N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

Ethical Considerations for Attorneys Responding to a Data-Security Breach

Robert J. Scott & Julie Machal-Fulks

Spring 2008 VOL. 6, NO. 2

Northwestern Journal of Technology and Intellectual Property
Volume 6, Number 2 (Spring 2008)

Ethical Considerations for Attorneys Responding to a Data-Security Breach

Robert J. Scott[*] & Julie Machal-Fulks[**]

I. INTRODUCTION

¶1 It seems that not a week goes by without news reports about yet another company or agency suffering a data-security breach: a laptop is lost, a firewall is penetrated, or sensitive personal information purportedly kept secure is exposed. The legal implications of such a breach are significant and, given the novelty of both data breaches and the laws meant to address them, the ethical implications for an attorney representing a client that has suffered such a breach are magnified.

¶2 This article will explore ethical considerations for attorneys responding to a data-security breach and the appropriate role for attorneys in a company's efforts to deal with such a breach. These main topics will be addressed: (1) the attorney's role in investigating a breach, including the applicability and scope of the attorney-client privilege; (2) the applicability and scope of the work-product rule in connection with the attorney's investigation and the company's response; (3) the attorney's role and ethical obligations with respect to preservation of electronic and documentary evidence as part of a breach response; (4) the standards under which an attorney should advise a client regarding state and federal data-security breach statutes; and (5) the attorney's ethical obligations during litigation over a data-security breach.

II. THE LEGAL LANDSCAPE FOR DATA-SECURITY BREACHES

¶3 There has been a proliferation of data-security breach incidents in the last few years, and many businesses have been required by state statutes or federal regulatory schemes to notify individuals whose data have been lost or stolen. Different types of data may be exposed during a data-security breach. For example, the data at issue could include a combination of any of the following: social security numbers, first and last names, phone numbers, addresses, banking and investment account numbers, credit account numbers, birth dates, medical information, and personal identification numbers (PINs).

¶4 In addition to being an embarrassment for a company, a data-security breach has many potential legal implications under both federal and state laws. For instance, the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) establishes both criminal penalties for violations of HIPAA's statutory prohibitions and civil penalties for violations of its implementing regulations, including its Privacy Rule and its

[*] Scott & Scott, LLP.
[**] Scott & Scott, LLP. The authors thank Jonathan C. Scott, Lawrence R. Lassiter, and Kathleen Kilanowski of Scott & Scott, LLP for their valuable assistance in the preparation of this article.

Security Standards for the Protection of Electronic Protected Health Information (Security Rule).[1] The Gramm-Leach-Bliley Act of 1999 (GLBA)[2] also may be implicated by a data-security breach, as well as the Federal Trade Commission's unfair trade practices rules.[3] Many states also have enacted statutes that require businesses suffering a data-security breach to notify affected individuals about the breach under certain circumstances.[4]

¶5 Beyond the statutory and regulatory implications, businesses suffering a data-security breach also may face civil litigation. Because this is a new and evolving area of law, a company may find itself facing various private causes of action, commonly including negligence, breach of contract, infliction of emotional distress, and state unlawful trade practices and consumer protection claims. In addition, there has been a recent trend of plaintiffs seeking relief in the form of compensation for future credit monitoring, though the viability of such a claim remains unclear.[5]

III. THE ATTORNEY-CLIENT PRIVILEGE AND INVESTIGATING A DATA-SECURITY BREACH

¶6 Companies that experience a data-security breach often will find it useful to employ outside counsel and outside information technology (IT) specialists to investigate the breach. If such an investigation is conducted by internal resources, the results of that investigation might not be protected by the attorney-client privilege or the attorney work-product privilege.

¶7 The attorney-client privilege protects communications between an attorney and a client.[6] The Supreme Court of the United States has held that the purpose of the attorney-client privilege is to encourage full communication between attorneys and their clients in order to "promote broader public interests in the observance of the law and administration of justice."[7] To be protected by the attorney-client privilege, a communication must be confidential and made for the purpose of obtaining legal advice from the attorney.[8] A communication is confidential only if it is not intended to be disclosed to third persons; such a disclosure may result in waiver of the privilege.[9] In addition, the attorney-client privilege is held by the client, not by the lawyer.[10]

---

[1] Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 42 U.S.C.).

[2] Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended in scattered sections of 15 U.S.C.). The GLBA protects nonpublic personal information by requiring that financial records be properly secured, safeguarded, and eventually disposed of in a manner that completely destroys the information so that it cannot be further accessed.

[3] *See In re* BJ's Wholesale Club, Inc., 140 F.T.C. 465 (2005).

[4] At least 39 states have enacted these notification statutes. *See, e.g.*, ARIZ. REV. STAT. § 44-7501 (2007); NY GEN. BUS. LAW § 899-aa (2007); WASH. REV. CODE ANN. § 19.255.010 (2007).

[5] For instance, in *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629 (7th Cir. 2007), the Seventh Circuit held that Indiana law did not recognize such a claim.

[6] *In re* Grand Jury Subpoena 92-1 (SJ), 31 F.3d 826, 829 (9th Cir. 1994).

[7] Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

[8] *See* XYZ Corp. v. United States, 348 F.3d 16, 22 (1st Cir. 2003); *In re* Bieter Co., 16 F.3d 929, 936 (8th Cir. 1994); Clover Staffing, LLC v. Johnson Controls World Servs., Inc., 238 F.R.D. 576, 578 (S.D. Tex. 2006).

[9] Permian Corp. v. United States, 665 F.2d 1214, 1219 (D.C. Cir. 1981).

[10] *See In re* Seagate Technology, LLC, 497 F.3d 1360, 1372 (Fed. Cir. 2007).

¶8 Communications between in-house counsel and corporate IT professionals may themselves be privileged when they meet the subject matter test established by the Court in *Upjohn Co. v. United States*.[11] Under *Upjohn*, the privilege protects communications by a corporate employee, regardless of position, when (1) the communications concern matters within the scope of the employee's corporate duties, and (2) the employee is aware that the information is being furnished to enable an attorney to provide legal advice to the corporation.[12] With respect to internal investigations, courts generally have held that "an attorney's investigation [to obtain facts] may constitute a legal service, encompassed by the privilege."[13]

¶9 However, courts often apply the protection of the attorney-client privilege more narrowly and cautiously to corporate in-house counsel.[14] The New York Court of Appeals has stated that less protection often is warranted, particularly when company officers have a mixed responsibility incorporating both business and legal aspects, and where their advice and communications are based on an ongoing, permanent business relationship rather than specific requests for legal advice.[15]

¶10 Given the often narrow approach taken by courts when addressing whether the privilege applies to communications involving in-house counsel, there are significant disclosure risks associated with relying solely on in-house counsel to direct an investigation. A common misconception (and frustration) in the corporate world is the belief that merely involving in-house counsel protects the information and investigation from disclosure in discovery litigation. As indicated above, this is not always the case. In-house attorneys often have both business and legal roles, and advice rendered in that business capacity is not protected by the attorney-client privilege. Involving in-house counsel alone does not mean the information and investigation is necessarily protected from disclosure in discovery.

¶11 The fact that many in-house counsel perform dual roles—as both corporate officers and attorneys—means that confusion often arises when courts are forced to determine whether in-house counsel were acting in their business capacity or in their legal capacity. This determination often is most difficult when in-house counsel assist with fact-gathering and regulatory compliance projects; courts in these situations typically must resort to evidence other than the face of documents or facts surrounding communications. For example, correspondence may contain both business and legal advice. It is well settled, however, that merely sending documents, correspondence, and e-mails to in-house counsel is not enough to establish privilege.[16] In addition, there is no presumption

---

[11] *Upjohn Co.*, 449 U.S. at 394.

[12] *Id.* at 389-90.

[13] *In re* Allen, 106 F.3d 582, 601 (4th Cir. 1997); *see also* United States v. Rowe, 96 F.3d 1294, 1297 (9th Cir. 1996) ("*Upjohn*. . . . make[s it] clear that fact-finding which pertains to legal advice counts as 'professional legal services.'").

[14] *See* Rossi v. Blue Cross and Blue Shield, 540 N.E.2d 703, 705 (N.Y. 1989).

[15] *Id.*

[16] *In re* Avantel, S.A., 343 F.3d 311, 321 n.11 (5th Cir. 2003) ("[E]-mails sent to or from attorneys acting in a non-legal capacity, e.g., as CEO, CFO, etc., and that are not addressed to or sent by Defendant's in-house or outside legal counsel should not be privileged . . . . To rule otherwise would allow parties to evade the privilege limitations by sending copies of every company-generated e-mail to the company's attorney so as to protect the communication from discovery, regardless of whether legal services were sought or who the other recipients of the e-mail were.").

that communications are privileged, and the party asserting the attorney-client privilege has the burden of establishing all of the required elements.[17]

¶12 In the context of a data-breach investigation, these issues can become especially difficult given the complex technical issues involved. The distinction between legal advice and technical, business-related advice will be more obvious to the court when the advice comes from outside counsel.

IV. THE WORK-PRODUCT RULE AND INVESTIGATING A DATA-SECURITY BREACH

¶13 In addition to the attorney-client privilege, the work-product rule also may protect an investigation into a data-security breach. In particular, when a business hires an outside firm to investigate a breach incident and to advise the business regarding risk mitigation that advice and investigation should qualify for protection under the work-product rule. The rule is "designed to balance the needs of the adversary system: promotion of an attorney's preparation in representing a client versus society's general interest in revealing all true and material facts to the resolution of a dispute."[18] In federal courts, Federal Rule of Civil Procedure 26(b)(3) protects attorney work product from discovery.[19] The work-product rule was created to protect trial preparation materials that might reveal an attorney's evaluations and strategies about a case.[20]

¶14 The two types of materials covered by the rule are opinion work product and ordinary work product. Opinion work product consists of mental impressions, opinions, conclusions, or legal theories of an attorney or other representative of a party.[21] This encompasses an attorney's notes (including purely factual notes), documents reflecting strategy discussions and evaluation of cases, compilations of documents that would disclose an attorney's mental impressions and thought processes, and the organization of the attorney's file.[22] In contrast, ordinary work product, including raw factual information, consists of preparation materials that do not disclose opinions or impressions.[23]

¶15 Under the Federal Rules, the two types of work product receive different levels of protection. Opinion work product is generally entitled to greater protection than ordinary work product and typically is not subject to discovery.[24] Ordinary work product can be discoverable, but usually only if the party seeking discovery can show a substantial need for the materials and an inability to obtain the substantial equivalent of the materials by some other means.[25]

---

[17] United States v. Munoz, 233 F.3d 1117, 1128 (9th Cir. 2000).
[18] Martin Marietta Corp. v. Pollard, 856 F.2d 619, 624 (4th Cir.1988).
[19] *See, e.g.*, United Coal Cos. v. Powell Constr. Co., 839 F.2d 958, 966 (3d Cir. 1988).
[20] Hickman v. Taylor, 329 U.S. 495, 510-11 (1947).
[21] FED. R. CIV. P. 26(b)(3).
[22] *See* Director, Office of Thrift Supervision v. Vinson & Elkins, 124 F.3d 1304, 1308 (D.C. Cir. 1997); *In re* San Juan Dupont Plaza Hotel Fire Litig., 859 F.2d 1007, 1015 (1st Cir. 1988); Shelton v. Am. Motors Corp., 805 F.2d 1323, 1328-29 (8th Cir. 1986).
[23] *In re* Green Grand Jury Proceedings, 492 F.3d 976, 981 (8th Cir. 2007).
[24] *In re* Cendant Corp. Sec. Litig., 343 F.3d 658, 663 (3d Cir. 2003).
[25] FED. R. CIV. P. 26(b)(3).

¶16 The scope of the work-product rule extends to materials prepared by, for, or in consultation with an attorney.[26] However, as with the attorney-client privilege, the dual roles of many in-house counsels—as both corporate officers and attorneys—may leave the reports of internal investigations open to disclosure in discovery. The applicability of the work-product rule also generally turns on whether the work was performed "in anticipation of litigation."[27] Under federal law, "in anticipation of litigation means only that the primary motivating purpose behind the creation of the document was to aid in possible future litigation."[28] The prevalence of lawsuits in connection with data-security breaches lends credence to a claim that any information gathered or acquired by an attorney in connection with a data breach was gathered or acquired in anticipation of litigation. The hiring of an outside counsel makes a clear statement that the company sought legal advice in anticipation of potential litigation. In contrast, a corporation turning to the advice of in-house counsel may find it more difficult to establish that the consultation was in anticipation of litigation. It should be noted, however, that "the collection of evidence, without any creative or analytic input by an attorney or his agent, does not qualify [for] work-product [protections]."[29]

¶17 While the work-product rule does not shield underlying facts or event information from discovery, the compilations and collections performed by an attorney or an attorney's team would probably be protected from disclosure in discovery. But ordinary business documents — those that would have been prepared by a company or third party regardless of whether an attorney was sent a copy — are not protected by the doctrine. Specifically, "documents created for a business purpose are not protected even though the 'information developed may be helpful [to the company] in legal proceedings.'"[30] Like the attorney-client privilege, the protections of the work-product rule can be waived by disclosing the materials to third parties.[31] In addition, the protections afforded by the rule may be waived if the work-product privilege is not asserted promptly.[32]

¶18

V. RESPONDING TO A DATA-SECURITY BREACH — THE ATTORNEY'S ETHICAL OBLIGATIONS AND ROLE

¶19 When a data-security breach occurs, evidence should be preserved and collected diligently. It is critical to document what the client was doing at the time of the breach incident in order to comply with ethical and discovery obligations. Attorneys have an ethical obligation to ensure that their clients avoid possible court sanctions for spoliation

[26] *Id. See also In re* Cendant Corp. Sec. Litig., 343 F.3d 658 at 667-68.

[27] FED. R. CIV. P. 26(b)(3)(A).

[28] Clover Staffing, LLC v. Johnson Controls World Serv., Inc., 238 F.R.D. 576, 579 (S.D. Tex. 2006) (quoting Smith v. Texaco, Inc., 186 F.R.D. 354, 357 (E.D. Tex. 1999)).

[29] Riddell Sports Inc. v. Brooks, 158 F.R.D. 555, 559 (S.D.N.Y. 1994).

[30] *Clover Staffing*, 238 F.R.D. at 579 (citing Navigant Consulting, Inc. v. Wilkinson, 220 F.R.D. 467, 473 (N.D. Tex. 2004)).

[31] *See* Norton v. Caremark, Inc., 20 F.3d 330, 339 (8th Cir. 1994) (finding no abuse of discretion by trial court admitting into evidence previously protected documents, which defendant counsel disclosed to plaintiff during pre-trial discovery).

[32] Marx v. Kelly, Hart & Hallman, P.C., 929 F.2d 8, 12 (1st Cir. 1991).

of evidence. Also, litigants have an obligation to preserve relevant evidence for use by the adverse party.

¶20 Spoliation poses a significant danger in responding to a data breach. A finding of spoliation can result in substantial court sanctions, including a jury instruction that jurors should infer that the destroyed evidence was unfavorable to the offending party. Generally, an adverse inference instruction is given when evidence has been destroyed and:

> (1) . . . the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) . . . the records were destroyed "with a culpable state of mind;" and (3) . . . the destroyed evidence was "relevant" to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense.[33]

¶21 The rationale for the adverse inference rule is predicated on the "common sense observation that a party who has notice that [evidence] is relevant to litigation and who proceeds to destroy [the evidence] is more likely to have been threatened by [that evidence] than is a party in the same position who does not destroy the document."[34] Such an instruction can be extremely damaging to a litigant's case, and may be far worse than the inference that the jury would have drawn if the evidence had been produced.

¶22 Courts also have the authority to grant an adverse inference instruction even where a party did not intentionally destroy the evidence. In cases where a party merely neglected to preserve evidence relevant to the case, the jury still could be instructed that it may infer that the unproduced evidence was damaging to that party's case and supportive of the adverse party's claims.[35] It is also important to recognize that spoliation sanctions can apply to destruction of electronic information, regardless of whether the destruction was intentional.[36] When responding to a data breach, attorneys therefore may want to have a computer forensics expert on their investigative team to make certain that all the electronic information is properly preserved.

¶23 It is important to document all the client's actions taken in connection with, and in response to, an incident. As mentioned above, these documents prepared in anticipation of litigation should be protected by the work-product privilege.[37] It is also important to identify appropriate law enforcement contacts to notify regarding security incidents that may involve illegal activities. An attorney should be involved in making this assessment.

---

[33] Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 107 (2d Cir. 2002) (citing Byrnie v. Town of Cromwell, 243 F.3d 93, 107-12 (2d Cir. 2001)).

[34] Nation-Wide Check Corp. v. Forest Hills Distrib., Inc., 692 F.2d 214, 218 (1st Cir. 1982).

[35] *See* Schmid v. Milwaukee Elec. Tool Corp., 13 F.3d 76, 78 (3d Cir. 1994) (finding error by the trial court in completely barring expert's testimony where spoliation inference may have been the more appropriate sanction).

[36] *See* Allstate Ins. Co. v. Sunbeam Corp., 53 F.3d 804, 806-07 (7th Cir. 1995); Marrocco v. General Motors Corp., 966 F.2d 220, 224-25 (7th Cir. 1992); *In re* Graham, 363 B.R. 32, 36 (Bankr. D.N.H. 2007).

[37] *See* Work Product discussion, *supra* page 174.

VI. STATUTORY NOTIFICATION — ADVISING CLIENTS REGARDING NEW STATUTES, RULES, AND REGULATORY COMPLIANCE

¶24 While data-security breach issues are of concern to every individual interacting with modern technology, it is only within the past few years that many states have enacted statutory schemes that address data-security breach and identity theft.[38] As a result, there is very little state or federal case law interpreting the scope or application of these statutes.[39] In an effort to ensure compliance with the new laws and regulations, an attorney should be involved in assessing whether a company is required to give notice in each state where it does business or where a potential loss of data may have occurred.

¶25 It is also important to determine, upon advice of counsel, how notice must be given, when notice should be given, the form notice should take, and the specific contents of any notice. States vary in their definition of what constitutes "personal information."[40] Therefore, it is critical to ascertain what a state's statute defines as personal information in order to determine if the breach is one giving rise to the notice requirement, and if so, the statutory requirement for how notice should be given.

¶26 When giving advice about statutes that have yet to be authoritatively interpreted, attorneys should be particularly careful. While an attorney generally is not liable for malpractice "for a mistake in a point of law which has not been settled by the court of last resort in his State and on which reasonable doubt may be entertained by well-informed lawyers,"[41] an attorney in such circumstances must be able to demonstrate that he or she acted in good faith "and in an honest belief that his advice and acts are well founded and in the best interest of his client."[42] To meet this standard, research should include legislative history when available, because if the language of the statute is ambiguous or confusing, a reading of the legislative materials may provide insight as to how to approach a new law or regulation.[43] Research also should be expanded to encompass decisions regarding similar statutes in other jurisdictions.[44] A client also should be

---

[38] *See supra* note 4.

[39] *See, e.g.*, Parke v. Cardsystems Solutions, Inc., No. C 06-04857, 2006 WL 2917604, at *4 (N.D. Cal. Oct. 11, 2006) ("Several of plaintiffs' claims implicate complicated issues of financial privacy on which the California courts have yet to rule. Plaintiffs brought claims under California Civil Code §§ 1798.181.5(b), 1798.81.5(c), 1798.81, and 1798.82, provisions of the financial-privacy regime enacted by the California legislature over the last six years. There appears to be no reported appellate decisions interpreting these code provisions.").

[40] For instance, in Connecticut, personal information includes a person's first name or first initial and last name, along with one of the following unencrypted pieces of information: social security number; driver's license number or state identification number; or account number, credit card number, or debit card number, combined with any password, security code, or access code. CONN. GEN. STAT. § 36a-701b(a) (2007). Several states use a similar definition. *See, e.g.*, 815 ILL. COMP. STAT. 530/5 (2007); TEX. BUS. & COM. CODE ANN. §§ 48.002, 48.103 (2007). Other states, however, have chosen to include additional information in their statutory definitions, including medical information and security codes. *See, e.g.*, CAL. CIVIL CODE, § 1798.82(e) (2007); GA. CODE ANN. § 10-1-911(6) (*year?*).

[41] Jerry's Enter., Inc. v. Larkin, Hoffman, Daly & Lindgren, Ltd., 711 N.W.2d 811, 818 (Minn. 2006) (quoting Meagher v. Kavli, 97 N.W.2d 370, 375 (Minn. 1959)).

[42] *Id*.

[43] United States v. Gregg, 226 F.3d 253, 257 (3d Cir. 2000) ("Where the statutory language does not express Congress's intent unequivocally, a court traditionally refers to the legislative history and the atmosphere in which the statute was enacted in an attempt to determine the congressional purpose."); Dir., Office of Workers' Comp. Programs v. Sun Ship, Inc., 150 F.3d 288, 291 (3d Cir. 1998) ("If the [statutory] language is ambiguous, we look to legislative history to determine congressional intent.").

[44] *See, e.g.*, Martinez v. Enter. Rent-A-Car Co., 13 Cal. Rptr. 3d 857, 862 (Cal. Ct. App. 2004) ("Where,

advised that public agencies are frequently the plaintiff in an action brought pursuant to a data-breach notification statute, and that the agency's opinion regarding statutory requirements is generally accorded deference by courts.[45] Opinion letters should contain caveats notifying the client that this is a new and unpredictable area of litigation.

VII. THE ATTORNEY'S ETHICAL OBLIGATIONS DURING LITIGATION OVER A DATA-SECURITY BREACH

¶27 Lawsuits over data-security breaches are becoming more common, and because most of the information in such cases is stored in electronic form, the cases present significant challenges for counsel. As in any other case, initial disclosures under Federal Rule of Civil Procedure 26 must be signed by an attorney, certifying that, after reasonable inquiry, the disclosure is complete and correct as of the time it is made.[46] Discovery obligations also require a signature by an attorney, certifying compliance with the rules, warranted by the law or a good faith argument for extension, not interposed for an improper purpose, and not unreasonably or unduly burdensome.[47] Attorneys are also subject to sanctions if these certifications are made in violation of the rules.[48] Attorneys have a duty to supplement disclosures and discovery responses under Federal Rule of Civil Procedure 26(e) as well.

¶28 The new e-discovery rules raise additional issues and obligations. Attorneys are advised to include IT personnel as part of the discovery team in light of the new rules because they can assist counsel in making certain that all information is collected and reviewed. Prior to the codification of guidelines regarding electronic discovery in Federal Rules of Civil Procedure 26, 34, and 37 (effective December 1, 2006), the federal courts addressed a litigant's obligations with respect to preservation and production of electronic evidence on a case-by-case basis. Now Federal Rule of Civil Procedure 37(e) establishes the so-called "safe harbor" for electronic discovery: "[a]bsent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."[49]

---

as here, there is no California case directly on point, foreign decisions involving similar statutes and similar factual situations are of great value to the California courts."); Pope v. Brock, 912 So.2d 935, 938 (Miss. 2005) ("[U]nder the 'Borrowed Statute' doctrine, we may consider a sister state's interpretation of its statutes where there is clear evidence that our Legislature consciously borrowed statutory language from that state's enactment."); Murray v. New Hampshire Div. of State Police, 913 A.2d 737, 740 (N.H. 2006) ("We also look to the decisions of other jurisdictions, since other similar acts, because they are in *pari materia*, are interpretatively helpful, especially in understanding the necessary accommodation of the competing interests involved.") (quoting Union Leader Corp. v. New Hampshire Hous. Fin. Auth., 705 A.2d 725, 730 (N.H. 1997)).

[45] Chevron U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 842-43 (1984) (agency interpretation of governing statutes is entitled to deference); *In re* Dir. of Prop. Valuation, 161 P.3d 755, 761 (Kan. 2007) (deference given to interpretation made by agency charged with enforcing statute); Racine Harley-Davidson, Inc. v. State Div. of Hearings, 717 N.W.2d 184, 189 (Wis. 2006) (The "court may accord an agency's interpretation of a statute great weight deference or due weight deference.").

[46] FED. R. CIV. P. 26(g)(1).

[47] *Id.*

[48] FED. R. CIV. P. 26(g)(3).

[49] FED. R. CIV. P. 37(e).

¶29 Care should be taken to remember that a "safe harbor" is not always safe. In reality, an attorney still has an ethical obligation to avoid a spoliation problem with electronic records. It is commonly understood that destroying relevant evidence after entry of a federal court order requiring its production to the adverse party will support severe sanctions.[50] While Rule 37(e) appears to provide a safe harbor protecting the party against sanctions for the routine destruction of electronic evidence except in exceptional circumstances, the committee notes for the rule qualify that language. The committee notes provide that:

> Rule 37(f) [sic] applies only to information lost due to the "routine operation of an electronic information system"—the ways in which such systems are generally designed, programmed, and implemented to meet the party's technical and business needs. The "routine operation" of computer systems includes the alteration and overwriting of information, often without the operator's specific direction or awareness, a feature with no direct counterpart in hard-copy documents. Such features are essential to the operation of electronic information systems.[51]

¶30 Accordingly, data loss that is not due to routine operation of a system may lead to a spoliation sanction. The committee notes also emphasize that for the safe harbor provision to apply, the loss of evidence must have been in good faith.[52]

¶31 Therefore, the rule should not be interpreted in absolute terms because the inclusion of a requirement of good faith places the issue of the reasonableness of the party's conduct squarely before the court for its determination. Further, the scope of the new safe harbor exception in practice remains to be clarified by litigation under the new rule. It would therefore be unwise to interpret this rule as broad-case immunity against sanctions for the routine destruction of electronic evidence. The committee notes also leave unanswered the question of whether the courts are to apply a subjective or an objective standard in determining if the party against whom sanctions were sought acted in good faith. For example, if an objective standard is applied, the professed good faith of the spoliator would not be controlling. Attorneys should keep in mind that even in the absence of a court order, litigants have an obligation to preserve relevant evidence for use by the adverse party.[53] Furthermore, when a party causes "the destruction or significant alteration of evidence, or . . . fail[s] to preserve property for another's use as evidence in pending or reasonably foreseeable litigation," it is guilty of spoliation.[54]

¶32 Because e-discovery compliance is an emerging topic, the courts are still sorting out which categories of data are necessary for litigation. For example, a federal court in California held that data stored in a computer's random access memory (RAM) is electronically stored information that must be turned over in litigation, despite the fact that RAM is not permanent storage and is continually being updated, changed, deleted, or

---

[50] *See* Recinos-Recinos v. Express Forestry, Inc., No. 05-1355, 2006 WL 2349459, at *8-11 (E.D. La. 2006).

[51] FED. R. CIV. P. 37(e) Committee Notes (2006).

[52] *Id.*

[53] Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. 1998).

[54] West v. Goodyear Tire & Rubber Co., 167 F.3d 776, 779 (2d Cir. 1999).

overwritten in business computers.[55] Attorneys also should make sure they are familiar with any specific document retention obligations for their client's industry, such as regulations by the Securities and Exchange Commission that require a broker-dealer to maintain records of electronic communications for a certain time period.[56] A private litigant in a federal civil action seeking such information due to its relevance in his or her case has no private right of action under industry record-keeping rules. However, there is a strong argument in federal court that a document retention policy is unreasonable as a matter of law if it allows for the destruction of potentially useful evidence that a party was required by law to independently maintain.[57]

VIII. CONCLUSION

¶33 Attorneys should be wary when dealing with this relatively new area of the law. Because the results of a data-breach investigation may be critical in subsequent litigation, attorneys must be careful to make certain that those results are protected from discovery. Until courts have definitively interpreted the state and federal laws and regulations applicable to data-security breaches, attorneys should be especially prudent when advising clients regarding the proper course of action. Counsel should assemble a team that includes IT professionals to make certain that all relevant information is collected, analyzed, and preserved. Attorneys also should not rely exclusively on the new "safe harbor" discovery provision when responding to e-discovery requests.

[55] Columbia Pictures Indus. v. Bunnell, 2007 WL 2080419, at *1 (C.D. Cal. 2007).

[56] 17 C.F.R. § 210.2-06 (2008).

[57] *Cf.* United States. v. Kitsap Physicians Serv., 314 F.3d 995, 1001 (9th Cir. 2002) (spoliation argument rejected where defendant destroyed documents in compliance with state regulations).