compiled by plaintiff); United States v. Stewart, 287 F. Supp. 2d 461, 465 (S.D.N.Y. Oct. 20, 2003) (applying the work product doctrine in a criminal case and concluding that an e-mail by defendant to her attorney in preparation of trial was privileged despite its
preserve a zone of privacy in which a lawyer can prepare and develop legal theories and strategy ‘with an eye toward litigation’ free from unnecessary intrusion by his adversaries.” The work product doctrine is perhaps even more strongly implicated in electronic discovery than in traditional discovery. In fact, “[c]omputers... enable users [including attorneys] to create summaries, indices, and methods of organizing vast quantities of information.” Attorneys, like other professionals, increasingly rely on computers to manage information and records relating to their cases. Considering the utility of electronic data compilations and the costs associated with creating them, parties are eager to discover litigation databases created by opposing counsel. For the same reason, attorneys in possession of such databases invoke the work product doctrine to shield them from discovery.

While attorney work product that reveals the “mental impressions, conclusions, opinions, or legal theories of an attorney... concerning the litigation” is entitled to almost absolute protection, work product that does not can be disclosed “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.” These general principles developed in the context of paper discovery apply to electronic documents as well.


96. Robins, supra note 85, at 414.

97. See Bennett, supra note 75.

98. See Portis, 2004 WL 1535854 at *1 (opposing a motion to compel a litigation database).


100. FED. R. CtV. P. 26(b)(3).
a. Litigation databases

Electronic work product such as computer files and database compilations often consists of aggregations of factual information that is either entitled to qualified protection as ordinary work product or no protection at all. However, as in the case of paper work product that appears in the first instance to be ordinary, electronic data may constitute opinion work product if, due to the manner in which they are compiled, they would reveal the legal theories and strategies that an attorney is pursuing. For example, computer databases prepared in anticipation of litigation and containing files of a corporate litigant’s personnel might not be discoverable. Although the personnel files themselves may not qualify as work product at all, the composition of files may nonetheless deserve protection as opinion work product if it reveals the litigant’s discovery plan.

101. In determining whether electronic data compilations qualify as ordinary work product or opinion work product, courts have looked for guidance to Sporck v. Peil, 759 F.2d 312 (3d Cir. 1985). See Portis, 2004 WL 1535854, at *2; Scovis v. Upjohn Co., 15 Conn. L. Rptr. 446 (Conn. Super. Ct. 1995), No. 526520, 1995 WL 731755, at *2–3 (Conn. Super. Ct. Nov. 22, 1995). In Sporck, the issue was whether an attorney’s selection and compilation of documents for his client to review in preparation for his deposition constituted opinion work product. Sporck, 759 F.2d at 315. The court held that “[i]n selecting and ordering a few documents out of thousands counsel could not help but reveal important aspects of his understanding of the case. Indeed, in a case such as this . . . the process of selection and distillation is often more critical than pure legal research.” Id. at 316.

A court also cited Washington Bancorporation v. Said, 145 F.R.D. 274 (D.D.C. 1992), in an attempt to resolve a work product claim involving an electronic database. See Portis, 2004 WL 1535854, at *2. In Washington Bancorporation, an attorney created an index cataloging 2,400 boxes of documents. 145 F.R.D. at 278. Although the index could be considered a hybrid of fact and opinion work product, the court in Washington Bancorporation was not concerned that the attorney’s strategy of the case would be revealed because it was “not selective enough.” Id. at 276–77.


103. Id. Plaintiffs moved to compel defendant to answer several interrogatories requesting detailed information regarding a computer file set up by defendant for the purpose of defending a sex discrimination claim. Id. The computer file contained information regarding defendant’s personnel records. Id. The court noted that it had previously protected discovery of the physical computer tape containing the file. Id. In this particular instance, even collateral information regarding the computer file was protected under the
On the other hand, courts have suggested that protection of litigation databases as opinion work product will only be granted under exceptional circumstances, as the general rule provides that information that would not be protected if it remained in a client’s hands do not acquire work product protection merely because they are transferred to counsel.\textsuperscript{104} Considering that databases are usually created for the management of large amounts of information, they are less likely than a discrete selection of paper documents to reveal opinion work product.\textsuperscript{105} As a result, even where a database constitutes a hybrid of fact and opinion work product, courts may order its production upon an adequate showing of need by the discovering party.\textsuperscript{106} In such cases, the volume of data is a crucial factor in determining whether access to an electronic database will enable a discovering party to discern the litigation strategies of opposing counsel.\textsuperscript{107} Another significant factor may be the objective
or subjective nature of the data. To the extent that a database contains written subjective comments as to the strategy behind the selection of documents, such comments constitute opinion work product which can be redacted from the material.

**b. Legal research databases**

The search terms employed by attorneys to find relevant law and to develop a theory of a case may qualify as opinion work product and be protected against discovery. Moreover, the compilation of results that such search terms elicit from legal databases is also entitled to protection as opinion work product even if each separate result may not reveal the mental impression of an attorney.

that a litigation database would not reveal the impressions of the attorney on the abundance of arrest records that had been compiled (20,000 records). The aggregation of such a large number of documents obscured opposing counsel’s ability to discern any discrete strategy developed by the producing party’s attorney. See also Scovish, 1995 WL 731755, at *3. The plaintiff in Scovish sought to discover a database prepared by defendant's attorney that referenced and indexed a large number of documents. Id. at *1. The court concluded that because of the vast amount of documents referenced in defendant’s database (a printout of which would exceed 100,000 pages), it would be highly unlikely that defense attorney’s mental impressions would be exposed by production. Id. at *1-*3.

108. See Minnesota v. Philip Morris, Inc., No. CX-95-2536, 1995 WL 862582, at *1 (Minn. App. Dec. 26, 1995). The court rejected a attorney’s claim that production of his client’s litigation database would reveal his strategies. Id. The court based its determination, in part, on a finding that “the computerized databases include fields containing objective information.” Id.

109. See Scovish, 1995 WL 731755, at *4. It is unclear just how such opinion work product would be redacted, whether by deleting it from a computer tape copy of the database or by redacting it from the paper printout of the database.

110. See United States v. Segal, No. 02-CR-112, 2004 WL 830428, at *8 (N.D. Ill. Mar. 31, 2004). Defendant opposed discovery of four e-mail communications containing judicial opinions transmitted by co-defendant’s general counsel to herself from Lexis-Nexis. Id. The court agreed with the defendant that “[t]he search terms used to gather [the] cases... provide a window into the attorney’s thinking.” Id. Although the search was performed before litigation commenced, “[t]he search terms closely relate[d] to the subject matter of the present litigation and indicate that [the] General Counsel was researching the claims at the heart of the present litigation.” Id.

111. See Burroughs Wellcome Co. v. Barr Labs., 143 F.R.D. 611, 624 (E.D.N.C. 1992). The court shielded from discovery the printed results of an electronic database search conducted in Nexis and Dialog at the request of counsel. Id. The court determined that “although the documents themselves
In rare instances, a party may maintain its own legal research system comprised of legislative materials and judicial opinions. Such databases are generally not discoverable—not because they qualify as opinion work product, but because they constitute a collection of the law. As discovery is a procedural tool for the gathering of facts, it cannot be used to extract the law from opposing counsel. In the interest of efficiency and economy, however, a court may encourage counsel to run a search according to criteria designated by opposing counsel.

The foregoing discussion regarding both attorney compiled and legal research databases demonstrates the potential for electronic data to be manipulated in ways that facilitate trial preparation for attorneys. It appears that compilation of databases for litigation purposes is usually undertaken by large corporate or governmental defendants attempting to determine the existence or extent of liability. Whether the party opposing discovery of a database compilation will prevail under the attorney work product doctrine

---

113. See id. at 265. Plaintiff appealed to the district court from the order of the Magistrate. Id. The order denied a motion to compel Defendants to allow Plaintiff access to “COALEX,” a legal research system containing 5,000 pages of legislative history, information regarding federal and state regulatory programs and judicial decisions. Id. The court rejected the magistrate judge’s finding that COALEX was a “confidential research system” entitled to qualified privilege under FED. R. Civ. P. 26(c)(7). Id. at 266. The court explained that all of the data that was searcheable by COALEX was publicly accessible and, therefore, could not be considered “confidential research.” Id. Furthermore, the court denied that the discovery request implicated the work product doctrine. Id. at 267. Instead, the court held COALEX was not discoverable, considering that it was a compilation of legal rather than factual information. Id. However, in the end the court concluded that in the interest of efficiency and economy, the plaintiff could request that defendant run a search according to criteria selected by plaintiff. Id. at 268.
114. See id. at 267. “The Federal Rules are designed to provide parties access to the [facts] but not the [law].” Id. The court considered the discovery request to be analogous to one seeking an order to compel opposing counsel to make available for review his superior collection of reporters. Id. at 268.
115. Id. (observing that defendant’s legal research database was a “highly valuable legal research tool and in the interests of the efficient administration of justice, defendants’ reluctance... [to reach a mutual agreement] to conduct limited search requests for the plaintiffs... seem[ed] wholly unreasonable”).
seemingly depends on two main factors: (1) the extent to which the
volume of the data facilitates or prevents revelation of the preparing
attorney's mental processes and (2) the extent to which the nature of
the data exposes or obfuscates the attorney's legal strategies. 
Production of litigation databases becomes more likely as the amount
of data hampers the ability to "extrapolate backwards from the
results of a selection process to determine the reason a document was
selected,"116 and as "the process of selecting the data becomes
increasingly mechanical."117 Alternatively:

[T]he more that a database's design reflects judgments of
counsel relating to anticipated litigation, such as by
selecting portions of documents for inclusion based on
judgments of counsel as to their importance to the litigation,
by arranging documents based on strategic priorities, and by
using indices that relate to litigation needs, the more likely
that database is to be protected from discovery by work
product immunity.118

C. Threats to Evidentiary Privileges That Are
Unresolved by the Federal Rules of Civil Procedure
and Increased by Electronic Discovery

1. Unique Characteristics of Electronic Data and
Their Practical Effects on Electronic Discovery

a. Volume

For purposes of the discovery process, electronic data differ in a
number of ways from information that is recorded on paper. The
most notable difference that affects privilege is the sheer volume of
data that can be stored electronically.119 Although traditional paper

117. See Robins, supra note 85, at 433 (1999) (citing 8A CHARLES A.
WRIGHT ET AL., FEDERAL PRACTICE AND PROCEDURE: CIVIL § 2218 (2d ed.
1994)).
118. Id.
119. See Wiginton v. C.B. Richard Ellis, Inc. No. 02 C 6832, 2004 WL
1895122, at *3 (N.D. Ill. Aug. 10, 2004) ("As contrasted with traditional paper
discovery, e-discovery has the potential to be vastly more expensive due to the
sheer volume of electronic information that can be easily and inexpensively
stored on backup media."); Medtronic Sofamor Danek, Inc. v. Michelson, 56
discovery can often involve large volumes of paper documents, electronic data systems have drastically increased the frequency with which documents are created and the volume of documents that are retained by individuals and corporations. Because parties are generally charged with the responsibility of identifying which of their own documents are privileged, any increase in number of documents renders the privilege screening process more arduous and creates a greater statistical likelihood of error, resulting in inadvertent disclosure of privileged materials.

b. Difficulty of deletion and proliferation

In contrast to paper documents, deletion of electronic documents may render the document more difficult to locate, though it usually does not irretrievably destroy the document. Thus, a party has

---

Fed. R. Serv. 3d (West) 1159, 1162 (W.D. Tenn. 2003). For example, the defendant in Medtronic requested the production of, among other electronic data, 993 backup tapes allegedly containing 61 terabytes. Id. The court noted it would take approximately 728,178 standard 3.5 inch diskettes to store one terabyte of data. Id. n.3; see also MICHELE C.S. LANGE & KRISTIN M. NIMSGER, ELECTRONIC EVIDENCE AND DISCOVERY: WHAT EVERY LAWYER SHOULD KNOW, 48 (2004) ("Electronic records present the problem of extreme volume that was previously unseen in the paper world."); Robins, supra note 85, at 416. ("[C]omputers offer a window on a broader spectrum of information than is traditionally recorded in printed documents.").

120. See Ronald J. Hedges, U.S. Mag. J., Discovery of Digital Information, at 1–2 (Sept. 27, 2004) ("Chief among [the] differences [between digital and paper discovery] is the sheer volume of electronic information."); http://www.kenwithers.com/articles/hedges092704.pdf (last updated Oct. 19, 2004); Withers, supra note 78 ("The numbers of electronic records that may be subject to discovery are reported to be huge, even in cases involving parties of relatively modest size.").


122. See Medtronic, 56 Fed. R. Serv. 3d (West) at 1177 (noting that the discovery plan involved a large quantity which rendered more likely the possibility of inadvertent disclosures); LANGE AND NIMSGER, supra note 119, at 48 (noting that where multiple reviewers screen tens of thousands or even millions of documents, "there is bound to be differences in judgment as to whether a particular document is privileged or responsive. The sheer volume of documents reviewed in a certain day can allow privileged documents to slip by unnoticed into the production set.").

123. See Withers, supra note 84.

Thoughtlessly worded e-mail messages . . . cannot be destroyed, no
sought to destroy a privileged electronic communication to ensure its confidentiality still must be concerned about the possibility of unintentionally producing copies of the document retained by the computer system.\textsuperscript{124} Similarly, proliferation of electronic files in a computer system may create a situation where there are multiple copies of an electronic document in a computer, all of which must be identified and withheld.\textsuperscript{125} The proliferation of electronic documents renders the privilege screening process more difficult in two ways. First, it augments the number of documents that must be screened for privilege, increasing the burden imposed by privilege review.\textsuperscript{126} In order to identify all copies of a privileged electronic document, litigants perform a procedure known as “de-duplication.”\textsuperscript{127} Second, matter how hard the author or recipient hits the “delete” key. E-mail is often backed-up on intermediary computers or network servers as a routine matter, and the back-up media may be kept indefinitely. The process of “deleting” seldom erases a computer file; it merely marks the file for overwriting if space is needed on the disk (which in these days of multi-gigabyte storage capacity, is almost never).

124. See Playboy Enters., Inc. v. Welles, 60 F. Supp. 2d 1050 (S.D. Cal. 1999). Although defendant customarily deleted e-mail soon after sending or receiving it, the court ordered her to resurrect and produce the e-mail communications, finding it implausible that they were irretrievable. \textit{Id.} at 1051, 1054, 1058. Defendant was concerned that some of the recovered e-mail would reveal attorney-client communications and private material. \textit{Id.} at 1054.

125. See Steven C. Bennett, \textit{E-Discovery by Keyword Search}, 15 PRAC. LITIGATOR, May 2004. (“An e-mail from a lawyer to a business executive, for example, may be duplicated and forwarded to other business executives. As a result, there may be multiple copies of the same message, all conceivably privileged.”).

126. See Hedges, \textit{supra} note 120, at 2 (“[C]omputers have the ability to capture several copies (or drafts) of the same e-mail, thus multiplying the volume of documents. All of these e-mails must be scanned for both relevance and privilege.”).

127. See Wiginton v. C.B. Richard Ellis, Inc., No. 02 C 6832, 2004 WL 1895122, at *2 (N.D. Ill. Aug. 10, 2004) (noting that de-duplication is a “process whereby documents which appear in a user’s mailbox on multiple days are not counted as multiple hits. For example, if the same e-mail appeared in an inbox over a period of several months, only one copy of the document would be produced.”); see also Medtronic Sofamor Danek, Inc. v. Michelson, 56 Fed. R. Serv. 3d (West) 1159, 1160 (W.D. Tenn. 2003). The court acknowledged in \textit{Medtronic} that duplication could complicate and impede the document review. \textit{See id.} Accordingly, the fact that discovery involved large volumes of data on multiple tapes required that “the restored files from each tape... be compared to the restored files from every other tape and duplicates eliminated...”. The de-duplication and conversion are required
a person performing a privilege review may gain a false sense of security when that person identifies one copy of the privileged communication. However, the successful identification of one copy of a privileged electronic communication will not protect [from disclosure] all copies that remain lurking in a computer system.

\[ \text{c. Metadata} \]

Unlike paper documents, electronic documents often contain data that are not represented within their four corners, such as attached documents that do not appear in a paper copy when generated. Review of the electronic document alone will not guarantee that all data associated with the document were screened for privilege. Although many common electronic file formats provide rudimentary search capabilities with “find” features that enable users to locate words or terms within a document . . . , these abilities are limited to searches within the same file format. A user cannot, for example, search through e-mail messages and their attachments at the same time in native file format.

so that large volumes of data in different formats may be searched in a reasonable time.” *Id.*

128. *See* United States v. Stewart, 287 F. Supp. 2d 461 (S.D.N.Y. 2003). Defendant sent a privileged e-mail to her attorney and later forwarded the same e-mail to her daughter. *Id.* at 463. Both e-mail communications were listed in the privilege log accompanying the documents produced in paper form. *Id.* However, on the privilege log accompanying the production of electronic data, defense attorney listed the first e-mail, but he inadvertently omitted the second e-mail communication from the privilege log. *Id.* He then disclosed it in production. *Id.* at 463–64.

129. *See* id. at 464.

130. *See* 7 MOORE ET AL. *supra* note 45, § 37A.01.

131. *See* United States v. KPMG LLP, No. 02-0295 (TFH), 2003 WL 22336072, at *5 (D.D.C. Oct., 10, 2003). In this case, although certain e-mail messages were not subject to the attorney-client privilege, the attached documents were. *Id.* Thus, a review of the e-mail alone would not have identified the privileged nature of the attachment. *See also* Doe v. Ashcroft, 334 F. Supp. 2d 471, 508–509 (S.D.N.Y. 2004) (noting that “production of [metadata such as] e-mail header information, including subject lines . . . conceivably may reveal information protected by the . . . attorney-client privilege, e.g., a communication with an attorney where the subject line conveys privileged or possibly incriminating information”).

Thus, ensuring that privileged information contained in an attached document is not produced may require the opening and reviewing of all attachments. A more technologically savvy way to resolve this problem is by enabling searches across multiple original file formats by transforming electronic documents to a common file type such as PDF or TIFF, and then indexing their full text for searching.

**d. Resurrection**

Finally, where compliance with a discovery request requires the restoration of data that are not presently stored on computer hard drives, but on computer backup tapes, the organization of the data may not be conducive to a systematic document review. The reason for the discrepancy inheres in the very purpose for creating backup copies—to prevent the irretrievable loss of data as a result of a computer system crash. In order to store the data contained in an entire computer system on a backup tape, the data are compiled so as to maximize the storage space rather than to facilitate accessibility of files and documents. Thus, whereas paper discovery is facilitated...
by business operations' general practices of filing and organizing paper documents according to one or more consistent themes such as subject matter and chronology, electronic records stored on backup tapes are not oriented in the same logical manner.\textsuperscript{137}

These differences between electronic and paper documents are particularly relevant to parties' preservation of their evidentiary privileges. In fact, inasmuch as the above characteristics generally increase the volume of information contained in electronic databases, they support the inference that there is a higher risk of unintentional disclosure of privileged information in electronic discovery.\textsuperscript{138} The ultimate danger, which varies in degree depending on the jurisdiction, is, of course, that of waiving privilege.\textsuperscript{139}

2. Traditional Methods of Protecting Privilege
   Applied to Electronic Discovery

   a. Rule 26(f) meet and confer conference

   Federal Rule of Civil Procedure 26(f) requires that before a Rule 16 conference,\textsuperscript{140} the parties:
   
   confer... to develop a proposed discovery plan that indicates the parties' views and proposals concerning: 
   (3) what changes should be made in the limitations on discovery imposed under these rules or by local rule, and

   uploading onto a computer system.” (quoting Kenneth J. Withers, Computer-Based Discovery in Federal Civil Litigation, 2000 FED. CT. L. REV. 2, 5)).


   138. See Bennett, supra note 125, at 9 (“With vast electronic records... there is a grave risk that some privileged records may slip through the review process.”).

   139. See Withers, supra note 35, at 35.

   140. Rule 16 provides in part that:

   [T]he court may in its discretion direct the attorneys for the parties... to appear before it for a conference or conferences before trial for such purposes as... (2) establishing early and continuing control so that the case will not be protracted because of lack of management; [and]

   (3) discouraging wasteful pretrial activities.

   FED. R. CIV. P. 16(a). During any Rule 16 conference, “consideration may be given, and the court may take appropriate action, with respect to... (6) the control and scheduling of discovery, including orders affecting disclosures and discovery pursuant to Rule 26.” Id. 16(c).
what other limitations should be imposed; and (4) any other orders that should be entered by the court under Rule 26(c) or Rule 16(b) and (c).141

As applied to electronic discovery, the Rule 26 “meet and confer” should include a discussion on whether each side possesses information in electronic form [and] whether . . . there exists any privilege issue requiring redaction. . . .”142 This rule has been construed to offer a special opportunity to parties’ counsel “to discuss issues associated with electronic discovery,”143 including whether or not the inadvertent disclosure of privileged documents should result in waiver.144

There are several kinds of protective measures that parties should begin to discuss together at the meet and confer. Keyword searches may be used to assist the attorney in performing the

---

141. Id. 26(f).
142. In re Bristol-Meyer Squibb Sec. Litig., 205 F.R.D. 437, 444 (stressing the importance of counsel’s duty to take advantage of the Rule 26(f) conference to alert opposing counsel of the existence of electronic data and to discuss methods and costs of privilege protection). The amendment to Rule 26(f) calls for discussion of whether the parties can agree on an approach to production that protects against privilege waiver. See PROPOSED AMENDMENTS AND COMM. NOTES, supra note 38, at 6.
143. Id.; see Hon. John H. Hughes New Jersey Local Rule Mandates Common Sense Approach, E-DISCOVERY STANDARD, Summer 2004, at 6. In response to a question asking what the most common mistakes attorneys make with regard to electronic discovery, Judge Hughes commented: “The biggest problem is that lawyers discuss electronic discovery issues too generally at the Rule 26(f) conference. They are not maximizing the benefits of the conference. They should discuss the specifics there, including [issues such as privilege].” See id. One judge has even expressed in an opinion his dismay with the failure of attorneys to discuss and resolve issues regarding electronic discovery and privilege. See Ind. Coal Council v. Hodel, 118 F.R.D. 264, 268 (D.D.C. 1988) (stating in regard to an electronic discovery dispute that “[i]t was] unfortunate that . . . an agreement could not have been reached several months [before] when th[e] issue was first raised”).
144. In its draft amendments of the FRCP addressing electronic discovery, the Advisory Committee proposed an alteration to Rule 26(f) that requires parties to consider the consequences of inadvertent production of privileged information. See PROPOSED AMENDMENTS AND COMM. NOTES, supra note 38, at 8–9. The suggested addition to Rule 26(f) provides that the parties must confer “to develop a proposed discovery plan that indicates the parties’ views and proposals concerning: . . . (4) whether, on agreement of the parties, the court should enter an order protecting the right to assert privilege after production of privileged information.” Id.
traditional process of privilege screening. Once privileged documents are identified, the parties can create a privilege log to warn of the existence of privileged documents and to communicate the basis for the claim. In addition to these common precautionary measures, the parties should discuss the consequences of inadvertent production and the possibility of preserving privilege claims despite inadvertent disclosure. Finally "[t]he results of these discussions are to be included . . . in the discovery plan presented to the court."  

b. Keyword searches

Although the unique characteristics of electronically stored information renders more burdensome the task of screening for privileged information, computer systems have features that mitigate the negative effects of document proliferation. For example, computer features that permit the search of electronic data by keywords or specific terms generally facilitate identification of privileged documents. In fact, "[b]road database searches may be 

---

145. Lisa Arent et al., E-Discovery: Preserving, Requesting & Producing Electronic Information, 19 SANTA CLARA COMPUTER & HIGH TECH. L.J. 131, 167–68 (2002) ("As part and parcel of 'meet and confer,' you might . . . consider methods to search for responsive information.").

146. See discussion supra Part V.A.3.

147. See Withers, supra note 35, at 32. Rather than formulating a rule which would specify the consequence of an inadvertent disclosure of privileged information, "the committee proposes that the parties discuss these issues, attempt to reach agreement, and come to the court if there is need for a court order to address . . . privilege." Id.


149. See Hon. John M. Facciola, Practice Tips from the Bench: Come to Court Prepared, E-DISCOVERY STANDARD, Summer 2004, at 8 ("Many people argue that electronic discovery is more difficult than paper discovery, but the advantages of full-text searching, the ability to sort and organize, and other electronic review functions make it much easier than paper review.").

150. See Bennett, supra note 125, at 11 ("[I]n a bulky electronic records collection, keyword searching may greatly improve the efficiency of the process."); Arent et al., supra note 145, at 168 ("Some e-mail systems have search functions that could expedite the process; also, there may be software to help search databases."); see also Wiginton v. C.B. Richard Ellis, Inc., No. 02 C 6832, 2004 WL 1895122, at *8 (N.D. Ill. Aug. 10, 2004) (advocating keyword searches as a cost effective method of performing privilege reviews without having to examine each document).
necessary, requiring safeguards against exposing confidential or irrelevant data to the opponent’s scrutiny.\textsuperscript{151}

At a minimum, keyword searches can be used to identify documents that are responsive. Keyword searching may “[limit] the scope of documents that must be reviewed,”\textsuperscript{152} thus, “reduce[ing] the volume of records that need to be reviewed for privilege.”\textsuperscript{153} For example, a preliminary keyword search that may efficiently identify privileged documents would target the terms “privileged” or “confidential.” It may, however, be unlikely that all privileged electronic communications are marked by such language.\textsuperscript{154} To increase the chances of identifying privileged communications, more sophisticated searches can be run that target documents containing the names of attorneys, a party’s in-house counsel, or issues that have been the subject of legal representation of the parties.\textsuperscript{155}

Keyword searching may, however, be fraught with technical difficulties, especially where resurrected data are concerned.\textsuperscript{156} For example, if a keyword search program is not compatible with the computer operating system, the hits may only indicate the physical location of the file (the sector address), but not the logical location (the file name and directory).\textsuperscript{157} In such cases, a searcher may have

\begin{itemize}
\item \textsuperscript{151} Manual for Complex Litigation § 11.446 (4th ed. 2004).
\item \textsuperscript{152} Sidney K. Kanazawa, Rethinking Discovery and Document Retention in the Digital Age, 13 PRAC. LITIGATOR, Jan. 2002, at 47.
\item \textsuperscript{153} Bennett, supra note 125, at 11–12.
\item \textsuperscript{154} Furthermore, some electronic documents bearing such labels may not actually be privileged. For a discussion of courts’ reactions to unfounded privilege claims asserted as to e-mail, see supra Part V.B.1.a.
\item \textsuperscript{155} See Bennett, supra note 125, at 10 (describing how to conduct a keyword search).
\item \textsuperscript{156} In re Bridgestone/Firestone, Inc., No. IP 00-9373-C B/S, MDL Docket No. 1373, 2001 WL 34131187, at *2 (S.D. Ind. Mar. 16, 2001) ("\textquote{W}ord search technology is not 100\% accurate; for example, handwritten words and documents which did not scan clearly may not be included in search results . . . . [W]here abbreviations are commonplace . . . [a party] would have no way of knowing whether they had developed a complete list of all interchangeable terms."); see also Massachusetts v. Ellis, Nos. 97-192, 97-562, 98-355, 97-193, 97-561, 97-356, 97-563, 1999 WL 815818, at *3–4 (Mass. Super. Ct. 1999) (recounting how technical difficulties complicated the computer expert’s keyword search).
\item \textsuperscript{157} See, e.g., Ellis, 1999 WL 815818 at *4. The court appointed a computer expert to perform searches of defendant’s computer server. Id. at *1. After resurrecting previously deleted data, the expert began a file-by-file search of directories according to search terms pre-defined in a search warrant.
\end{itemize}
to use the "view" function to examine responsive files visually. 158 Perhaps such difficulties can be avoided by restoring resurrected files to a common format so that a search program may properly seek information within them. 159

Thus, keyword searches constitute a tool that enables parties to overcome the increased burden of screening large volumes of electronic records to prevent disclosure of privileged information. However, the capacity of searches to prevent disclosures of privileged documents should not be overestimated. Ensuring reasonable measures have been taken to prevent an inadvertent disclosure may still require a manual review of all documents that are found to be responsive. 160 In the end, the costs involved in performing keyword searches, compounded by the costs parties may have to incur in performing a manual privilege review, will generally render the protection of privilege one of the most costly endeavors of litigation. 161

---

158. Id. at *3. The search only located the sector address of the hits. Id. at *4.
159. See Medtronic Sofamor Danek, Inc. v. Michelson, 56 Fed. R. Serv. 3d (West) 1159, 1160 (W.D. Tenn. 2003). The judge warned that before designing and applying a search program, preliminary steps must be performed. See id. First, "[a]ll data on each backup tape must be restored . . . to a format that a standard computer can read." Id. Second, restored files "must be converted to a common format so that a search program may seek information within them." Id.
161. See Kenneth J. Withers, Electronic Discovery Disputes: Decisional Guidelines, CIVIL ACTION, Summer 2004, at 6 ("To some extent technology can ease the burden by helping counsel identify particular authors, recipients, or terms. But in the end, attorneys will need to manually review tens of thousands (if not millions) of e-mail messages, word-processing documents, and other files to make privilege determinations."); see also Medtronic, 56 Fed. R. Serv. 3d (West) at 1169 (acknowledging an estimate that privilege screening alone would cost between sixteen and seventy million dollars); Computer Assocs. Int'l Inc. v. Quest Software Inc., 56 Fed. R. Serv. 3d (West) 401, 402 (N.D. Ill. 2003) (noting that the estimated cost of copying and conducting a privilege search of eight hard drives would be between $38,000 and $40,000); Rowe Entm't, Inc. v. William Morris Agency Inc., 205 F.R.D. 421, 432 (S.D.N.Y. 2002) (stating that one defendant estimated the cost of conducting a privilege review would be $250,000, while another projected a
3. Innovations in Privilege Protection:  
Stipulated Confidentiality Agreements

Because of the difficulty of protecting privileged matters in the context of electronic discovery, litigants increasingly enter into agreements that address the question of whether inadvertent disclosure of a document will constitute a waiver. Among the types of arrangements providing greater assurances against privilege waiver are the “claw back” agreements and “quick peek” agreements.162

a. “Claw back” agreements

A “claw back” arrangement consists of an agreement between the parties to disclose documents after a privilege review with the understanding that they can promptly demand the return of any privilege document that has been inadvertently disclosed.163 “Claw back” arrangements have become a “common practice in complex litigation.”164 Before entering a protective order that sanctions a “claw back” agreement, a court may order the parties to follow an exacting discovery protocol.165 The discovery plan may divide the task of privilege review in multiple segments, promoting a more fluid and efficient discovery process.166 This phased approach to privilege review encourages the producing party to adhere to a steady but disciplined privilege review, while allowing for an opposing party to receive responsive material earlier and in quantities more conducive to consistent analysis. Additionally, adherence to a

162. For a discussion of “quick peek” arrangements, see infra Part V.C.3.b.
163. See Withers, supra note 161, at 6.
164. Withers, supra note 35, at 26. See Joseph, supra note 38 (stating it is a “commonly-entered agreement that inadvertent production of privileged document will not effect a waiver”).
165. See Medtronic, 56 Fed. R. Serv. 3d (West) at 1171-76. The court ordered discovery pursuant to a “claw back” protocol after delineating an exhaustive discovery plan. Id. at 1176-77. The discovery plan required that the defendant perform a keyword search using terms approved by the court or mutually agreed upon by the parties. Id. at 1172, 1174. Defendant’s next step under the protocol was separating the files identified in the privilege search into five sections of equal size. Id. at 1172, 1175. The defendant would then review the files in five separate phases for responsiveness and privilege. Id. at 1173, 1175.
166. See id.
cautious privilege screening process may justify in the eyes of the court a protective order providing that inadvertent disclosure does not constitute a waiver.167

Protective orders endorsing the "claw back" approach may contain a provision directing that any documents produced by a party after the privilege review be marked "Confidential—Attorneys' Eyes Only."168 The court should include instructions that "[t]he deliberate or inadvertent disclosure of any document to... an expert or vendor does not waive privilege with regard to that document."169 Additionally, the court may direct the receiving party to notify the producing party immediately of any document that appears to be privileged, whereupon the producing party should promptly respond by indicating whether or not privilege is asserted with respect to that document.170

b. "Quick peek" agreements

Perhaps the most controversial of the stipulated agreements between the parties is one enabling the opposing party to review the producing party's documents for relevance before any privilege review has taken place.171 Under this type of agreement, the responding party engages in a privilege review of a reduced amount of documents after the requesting party has taken a "quick peek" of the electronic documents and has identified those that are responsive.172 The "quick peek" approach to electronic discovery

167. See id. at 1177 (noting that "[g]ood cause exists [for the protective order] because the volume of data that will be produced by electronic discovery will make it difficult for the producing party to identify with certainty every potentially privileged document prior to production").

168. Id.

169. Id.

170. Id.

171. This type of agreement is still very rare and has been referred to as "esoteric." See Joseph, supra note 38; see also Withers, supra note 35, at 37 (describing the "quick peek" arrangement as a "sort of procedural high-wire act... [requiring] an extremely high level of trust between the parties").

172. See Rowe Entm't, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, 432–33 (S.D.N.Y. 2002). The court proposed Defendant make hard drives and backup tapes available to Plaintiff for mirror imaging. Id. at 433. Plaintiff, in possession of the requested e-mail messages, would then perform word searches using terms mutually agreeable to the parties. Id. Plaintiff would review e-mail messages identified by the search for relevance on an "attorney's-eyes-only basis." Id. At this point, the court indicated that
PRIVILEGE & THE ECPA

reduces costs for the producing party by placing the initial burden of identifying relevant documents on the opposing party. For this reason, the court may develop a “quick peek” proposal in response to a producing party’s argument that compliance with opposing party’s discovery request is unduly burdensome due to the costs of privilege review.

The feasibility of the “quick peek” arrangement depends largely, even more so than in the “claw back” context, on the court’s provision of a protective order preventing against waiver by voluntary disclosure of documents. Courts have, however, recognized that they cannot compel parties to adhere to a “quick peek” arrangement, noting protective orders may be an inadequate substitute for privilege reviews. Thus, a court may suggest the “quick peek” option as merely a “set of guidelines.” Accordingly, courts may allow a producing party to reject the “quick peek”

defendant would have the opportunity to review for privilege documents identified by plaintiff as responsive. Id.

173. See Withers, supra note 35, at 37 (noting that the “quick peek” approach “can result in tremendous cost savings for both parties”).

174. See Rowe Entm’t, Inc., 205 F.R.D. at 432–33. In response to defendant’s argument that the costs of reviewing requested e-mail messages for privilege review constituted an undue burden, the court suggested that “[t]he sanctity of the defendants’ documents [could] be adequately preserved at little cost by enforcement of the confidentiality order and by the . . . [‘quick peek’] protocol.” Id. at 432.

175. See id. at 433 (providing “the fact that . . . a document has been reviewed by counsel or by the expert shall not constitute a waiver of any claim of privilege or confidentiality”); Withers, supra note 35, at 37 (suggesting that the “quick peek” agreement requires a “strong safety net” that may be provided by a case management order).

176. See In re Down Corning Corp., 261 F.3d 280, 284 (2d Cir. 2001). The court conceded that “compelled disclosure of privileged attorney-client communications, absent waiver or an applicable exception, is contrary to well established precedent.” Id. “[W]e have found no authority . . . that holds that imposition of a protective order like the one issued by the district court permits a court to order disclosure of privileged attorney-client communications . . . . [A] protective order is an inadequate surrogate for the privilege.” Id.; see also Rowe Entm’t, Inc., 205 F.R.D. at 432 (observing that “even with [the provision of protective orders], however, the disclosure of privileged documents cannot be compelled”); PROPOSED AMENDMENTS AND COMM. NOTES, supra note 38, at 21 (emphasizing the voluntary nature of the “claw back” and “quick peek” agreements).

177. See Rowe Entm’t, Inc., 205 F.R.D. at 432.
proposal and choose to perform their own privilege review according to more traditional methods.\textsuperscript{178}

c. Dual option: "claw back" or "quick peek"

Courts may also propose a "claw back" arrangement as one of two alternatives, the other being a "quick peek" arrangement.\textsuperscript{179} A court's willingness to enter a protective order preventing against waiver in the event privileged documents are disclosed may depend upon the option the producing party chooses.\textsuperscript{180} For example, the court may decline to enter a protective order if the party chooses the "claw back" rather than the "quick peek" alternative.\textsuperscript{181} This reflects the notion that if a party insists on performing a privilege review before producing documents, that party should bear the risk that inadvertent disclosure may constitute a waiver.\textsuperscript{182} On the other hand, if the party is willing to place its trust in the hands of the court and the opposing party, in the interest of the increased efficiency afforded by the "quick peek" arrangement, the party may receive the

\textsuperscript{178} See id. at 433. Defendants could elect to review their own electronic data, producing to plaintiff a privilege log along with hard drives and backup tapes from which irrelevant and privilege materials have been erased. Id. On the other hand, defendants could turn over the electronic documents before conducting a privilege review. See also Gambale v. Deutsche Bank Ag, No. 02 Civ. 4791 HB DFE, 2002 WL 31655326 at *1 (S.D.N.Y. Nov. 21, 2002) (providing the producing party with a choice between following a "claw back" discovery plan, similar to the one adopted in Rowe, and submitting a different discovery protocol agreed to by both parties).

\textsuperscript{179} See Murphy Oil USA, Inc. v. Fluor Daniel, Inc., 52 Fed. R. Serv. 3d (West) 168, 179–81 (E.D. La. 2002) (providing that Defendant could produce documents pursuant to a "quick peek" agreement (option one) or to a "claw back" agreement (option two)); Rowe Entm't., Inc., 205 F.R.D. at 432; Gambale, 2002 WL 31655326, at *1.

\textsuperscript{180} See Murphy Oil, 52 Fed. R. Serv. 3d (West) at 179–81 (providing more protection against waiver under the "quick peek" option than under the "claw back" option).

\textsuperscript{181} See id. at 179 n.3. In contrast to the court in Medtronic Sofamor Danek, Inc. v. Michelson, 56 Fed. R. Serv. 3d (West) 1159 (W.D. Tenn. 2003), the court in Murphy Oil expressly denied to grant an attorney's-eyes-only provision in the event Defendant chose the "claw back" option. Murphy Oil, 52 Fed. R. Serv. 3d (West) at 179 n.3. Furthermore, unlike the court order for the "quick peek" arrangement, the court order for the "claw back" arrangement did not include a provision protecting against waiver of privilege in the event the defendant inadvertently produced a privileged document. Id. at 180–91.

\textsuperscript{182} See id.
court’s assurance that production will not constitute a waiver.¹⁸³

Some courts, however, will not expressly condition a protective order on selection of the “quick peek” option.¹⁸⁴ Nonetheless, a producing party should urge the court to use language that clearly provides for a non-waiver provision in either case. Lack of clarity in this respect creates uncertainty as to whether the producing party will be entitled to the same protective provisions in the event a privilege document is inadvertently produced pursuant to the “claw back” as opposed to the “quick peek” option.¹⁸⁵

d. Special masters and neutral computer experts

In cases involving complex electronic discovery issues, parties may agree to the appointment of a neutral computer expert or special master¹⁸⁶ under a duty to facilitate protocols such as those endorsing the “claw back” and “quick peek” methods.¹⁸⁷ For example, courts

¹⁸³. See id.
¹⁸⁴. See Rowe Entm’t, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, at 432–33 (S.D.N.Y. 2002). The “quick peek” option included an attorney’s-eyes-only provision and an order ensuring production of privileged documents would not constitute a waiver or privilege. Id. In the event Defendants chose to review the electronic data for privilege before turning it over to Plaintiff, the court indicated that the “process would then continue as described above,” under the “quick peek” option. Id.

This language seems to indicate any privileged documents produced under the “claw back” approach would be treated in the same manner as documents produced under the “quick peek” arrangement. Thus, in either case, produced documents would be subject to the attorney’s-eyes-only provision and any production of any privileged documents would not constitute a waiver.

¹⁸⁵. See id. at 432–33. The court’s use of vague language (“process would then continue as described above”) created uncertainty as to whether the Defendants would be entitled to the same protective provisions as were provided under the “quick peek” option. Id.; see also, Murphy Oil, 52 Fed. R. Serv. 3d (West) at 179 n.3. At the least, litigants in Murphy Oil enjoyed the certainty provided by the court’s statement that the attorney’s-eyes-only provision intended to protect against dissemination of defendants’ privileged documents by plaintiff would only be in place if defendants chose the “quick peek” rather than the “claw back” arrangement. Id.

¹⁸⁶. “The court in which any action is pending may appoint a special master therein. As used in these rules the word ‘master’ includes a referee, an auditor, an examiner, and an assessor.” FED. R. CIV. P. 53(a). “A reference to a master shall be the exception and not the rule.” Id. 53(b).

¹⁸⁷. See Withers, supra note 161, at 6 (“When the parties cannot come to agree on a privilege protection protocol, particularly when discovery involved
and litigants have relied on computer experts to retrieve electronic data from storage devices as well as to perform the technical procedures necessary to search electronic data. Courts generally provide that the computer expert should be designated either by mutual agreement of the parties or selected by the court from a list of experts provided by the parties.

Reliance on a neutral computer expert for the retrieval and searching of data for privilege and relevance naturally requires a litigant to permit the third party to access potentially privileged documents. In order to protect litigants against claims that any

the production of a computer itself and review of all the files on the computer’s hard drive, many courts have resorted to the use of a neutral expert.”). Where parties can agree to on a neutral expert, a special master does not need to be appointed by the court. See Medtronic Sofamor Danek, Inc. v. Michelson, 56 Fed. R. Serv. 3d (West) 1159, 1171 (W.D. Tenn. 2003) (appointing a special master to oversee the “claw back” discovery protocol); Rowe Entm’t, Inc., 205 F.R.D. at 433 (deciding to appoint a computer expert to oversee production pursuant to a “quick peek” agreement); Murphy Oil, 52 Fed. R. Serv. 3d (West) at 179 (appointing computer expert to oversee either the “quick peek” or “claw back” discovery process.); see also Playboy Enters., Inc. v. Welles, 60 F. Supp. 1050, 1054–55 (S.D.N.Y 1999). The court in Playboy Enterprises took it upon itself to develop an electronic discovery protocol overseen by a computer expert either designated by the court or appointed by the parties. See id.

188. See Medtronic, 56 Fed. R. Serv. 3d (West) at 1171 (“Given the amount of electronic data at issue, the court finds that the appointment of a special master to oversee discovery is warranted and that the special master should be a technology or computer expert.”); see also Rowe Entm’t, Inc., 205 F.R.D. at 433 (ordering plaintiff’s expert to obtain a mirror image of hard drives and back-up tapes); Murphy Oil, 52 Fed. R. Serv. 3d (West) at 179 (ordering that an expert retrieve selected data from backup tape); Playboy Enters., Inc., 60 F. Supp 2d at 1055 (S.D. Cal. 1999) (ordering the expert to determine whether deleted e-mail messages could be resurrected and to create a mirror image of defendant’s hard drive).

189. See Medtronic, 56 Fed. R. Serv. 3d (West) at 1171 (instructing the parties to reach an agreement on the designation of a special master and providing in the alternative that the court would appoint a special master from lists provided by both parties); Rowe Entm’t, Inc., 205 F.R.D. at 433 (instructing the plaintiff to designate a computer expert and giving defendant an opportunity to object to the designation); Murphy Oil, 52 Fed. R. Serv. 3d (West) at 179 (instructing the plaintiff to designate a computer expert and giving defendant an opportunity to object to the designation); Playboy Enters., Inc., 60 F. Supp. 2d at 1055 (requesting the parties meet and confer to agree on the designation of a computer expert and providing if the parties failed to agree that the court would select one from candidates chosen by the parties).
privilege was waived by disclosure to a third party, courts have issued protective orders complementing any appointment of a computer expert to assist in electronic discovery. Courts may rely on special masters and neutral computer experts particularly where parties have engaged in spoliation of electronic data to evade producing documents responsive to opposing counsel's discovery requests.

4. Protective Orders

Protective orders are essential to the cooperation of the parties in creating innovative and effective electronic discovery plans. Pursuant to FRCP 26(c), a party may solicit the court to "make any order which justice requires to protect a party or person from annoyance, embarrassment, oppression or undue burden or expense."

190. See Medtronic, 56 Fed. R. Serv. 3d (West) at 1177 ("[T]he neutral computer expert[] shall be bound by the terms of any and all confidentiality agreements and protective orders now in place, or to be put in place in the future . . . ."); Rowe Entm't., Inc., 205 F.R.D. at 433 (indicating that privilege claims would not be waived as to documents reviewed by the expert); Murphy Oil, 52 Fed. R. Serv. 3d (West) at 180; Playboy Enters., Inc. 60 F. Supp. 2d at 1055 ("To the extent the computer specialist has direct or indirect access to information protected by the attorney-client privilege, such 'disclosure' will not result in a waiver of the attorney-client privilege.").

191. See Playboy Enters., Inc., 60 F. Supp. at 1051 (determining it would appoint a neutral computer expert after defendant had pursued a practice of deleting in and out-going e-mail messages despite the fact that the "e-mails [were] responsive to Plaintiff's request for production of documents").

192. See Withers, supra note 35, at 37 ("A case management order may be useful in shielding the parties from the worst consequences of well-intentioned efforts to reduce the potential cost and delay of privilege screening . . . .").

193. FED. R. CIV. P. 26(c). Among the types of orders that the Federal Rules has anticipated the court may issue are:

(1) that the disclosure or discovery not be had; (2) that the disclosure or discovery may be had only on specified terms and conditions, including a designation of the time or place; (3) that the discovery may be had only by a method of discovery other than that selected by the party seeking discovery; (4) that certain matters not be inquired into, or that the scope of the disclosure or discovery be limited to certain matters; (5) that discovery be conducted with no one present except persons designated by the court; (6) that a deposition, after being sealed, be opened only by order of the court; (7) that a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a designated way; and (8) that
While courts have readily adopted protective orders where parties have worked together and with the court to reach a feasible electronic discovery protocol, courts will endorse a blanket protection against waiver of privilege through inadvertent disclosure without some showing that efforts will be made to protect the privilege.  

All three of the scenarios discussed above—the "claw back" and "quick peek" arrangement, as well as the use of a neutral expert or special master to conduct electronic discovery—raise one question on which courts have largely remained silent. Even subject to a protective order, does the disclosure of privileged information by a litigant to opposing counsel, a neutral computer expert or a special master, waive the claim of privilege as to a third party not bound by the protective order in a parallel or subsequent litigation? Perhaps the parties simultaneously file specified documents or information enclosed in sealed envelopes to be opened as directed by the court.  

Id.; see also Playboy Enters., Inc., 60 F. Supp. 2d at 1053 ("The only restriction in [electronic discovery] is that the producing party be protected against undue burden and expense and/or invasion of privileged matter.").  

194. See Holland v. GMAC Mortgage Corp., No. 03-2666-CM, 2004 WL 1534179 (D. Kan. June 30, 2004). The parties sought a protective order allowing them to designate as confidential all computer records or other confidential electronic information. Id. at *1. Noting that "the decision to enter a protective order lies within the sound discretion of the court," the court declined to adopt such protective order. Id.; see also Rowe Entm't., Inc., 205 F.R.D. at 428 (finding a blanket protective order against discovery of defendant's e-mail messages was unwarranted considering the confidentiality order was adequate to protect defendant's privilege interests); Ciba-Geigy v. Sandoz Ltd., 916 F. Supp. 404, 406 (D.N.J. 1995). Before issuing a protective order effectuating a "claw back" arrangement, the court noted that it had rejected the "'blanket' inadvertent disclosure clause advocated by plaintiff's counsel, and insisted that any such provision would not excuse the parties from conducting a privilege review prior to the production of documents, in accordance with controlling case law." Id. Subsequently, when defendants inadvertently produced privileged information from a litigation database, the court rejected the contention that that "the Protective Order immuniz[ed] all [unintentional] disclosures against any waiver argument." Id. at 408.  

195. See Eric Van Buskirk, Practical Strategies for Digital Discovery: Preliminary Considerations, 52 THE DIGITAL DISCOVERER, Feb. 2003, at 4 ("Prior to seeking the order of protocol, counsel should investigate the degree to which non-parties will be bound by it. Even if parties stipulate that waiver is restricted to a particular suit, courts in subsequent or parallel litigations are not bound by and might not respect the stipulation."). In his article, Ken Withers stated:
this is one of the uncertainties influencing the courts to conclude that “quick peek” arrangements cannot be forced upon unwilling litigants.

Although case law on this topic is scarce, particularly in the electronic context, recent case law in the context of paper discovery suggests no waiver occurs where “documents [are] produced... under a protective order, stipulation or other express reservation of the producing party’s claim of privilege as to the material disclosed.” Production of privileged documents under such circumstances has been likened to the court compelled disclosure of privileged documents for in camera review which cannot possibly effect a waiver. It is argued this approach promotes the letter and the spirit of the FRCP as provided by Rule 37(a)(2), requiring parties to confer before bringing a motion to compel, and by Rule 1, requiring that the Federal Rules be construed to secure the “just, speedy, and inexpensive determination” of controversies. Although it is unclear what the consequences that the innovative approaches to electronic discovery will have on privilege claims, perhaps this reasoning will provide some guidance to courts confronting the issue.

D. Waiver of Privilege by Inadvertent Disclosure: The Three Different Tests and the Significance of the Electronic Medium

If the “specter” of inadvertent disclosure has always plagued attorneys involved in discovery, it becomes even more harrowing

---

196. See Rowe Entm’t, Inc., 205 F.R.D. at 432; Murphy Oil USA, Inc. v. Fluor Daniel, Inc., 52 Fed. R. Serv. 3d (West) 168, 177 (E.D. La. 2002).
198. Id.
199. Id.
in the context of electronic discovery.\textsuperscript{201}

The problem of privilege review centers on its corollary in many jurisdictions: the consequences of inadvertent production of privileged information that have been overlooked in the mass of otherwise relevant and producible data. This problem predates the advent of electronic discovery, of course but it has been brought into sharp focus in recent years. The volume of electronically stored information has increased exponentially, resulting in productions of e-mail messages, word processing files, and other data equivalent to tens of millions of pages of conventional paper documents. Depending on the jurisdiction and the facts of each case, the consequences of inadvertently producing privileged information can mean that the privilege is deemed waived as to that document, to that category of privileged documents, to all privileged documents related to that issue, or perhaps to all privileged documents related to the case.\textsuperscript{202}

Courts are split among three different theories of the effect that the inadvertent production of a document has on a litigant’s claim to privilege.\textsuperscript{203} The most unforgiving approach provides that any disclosure of a privileged document, whether intentional or inadvertent, constitutes a waiver of the privilege.\textsuperscript{204} The most lenient

\textsuperscript{201} David Shub, \textit{The e-discovery edge: Expertise and Preparation Can Save Millions}, at 6 (2003), (“Any document production carries the risk of inadvertent waiver of the attorney-client privilege, but electronic document productions heighten that risk. When producing a mountain of e-mail messages with myriad attachments, the danger that an otherwise protected attorney-client communication may be missed and mistakenly produced rises dramatically.”), \textit{at} http://www.dtiglobal.com/pdf_articles/The\%20E-Discovery\%20Edge\%20Expertise\%20and\%20Preparation\%20Can\%20Save\%20Millions.pdf.

\textsuperscript{202} See Withers, \textit{supra} note 35, at 35–36.


\textsuperscript{204} The D.C. Circuit and the Federal District Court for the state of Maine have endorsed this approach. See Bowles v. Nat'l Ass'n of Home Builders, 224 F.R.D. 246, 253 (D.D.C. 2004). Defendant sought to recover several e-mail communications from the Plaintiff. \textit{Id.} The court observed that “[t]he D.C. Circuit follows a ’strict rule on waiver of privileges.’” \textit{Id.} (quoting SEC v. Lavin, 111 F.3d 921, 929 (D.C. Cir. 1997)). “A client wishing to preserve the privilege ‘must treat the confidentiality of attorney-client communications like jewels—if not crown jewels.”’) \textit{Id.} (quoting \textit{In re} Sealed Case, 877 F.2d 976, 980 (D.C. Cir. 1989)); FDIC v. Singh, 140 F.R.D. 252, 253 (D. Me. 1992)
approach defines waiver as an intentional and knowing relinquishment, and thus, holds that the attorney-client privilege can be waived through inadvertence. The possibility that an inadvertent disclosure could take place in the context of electronic discovery would probably have little bearing on the result produced by either of these absolute approaches.

The third and more moderate approach permits the court to balance five factors in order to determine whether inadvertent disclosure of privileged documents results in a waiver. The factors are: (1) the reasonableness of the precautions taken to prevent the inadvertent disclosure; (2) the time taken to rectify the error; (3) the volume of discovery versus the extent of the specific disclosure at issue; (4) the extent of disclosure; and (5) whether the overriding interests of justice would be served by relieving a party of its error. Because electronic discovery poses unique risks of inadvertent disclosure, perhaps the outcome of this test would be affected by its application in the electronic context. The factors on which, as a practical matter, electronic discovery probably has the most influence are the adequacy of the precautions, the scope of the disclosure relative to the volume produced, and the extent of the disclosure.

1. Reasonable Precautions

In the context of electronic discovery, litigants can take various technical measures to prevent inadvertent disclosures that go beyond manual review and segregation of privileged documents from responsive documents. Keyword searches discussed above in Part C represent one such measure. Another way to prevent against

("[W]hen a document is disclosed, even inadvertently, it is no longer held in confidence despite the intentions of the party . . . . One cannot 'unring' a bell.").


207. For cases applying the five factor test, see Keystone Sanitation, 885 F. Supp. at 676; Rigas, 281 F. Supp. 2d at 738.

208. For a discussion on the use of keyword searches to perform initial screening of documents for privilege, see supra Part V.C.2.b.
inadvertent disclosure is isolating responsive files on hard drives immunized from deletion or addition. This prevents inadvertent disclosures by making it impossible to create new possibly privileged documents on hard drives containing documents designated for production. A court may also consider whether a party has arranged for the production process to be handled by information technology specialists and has obtained assurances of their security measures. In some instances, prudence may call for supervision of the information technology (IT) specialists to ensure that they don’t access non-responsive data. Accounts containing sensitive data known to be privileged should be password protected. Finally, although protective orders providing that inadvertent disclosure do not constitute waivers may not be binding on third parties, they would probably favor a finding that reasonable precautions had been taken to avoid waiver of privilege.

If despite such precautionary steps a party inadvertently discloses electronic documents, the producing party will probably be found to have adopted reasonable precautions to prevent the disclosure. In fact, courts may use this factor to take into

---

209. See Rigas, 281 F. Supp. 2d at 739.
210. See id.
211. See id. at 738.
212. See id.; see also Entry Regarding Inadvertently Disclosed Document at 3, In re Bridgestone/Firestone, Inc., Tires Prod. Liab. Litig., Master File No. IP No. 00-9373-C-B/S (S.D. Ind., entered Oct. 10, 2001) (MDL No. 1373), at http://www.insd.uscourts.gov/Firestone/bf_docs/93731739.pdf (“[O]ne might certainly question whether Ford sufficiently supervised its outside vendors and had adequate procedures in place ... to prevent ... inadvertent productions from occurring.”).
213. See Rigas, 281 F. Supp. 2d at 738.
214. See PROPOSED AMENDMENTS AND COMMENTARY, supra note 38, at 15 (“Orders entered [pursuant to the Rule 26(f) conference] may bear on whether a waiver has occurred.”).
215. See Rigas, 281 F. Supp. 2d at 738–39. The government obtained defendant’s hard drives and was reviewing them prior to defendant’s demand that the government produce a copy of the hard drives to defendant. Id. at 735. The government took adequate precautions to ensure that its own files would not be intermingled with the electronic data on defendant’s hard drives. Id. at 740. For example, the government directed its IT staff to install the defendant’s material on computer terminals designated to screening defendant’s files. Id. at 738. The hard drives of these terminals were to be partitioned in such a manner as to prevent the people screening the material from writing government files on to the hard drives. Id. at 739. Government
consideration the technical difficulties that might impair a producing party’s ability to foresee and guard against inadvertent disclosures.216

2. The Scope of the Discovery

Because electronic discovery often entails the production of immense amounts of electronically stored data, this factor will frequently weigh in favor of a finding of no waiver.217 In order to tip the balance in one’s favor on this factor, a party should bring the scope of discovery to the court’s attention before production and should avoid rushing production where there is no immediate deadline for completion.218 Additionally, because keyword searches often produce an inexact forecast of responsive documents, parties disputing the issue of waiver may be able to characterize the scope of production in a manner that supports their particular positions.219

user accounts were password protected and maintained on a secure network. Id. at 738. The computer vendor hired by defendant to copy the government hard drives containing the seized material performed this task under government supervision. Id. Nonetheless, due to the inadequate partitioning of the hard drives by the government IT staff, the copy obtained by defendant contained an entire government user account. Id. at 739.

216. Id. (considering that although in hindsight the government could have prevented the disclosure, it occurred as a result of a rare technical occurrence which could not have been foreseen at the time of production).

217. See id. at 741. The court reached this conclusion where the government produced a “tremendous” volume of discovery documents, including “hundreds of CD ROMs” and numerous hard drives. Id. at 740–41. The court considered the 130 replicated files produced by the government were insignificant in comparison to the overall volume of production. Id. at 741.

218. See United States v. Keystone Sanitation Co., Inc., 885 F. Supp. 672, 676 (M.D. Pa. 1994). The court noted “[a]lthough they now complain that it was ... a massive production, the court set no immediate deadline for completion of that particular production and the Keystone Defendants did not request additional time to review the documents before they began production so that they could devise a statement of privilege.” Id. The court concluded that defendant had waived its claim of privilege as to e-mail messages advising the extraction of as many resources out of the defendant corporation as possible. Id. at 675–76.

219. See Wiginton v. CB Richard Ellis, Inc., No. 02 C 6832, 2004 WL 1895122, at *2 (N.D. Ill. Aug. 10, 2004) (“The parties have manipulated the numbers and categorized the 8,660 documents in various ways that supports their respective positions.”); Medtronic Sofamor Danek, Inc. v. Michelson, 56 Fed. R. Serv. 3d (West) 1159, 1161 (W.D. Tenn. 2003) (indicating that the requesting party estimated that the information sought contained about 20,000 gigabytes, while the producing party claimed that the production would approximate 61 terabytes).
For example, a keyword search may count as hits all of the documents attached to an e-mail message, even if the message alone contains the targeted term.220 A party arguing that a waiver had taken place should seek to account for these false hits and argue that the scope was smaller than the keyword search would indicate. On the other hand, a party arguing that a disclosure did not effect a waiver should include all hits in its assessment of the scope of discovery considering that all such hits probably have to be verified anyway.

Even where discovery is vast, courts have shown intolerance toward arguments that no waiver has occurred where the same document has been disclosed inadvertently on more than one occasion.221 Furthermore, even in the presence of a court sanctioned "claw back" agreement, a court may find that a litigant has waived any privilege by inadvertently producing a document more than once.222

220. See Wiginton, 2004 WL 1895122, at *1 (describing the phenomenon known as family cascading).

221. See, e.g., Entry Regarding Inadvertently Disclosed Document, In re Bridgestone/Firestone, Inc., Tires Prod. Liab. Litig., Master File No. IP No. 00-9373-C-B/S (S.D. Ind., entered Oct. 10, 2001) (MDL No. 1373), at http://www.insd.uscourts.gov/Firestone/bf_docs/93731739.pdf. In a multi-district products liability case, defendants produced an immense amount of data from electronic databases. Id. at *2. The court was willing to agree defendant had not waived any privilege by inadvertently posting a document on a Web site established specifically for discovery purposes. Id. at *3. However, the court held that the privilege had been waived when the privileged document was produced a second time in a hard copy version. Id. at *4. "To produce the document once was inadvertence; to produce it again while at the same time vigorously asserting in court the importance of keeping it confidential, was something else entirely." Id.; Ciba-Geigy Corp. v. Sandoz Ltd., 916 F. Supp. 404, 414 (D.N.J. 1996) (finding clear waiver where defendant produced 681 documents from its litigation database including six copies of a privileged document).

222. See Entry Regarding Inadvertently Disclosed Document at 3–4, In re Bridgestone/Firestone, Inc., Tires Prod. Liab. Litig., Master File No. IP No. 00-9373-C-B/S (S.D. Ind., entered Oct. 10, 2001) (MDL No. 1373), at http://www.insd.uscourts.gov/Firestone/bf_docs/93731739.pdf. Defendant’s argued that the "claw back" provision in the case management order protected against waiver even in the event of a second inadvertent production. Id. The court rejected this contention stating that these "unusual circumstances—which certainly were not contemplated by the court when it approved the" case management order—warranted the determination that Ford’s second disclosure "was inexcusable and constituted a waiver of any privilege that may have
3. The Extent of Disclosure

The extent of disclosure is a factor that could arguably be impacted in the context of electronic discovery. For example, considering that e-mail allows for quick and broad dissemination of information through its copy and forwarding functions, the extent of disclosure of an e-mail message could be significant. In this sense, extent of disclosure may weigh in favor of a finding of waiver more often in the context of electronic discovery than in that of paper discovery.

A court would probably find, however, that if a privileged e-mail message were copied to anyone other than a client's attorney, the communication was not privileged in the first place because it would "lack[] the required attribute of a confidential communication to the corporate attorney." Furthermore, if a client sends a privileged e-mail message to his attorney and later forwards it to a non-privileged person, the disclosure would represent an intentional waiver of privilege rather than an inadvertent disclosure.

E. Electronic Discovery and the Electronic Communications Privacy Act

1. Title I of the ECPA: The Wire Tap Act

The Electronic Communications Privacy Act (ECPA) is aimed at increasing the expectation of privacy in electronic communications. Title I of the ECPA (Wire Tap Act) prohibits

originally attached to the document." Id. at *4.

223. See United States v. Segal, No. 02-CR-112, 2004 WL 830428, at *3 (N.D. Ill. Apr. 16, 2004) ("[E]-mail... permits the broad dissemination... [of] communications.").


225. See Women's InterArt Ctr., Inc. v. N.Y.C. Econ. Dev., 223 F.R.D. 156, 161 (S.D.N.Y. 2004) ("Generally, [an e-mail attachment] to be sent to a third party 'removes the cloak of confidentiality necessary for protection under the attorney-client privilege.'").


any person\textsuperscript{228} from intercepting\textsuperscript{229} or attempting to intercept any electronic communication.\textsuperscript{230} In addition to criminalizing interception of electronic communications, the Wire Tap Act also creates a civil cause of action which permits persons to sue for damages anyone who intercepts their electronic communications.\textsuperscript{231}

Because all circuits applying the statute have construed the term "intercept" narrowly,\textsuperscript{232} the Wire Tap Act has limited applicability to electronic discovery in the civil context. "Interception" of an electronic communication within the meaning of the Wire Tap Act can only occur contemporaneously with the transmission of electronic data.\textsuperscript{233} Thus, in order to "intercept" an e-mail message, a

\begin{itemize}
  \item 228. Title 18 U.S.C. § 2510(6) defines "person" as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." \textit{Id.} § 2510(6) (2000).
  \item 229. Title 18 U.S.C. § 2510(4) defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." \textit{Id.} § 2510(4) (2000).
  \item 230. Title 18 U.S.C. § 2510(12) defines "electronic communication" as: any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted ... by a wire, radio, electromagnetic, photoelectronic or photooptical system ..., but does not include—(A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device ... or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds. \textit{Id.} § 2510(12) (2000).
  \item 233. \textit{See} Fraser, 352 F.3d at 113 ("Congress amended the Wiretap Act in 1986 ... to extend protection to electronic communications, [however] it 'did not intend to change the definition of 'intercept.'") (quoting Steve Jackson Games, Inc., 36 F.3d at 462). Under the old Wire Tap Act, "intercept" had been judicially defined as "contemporaneous in the context of an aural communication." \textit{See id.; see also} Steiger, 318 F.3d at 1048–49 (endorsing the Fifth and Ninth Circuit view that "contemporaneous interception—i.e., an acquisition during 'flight'—is required to implicate the Wiretap Act with respect to electronic communications"); Konop, 302 F.3d at 878 (holding that
person would have to access the electronic communication while in transit through the Internet during the instant between the moment of transmission and that of receipt for storage. For technical reasons, it would be virtually impossible for any civil litigant to seek electronic discovery in this manner. Furthermore, resort to such tactics would trigger criminal as well as civil liability. At the very least, however, a civil litigant engaged in production of electronic data via the Internet can be reassured that no third party could intercept the data without violating the Wire Tap Act.

2. Title II of the ECPA: The Stored Communications Act

Title II of the ECPA (Stored Communications Act) imposes criminal and civil liability on any person who “(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; [and obtains access to an] electronic communication while it is in electronic storage in such system.” Title 18 U.S.C. Section 2510(17) defines electronic

“for a website . . . to be ‘intercepted’ in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage”); Wesley Coll., 974 F. Supp. at 385–86 (“[E]ach court . . . has concluded that there can be no interception under Title I if the acquisition of the contents of electronic communications is not contemporaneous with their transmissions.”).

234. See Fraser, 352 F.3d at 114. The term electronic communication does not include electronic storage. Id. Therefore, “there can be no ‘intercept’ of an e-mail in storage, as an e-mail in storage is by definition not an ‘electronic communication.’” Id.; see also Konop, 302 F.3d at 878 (indicating that an electronic communication cannot be intercepted if it is in storage).

235. See Ian C. Ballon, IP and Internet Litigation: Law and Developing Trends, in EIGHTH ANNUAL INTERNET LAW INSTITUTE: HOW CORPORATE AMERICA IS HARNESSING THE INTERNET, 475–76 (2004) (“It is virtually impossible to intercept an email while in transit over the Internet . . . .[I]nformation is transmitted over the Internet in packets. A single message may be broken into several different packets, which may be sent over different routes before being reassembled at their destination point. A single packet would be almost impossible to target and virtually unintelligible.”).


237. See id. §§ 2701–2712.

238. See id. § 2701 (providing for criminal liability); id. § 2707 (providing for injunctive relief, damages and punitive damages).

239. Id. § 2701(a)(1)–(2) (2000). 18 U.S.C. § 2701(c)(1)–(2) exempts from liability under the Stored Communications Act people or entities “providing a wire or electronic communications service” and “user[s] of [the] service with respect to a communication of or intended for that user.” Id. § 2701(c)(1)–(2).
storage as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any... storage by an electronic communication service for purposes of backup protection of such communication." Although the statute defines "electronic storage" to some extent, there is a split in authority on the precise meaning of this term. The degree to which the Stored Communications Act is implicated by electronic discovery in the civil context may depend on the interpretation of "electronic storage."

a. Interpretations of "electronic storage"

Several courts have concluded that the term "electronic storage" refers only to those electronic communications that are held on the Internet Service Provider's (ISP) server that have not been accessed or opened by the intended recipient. This narrow definition of

240. Id. § 2510(17).
241. See Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) (noting that any disagreements over the construction of the Stored Communications Act may be attributable to the fact that the "intersection of [Title I and Title II] is a complex, and often convoluted, area of the law.... [U]ntil Congress brings the laws in line with modern technology, protection of the Internet and websites... will remain a confusing and uncertain area of the law."); Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 633 (E.D. Pa. 2001), rev'd in part on other grounds, 352 F.3d 107 (3d Cir. 2003) ("The ECPA has been noted for its lack of clarity."); Doe v. Ashcroft, 334 F. Supp. 2d 471, 488 n.72 (S.D.N.Y. 2004) ("Courts are not uniform in interpreting the statute's confusing and overlapping definitions.").

It appears that the section is specifically targeted at communications temporarily stored by electronic communications services incident to their transmission—for example, when an email service stores a message until the addressee downloads it.... Title II only protects electronic communications stored "for a limited time" in the "middle" of a transmission, i.e. when an electronic communication service temporarily stores a communication while waiting to deliver it.

Id.; see also Fraser, 135 F. Supp. 2d at 633–34, 636 (interpreting electronic storage to mean the period of intermediate storage prior to recipients access to the communication whereupon transmission is complete); In re CI Host, Inc., 92 S.W.3d 514, 515 (Tex. 2002) (applying federal law and declining to address plaintiff's claim that e-mail messages are only in electronic storage when they are in "temporary, intermediate storage, before they are received [or opened] by the intended recipient").
electronic storage limits the applicability of the Stored Communications Act in the context of electronic discovery. For example, a discovery request which seeks production of e-mail messages could only plausibly trigger the ECPA if the messages it seeks have not been opened by the intended recipient. Furthermore, a litigant that accesses electronic communications in storage pursuant to the authorization of the opposing party as part of the discovery plan would be exempted from liability under the ECPA.

The Ninth Circuit envisions a broader application of the Stored Communications Act by relying on subsection (B) of the statutory definition of electronic storage, which includes e-mail messages stored for the purpose of backup protection. In Theofel, plaintiffs sued defendants for violation of their privacy rights under the ECPA. Pursuant to a subpoena issued for purposes of discovery in a different civil case against the defendants, corporate officers of Integrated Capital Associates, Inc. (ICA), obtained e-mail messages from ICA’s ISP, NetGate. A number of the messages obtained by the defendant were taken from the plaintiff’s e-mail accounts and were not related to the subject matter of the litigation. The Ninth Circuit adopted the magistrate judge’s finding that the “subpoena was ‘transparently and egregiously’ overbroad and that defendants

---

243. Even un-opened e-mail which remains on an Internet service provider’s server is only in “electronic storage” within the meaning of the Stored Communications Act for 180 days, beyond which point in time, electronic storage of such communication ceases to be temporary or intermediate. Doe v. Ashcroft, 334 F. Supp. 2d 471, 487-88 (S.D.N.Y. 2004).
244. See 18 U.S.C. § 2701(c)(2) (2000) (expressly exempting conduct authorized by a user of an Internet service “with respect to a communication of or intended for that user”).
245. See Theofel v. Farey-Jones, 359 F.3d 1066, 1072-73 (9th Cir. 2004).
246. Id. at 1072.
247. Id. at 1071.
248. Id.

One might have thought... that the subpoena would request only e-mail related to the subject matter of the litigation, or maybe messages sent during some relevant time period... [b]ut [the subpoena] ordered “production of all copies of e-mails sent or received by anyone at ICA, with no limitation as to time or scope.... Most [of the e-mail messages]... were privileged or personal.”
acted with gross negligence and in bad faith." 249

The Ninth Circuit rejected the defendants’ contention that the opened or "delivered" e-mail messages did not fall within the purview of the Stored Communications Act. 250 The court held that even if the messages were not in temporary or intermediate storage for the purpose of subsection (A), they were still protected under subsection (B) of the Stored Communications Act as communications being stored for backup purposes. 251 The court explained:

An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again—if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a "backup" for the user. Notably, nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user. Storage under these circumstances thus literally falls within the statutory definition. 252

The court criticized interpretations of the Stored Communications Act that interpreted "backup protection" to include "only temporary backup storage pending delivery." 253 According to the Ninth Circuit this construction of the Act was contrary to the plain language of the act because subsection (B), in contrast to subsection (A), does not distinguish between intermediate and post-transmission storage. 254 By drawing this distinction the court held that while subsection (A) protects only unopened e-mail, subsection (B) protects opened e-mail

249. See id. at 1079.
250. See id. at 1075 (declining to adhere to Fraser's holding that "backup protection" includes only temporary backup storage of transmitted messages that have not been opened and not transmitted messages that have been opened and remain in storage).
251. See id.
252. Id.
253. See id. at 1075. Both the court in Fraser as well as the United States, as amicus curiae, adhered to this interpretation of the Stored Communication Act on the basis that the language in subsection (B) ("any storage of [wire or electronic] communications") applies only to backup copies of messages that are themselves in temporary, intermediate storage under subsection (A). See id. at 1075–76.
254. Id. at 1076.
messages retained on the ISP's server as backup copies. The court noted that construing subsection (B) to include only those communications that are protected by subsection (A) essentially deprives subsection (B) of any independent significance, thus rendering it superfluous.

Before applying its divergent interpretation of the Stored Communications Act, the court resolved the question of whether NetGate "authorized" the access to the e-mail messages such that the defendants' conduct was immunized under Section 2701(c). Considering that the subpoena was overbroad and, therefore, invalid, NetGate's consensual provision of e-mail in compliance with the subpoena was vitiates

The court reversed the district court's dismissal of the plaintiffs claim under the Stored Communications Act and remanded for final resolution.

b. Implications for electronic discovery obtained from ISPs

Theofel provides an example of an overzealous litigant who abused an invalid subpoena to obtain discovery of electronic communications unrelated to the subject matter of litigation. At least in the Ninth Circuit, such conduct constitutes grounds for both criminal and civil liability under the Stored Communications Act. Because the United States Supreme Court has not had occasion to resolve the disagreement among the courts over the meaning of "electronic storage," litigants retrieving e-mail messages from ISPs as a part of electronic discovery should exercise extreme caution to stay within the scope of relevancy regardless of any subpoena's purported authorization of a broader discovery mandate.

c. Implications for Web-based discovery

Another use of electronic technology that facilitates discovery and that may increase the applicability of the Stored Communications Act to electronic discovery is the creation and

255. See id. at 1075, 1077.
256. See id. at 1075–76.
257. See id. at 1073–75.
258. See id.
259. Id. at 1079.
260. See supra notes 245–59 and accompanying text.
261. See Theofel, 359 F.3d at 1079.
maintenance of discovery Web sites in complex litigation. At least one court has held that Web sites are electronically stored communications within the meaning of the Stored Communications Act. The practical effect of this holding is that the Stored Communications Act may impose criminal and civil liability on a person who gains unauthorized access to a user-restricted Web site.

The notion that Web sites are protected under the Stored Communications Act may have implications for litigants engaged in Web-based discovery for complex litigation cases. Assuming discovery Web sites are secure and accessible only by designated users that are parties to the litigation, it is conceivable a designated user could permit access to an unauthorized user. Under such circumstances, a litigant participating in Web based discovery may state a claim against the person who accessed the stored electronic communications posted on the Web site. Thus, the Stored Communications Act places on guard strangers to complex litigation cases that may have an interest in accessing the information made available on a discovery Web site. Certain forms of unauthorized access to a discovery Web site could trigger criminal and civil liability under the stored communications act.


263. See Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002). In Konop, plaintiff established a Web site where he posted information critical of defendant employer, its officers and the union. Id. at 872. Plaintiff restricted access by designating eligible users and requiring them to log on with a username and password. Id. at 872–73. Vice President for defendant asked permission from a designated user to use his name to create a password and access the Web site. Id. at 873. By finding there was a triable issue of fact as to whether defendant violated the Stored Communications Act, the court essentially held that the Web site was a stored communication within the meaning of the Stored Communications Act. Id. at 880.

264. See id.

265. See supra notes 262–64 and accompanying text.

266. See Konop, 302 F.3d at 873.

267. See id. at 880.

268. See id. at 880. The Konop court refrained from labeling the employees authorized to access the Web site as “users” as defined under the ECPA. Id. Although the employee was eligible to view the Web site, there was no
F. Conclusion

In responding to an electronic discovery request, litigants must give careful thought to the issue of privilege. A proactive approach to resolving technical difficulties involved in electronic discovery is the most important step in protecting privilege claims. Cooperation with opposing counsel and communication with the court will enable litigants to develop discovery plans that minimize the threats that electronic discovery poses to evidentiary privileges. Although the electronic medium does not distract courts from evaluating the substantial merit of a privilege claim, courts are generally sympathetic to the unique burden that electronic discovery places on litigants. Nonetheless, in the case of litigants and attorneys who abuse the electronic discovery process, the courts may look to the Stored Communications Act as a source of liability.