Ethical Considerations for Attorneys in Responding to a Data-Security Breach

By Robert J. Scott & Julie Machal-Fulks
Attorneys are increasingly confronting the significant ethical issues raised when a data-security breach occurs. Many traps exist for the unwary in this newly evolving area of the law, where the applicable statutes have yet to be interpreted by the courts and e-discovery concerns abound. This article provides a legal framework in this area of the law and explores ethical considerations arising when an attorney represents a client that has suffered a data-security breach.

Introduction

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, and sensitive personal information purportedly kept secure is exposed. The legal implications of such a breach are significant, and given the novelty of data breaches and the laws meant to address them, the ethical implications for an attorney representing a client that has suffered a data breach are magnified.

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

The Legal Landscape for Data-Security Breaches

There has been a proliferation of data-security-breach incidents in the last few years, and many businesses have been required by state statute or federal regulatory schemes to notify individuals whose data has been lost or stolen. Different types of data may be exposed during a security breach. For example, the lost data 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/or PIN numbers.

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 Security Standards for the Protection of Electronic Protected Health Information (the “Security Rule”). The Gramm-Leach-Bliley Act (“GLBA”) may also be implicated by a data breach, as well as the Federal Trade Commission’s unfair trade practices rules. Many states have enacted statutes requiring businesses that have suffered a security breach to notify individuals about the breach under certain circumstances.

Beyond the statutory and regulatory implications, businesses suffering a data breach may face civil liability. Because this is a new and evolving area of law, a company may find itself facing various causes of action. Commonly raised causes of action for data breach include negligence, breach of contract, emotional distress, and state unlawful trade practices and consumer protection claims. There has also 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.

The Attorney-Client Privilege and Investigating a Data Breach

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

The attorney-client privilege protects communications between an attorney and the attorney’s client. 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 interest in the observance of the law and administration of justice. 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. A communication is only confidential if it is not intended to be disclosed to third persons, and such a disclosure may result in waiver of the privilege. The attorney-client privilege is held by the client, not the lawyer.

Communications between in-house counsel and corporate IT professionals may themselves be privileged when they meet the subject matter test established by the United States Supreme Court in Upjohn Co. v. United States. Under Upjohn, the privilege protects communications by a corporate employee, regardless of position, (1) when 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. With respect to internal investigations, courts have generally held that “an attorney’s investigation [to obtain facts] may constitute a legal service, encompassed by the privilege.”

But the protection of the attorney-client privilege is often applied more narrowly and cautiously to corporate in-house counsel. The New York Court of Appeals has stated that less protection is often 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 on-going permanent business relationship rather than specific requests for legal advice.

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 that merely involving in-house counsel protects the information and investigation from disclosure in discovery litigation. In-house attorneys, however, 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.

There is no presumption that documents are privileged, and the party asserting the privilege has the burden of establishing all of the elements of the attorney-client privilege. Ordinary business documents 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 in legal proceedings. The dual roles of in-house counsel – as a corporate officer and an attorney – may leave the reports of internal investigations open to disclosure in discovery. Confusion often arises when courts are forced to determine whether the in-house counsel was acting in their business capacity or in their legal capacity. It is often not clear from the face of documents or facts surrounding communications, especially in the area of fact-gathering and regulatory compliance. For example, correspondence may contain both business and legal advices. It is well settled that merely sending documents, correspondence, and e-mails to in-house counsel is not enough to establish privilege.

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

The Work-Product Privilege and Investigating a Data Security Breach

The work-product privilege may also protect an investigation into a data-security breach. In particular, when a business hires an outside firm to investigate a security-breach incident and to
advise the business regarding risk mitigation, that advice and investigation should qualify for protection under the work–product privilege.

The work–product doctrine 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.”\(^\text{18}\) In federal courts, Federal Rule of Civil Procedure 26(b)(3) protects attorney work product from discovery.\(^\text{19}\) The work–product privilege was created to protect trial preparation materials that might real an attorney’s evaluations and strategies about a case.\(^\text{20}\) The two types of materials covered by the work–product privilege are opinion work product, and ordinary work product. Opinion work product consists of mental impressions, opinions, conclusions, legal theories and such of an attorney or other representative of a party.\(^\text{21}\) This encompasses attorney 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.\(^\text{22}\) Opinion work product is generally entitled to greater protection than ordinary work product.\(^\text{23}\) Ordinary work product, including raw factual information, consists of preparation materials that do not disclose opinions or impressions.\(^\text{24}\) Ordinary work product is not discoverable unless the party seeking discovery has a substantial need for the materials and the party is unable to obtain the substantial equivalent of the materials by some other means.\(^\text{25}\) 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 as work product.\(^\text{26}\)

The scope of the work–product privilege extends to materials that were prepared by a party or its representative, including an attorney, consultant, indemnitor, insurer, or agent.\(^\text{27}\) While the work–product privilege does not shield underlying facts and event information from discovery, the compilations and collections performed by an attorney or an attorney’s team would be protected from disclosure in discovery. Like the attorney–client privilege, the work–product privilege may be waived by intentionally disclosing the materials to third parties.\(^\text{28}\) In addition, the privilege may be waived if it is not timely asserted.\(^\text{29}\)

The applicability of the privilege generally turns on whether the work was performed “in anticipation of litigation.” Under federal law, “in anticipation of litigation means that the primary motivating purpose behind the creation of the document was to aid in possible future litigation.”\(^\text{30}\) The prevalence of lawsuits in connection with data–security breaches lends credence to a claim that information gathered or acquired by an attorney in connection with a data breach was gathered in anticipation of litigation. Hiring outside counsel makes a clear statement that the company sought legal advice in anticipation of potential litigation, as opposed to a corporation turning to the advice of in–house counsel, who may have a more difficult time of establishing that the consultation was in anticipation of litigation.

Responding to a Data–Security Breach – The Attorney’s Ethical Obligations and Role

When a data breach occurs, evidence should be preserved and collected diligently. It is critical to document what the client was doing at the time of the data breach incident in order to comply with ethical and discovery obligations. Attorneys have ethical obligations to avoid having the client get into a spoliation situation. Also, litigants have an obligation to preserve relevant evidence for the use of the adverse party.

Spoliation is a significant danger in responding to a data breach. Generally, an adverse inference is created 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.”\(^\text{31}\) The rationale for the rule that the fact finder may draw an adverse inference is predicated on the “common sense observation that a party who has notice that [evidence] is relevant to litigation and who proceeds to destroy [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.”\(^\text{32}\) Such an instruction is extremely damaging to the litigant’s case and may be far worse than the inference that the jury would have drawn if the evidence was produced. Courts have the authority to grant an adverse inference instruction even where party did not intentionally destroy the evidence. In such cases, where a party failed to preserve evidence relevant to the
case, the jury could be instructed that it may infer that the unproduced evidence was damaging to that party’s case and supported the claims of the adverse party.\textsuperscript{33} It is important to recognize that spoliation applies to electronic information as well as other documents, destroyed intentionally or unintentionally. When responding to a data breach, attorneys may want to have a computer forensics expert on their investigative team to make certain that all the electronic information is properly preserved.

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. 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.

**Statutory Notification – Advising Clients Regarding New Statutes, Rules, and Regulatory Compliance**

Data breach issues are of concern to every individual interacting with modern technology. Only within the past few years have many states enacted data breach and/or identity theft statutory schemes.\textsuperscript{34} As a result, very few of the statutes have been applied or interpreted by the state or federal courts. In an effort to assure 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.

It is also important to determine, upon advice of counsel, how notice is required to be given, when notice should be given, the form notice should take, and what the contents of any notice should be. States vary in their definition of what constitutes “personal information.”\textsuperscript{35} Because of this, it is critical to determine what your state’s statutes defines as “personal information,” in order to determine if the breach is one giving rise to the notice requirement, as well as statutory requirement for how notice is to be given.

An attorney giving advice about statutes that have yet to be interpreted authoritatively has to be particularly careful. While an attorney is generally 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,” 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 . . . .”\textsuperscript{36} To meet this standard, research should include legislative history when available because if the language of that statute is ambiguous or confusing, a reading of the legislative materials may provide insight as to how to approach a new law or regulation.\textsuperscript{37} Research should also be expanded to encompass decisions regarding similar statutes in other jurisdictions.\textsuperscript{38} A client should also be advised that the plaintiff in an action brought pursuant to a data-breach-notification statute is likely to be a public agency and that the agency’s opinion regarding the statutory requirements is generally accorded deference by courts.\textsuperscript{39} Opinion letters should contain caveats notifying the client that this is a new and unpredictable area of litigation.

**The Attorney’s Ethical Obligations During Litigation Over a Data Security Breach**

Lawsuits over data security breach 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 attorney, certifying that, after reasonable inquiry, the disclosure is complete and correct as of the time it is made.\textsuperscript{40} Discovery obligations also require a signature by 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, and attorneys are also subject to sanctions if these certifications are made in violation of the rules.\textsuperscript{41} Attorneys also have a duty to supplement disclosures and discovery responses under Federal Rule of Civil Procedure 26(e).

The new e-discovery rules raise additional issues and obligations. It is advisable to include IT personnel as part of the discovery team in light of the new e-discovery 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(f) establishes the so-called “safe harbor” for electronic discovery: “Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.”

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. While Rule 37(f) 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 qualify that language. The Committee Notes provide that

Rule 37(f) 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.

Accordingly, data that is not lost 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.

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 new rule has carved out a safe–harbor exception, but the scope of that 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. Also left unanswered by the Committee Notes is the question of whether the courts are to apply a subjective standard or an objective standard in determining whether 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 the use of the adverse party. And 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,” they are guilty of spoliation.

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 information stored in RAM (“Random Access Memory”) is a tangible document that must be turned over in litigation, despite the fact that RAM is not permanent storage and is continually being updated, changed, deleted, or overwritten in business computers. Attorneys should also 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’s that require a broker–dealer to maintain records of electronic communications for a certain time period. While it is true that a private litigant in a federal civil action seeking such information because it is relevant to his or her case against a party has no private right of action under industry record keeping rules, there is a strong argument that a document retention policy that destroys evidence for use in federal court that the party was required by law to independently maintain is unreasonable as a matter of law.

Conclusion

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. And attorneys should not rely exclusively on the “safe harbor” provision when responding to e–discovery requests.
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.

For instance, in *Pisciotta v. Old Nat. Bancorp*, --- F.3d ----, 2007 WL 2389770 (7th Cir. 2007), the Seventh Circuit held that Indiana law did not recognize such a claim.

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


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


*Upjohn*, 449 U.S. at 389–90.

*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 made “clear that fact-finding which pertains to legal advice counts as ‘professional legal services.’ ”).


*Id.*

*United States v. Munoz*, 233 F.3d 1117, 1128 (9th Cir. 2000).


*See In re Avantel*, 343 F.3d 311, 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”).

*In re Martin Marietta Corp.*, 856 F.2d 619, 624 (4th Cir.1988).


*Fed. R. Civ. P. 26(b)(3).*

*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 Litigation*, 859 F.2d 1007, 1015 (1st Cir. 1988); *Shelton v. American Motors Corp.*, 805 F.2d 1323, 1328–29 (8th Cir. 1986).

*In re Cendant Corp. Securities Litigation*, 343 F.3d 658, 663 (3d Cir. 2003).

*In re Green Grand Jury Proceedings*, 492 F.3d 976, 981 (8th Cir. 2007).

*See FRCP 26(b)(3).*


37 See 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.”).

38 See, e.g. Pope v. Brock, 912 So.2d 935, 938 (Miss. 2005) (“under 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.”); Martinez v. Enterprise Rent–A–Car Co. 13 Cal.Rptr.3d 857, 862 (Cal. App. 2004) (“Where, 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.”).

39 See, e.g. Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc., 467 U.S. 837, 842–43 (1984) (agency interpretation of governing statutes entitled to deference); In re Director of Property 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 Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. 1998).
49 17 C.F.R. §210.1–01 et seq.