ASSOCIATION OF BUSINESS TRIAL LAWYERS
SAN DIEGO

abtl REPORT

Volume XIV No. 2 *Spring 2007*

From the Courts

Dealing with Electronically Stored Information: Production & Privilege

by the Hon. Anthony J. Battaglia, United States Magistrate Judge

Electronically stored information, referred to as "ESI", is prolific in our lives. It exists in our computers, computer peripherals (like printers and fax machines), PDA's, as well as pagers and wireless (cell) telephones. It also resides in storage on disks, backup tapes or removable drives, CDs and other forms of media. There is also a great deal of hidden data in areas such as "metadata", system data, and deleted data readily overwritten.

Hon. Anthony J. Battaglia

The greatest technological challenge for lawyers and judges is dealing with ESI and "E-discovery." From preservation of ESI to its disclosure and discovery, more questions than answers currently face the legal community.

In August 2004, the Judicial Conference Committee on Rules of Practice and Procedure proposed amendments to Civil Rules 16, 26, 33, 34, 37 and 45 to deal with the distinctive features and issues associated with ESI. These amendments took effect on December 1, 2006. Once enacted, they superceded existing law. 28 U.S.C. §2072(b).

In general terms, as reported by the Civil Rules Advisory Committee in its May 17, 2004 Report

(See "ESI" on page 6)

A Tribute to the Hon. J. Michael Bollman

by Hon. J. Richard Haden, JAMS

Mike Bollman knew more about friendship and being a friend than anyone I've ever known. Many years ago he encountered a lawyer who was obviously having a bad day. When he asked about the problem, the lawyer told him it was his birthday but no one seemed to know or care. Mike immediately wished him "Happy Birthday" and assured him he'd call him to do the same next year. He continued to call this lawyer on his birthday for over 30 years. During that time, Mike's "Birthday list" grew to over 100 and expanded to include "Happy Anniversary," "Congratulations," etc. Mike not only maintained his list, he also coached his best friends on developing their own and often called them with reminders to make

J. Michael Bollman

(See "Michael Bollman" on page 6)

Inside

President's Column

by the Hon. Jan M. Adler, President ABTL

As I write my second column for the ABTL Report, it is hard to imagine that March Madness is already behind us and that baseball season is underway. In the first three months of the year, our chapter has been characteristically busy and productive. In January, we presented an entertaining and educational program featuring Vincent Bartolotta, Jr. and David Noonan, the past two winners of the Broderick Award (which is co-sponsored by ABTL each year), who gave us their insights on what to do in trial "When Things Go Wrong."

Hon. Jan M. Adler

In February, we presented another in our series of "Meet the Judge" brown bag lunch programs featuring U.S. Magistrate Judge Cathy Bencivengo. In March, a distinguished panel of state court judges, consisting of Presiding Judge Janis Sammartino and Judges Jeffrey Barton, Steven Denton and Frederick Link, presented a highly informative program on the Independent Calendar System and the overflow civil trial department presided over by Judge Link. During the March dinner program, we were all delighted to learn from Chief Judge Irma Gonzalez that Judge Sammartino had been nominated earlier in the day to become our newest United States District Court Judge. We also recognized Cynthia Chihak, who will receive this year's Broderick Award at the 23rd Annual Red Boudreau Dinner on June 16. We thank all of the lawyers and judges who have taken the time and effort to present these excellent programs.

Looking forward, we have lined up numerous additional outstanding programs for the remainder of the year. On April 24, we will present Judge Ronald Styn in our next "Meet the Judge" brown bag lunch program. On June 10, in conjunction with the San Diego chapter of the Harvard Law School Association, we will present a dinner program featuring Harvard Law School Professor Charles Ogletree, who is a truly gifted and dynamic speaker. We will present a very special and inspiring program on September 10 featuring Lieutenant Commander Charles Swift, who represented Guantanamo detainee Salim Ahmed Hamdan before the United States Supreme Court. We will close out this year's schedule on December 3 with a flourish, presenting two nationally renowned experts on the Supreme Court — Professors Erwin Chemerinsky of Duke University and Charles Whitebread of the University of Southern California — who will discuss the first two years of the Roberts Court and what we might expect from the Court in the future.

I also want to remind all of our members to save the weekend of October 5-7 for ABTL's Annual Program. This year's program will take place at the Silverado Resort in the magnificent Napa Valley, and will focus on the cutting-edge topic of information security and privacy. The keynote speaker for the event will be former United States Supreme Court Justice Sandra Day O'Connor. In addition, there will be a special wine tasting event at the resort featuring "The Secret Wines of the Napa Valley," at which former Stanford University Law School Dean Katherine Sullivan will speak. We thank Marisa Janine-Page, Frank Tobin, Katherine Bacal and Monty McIntyre, our chapter's representatives on the statewide planning committee, for their hard work on what promises to be a wonderful program.

As I stated in my first column, while our chapter is acclaimed for the high quality of its programs, I have long thought that its most important function is to promote cordiality, professionalism and civility among our membership. Several years ago, our chapter adopted

(See "President's Column" on page 7)

Ethics, Professionalism and Civility Guidelines for the ABTL of San Diego

Adopted by the Association of Business Trial Lawyers Board of Governors

The Association of Business Trial Lawyers of San Diego has adopted Ethics, Civility and Professionalism Guidelines. They identify principles of conduct for lawyers engaged on litigation. The goal of the guidelines is to eliminate unnecessary conflict and to reduce the level of contentiousness and stress in the resolution of legal disputes.

The ABTL of San Diego, as a voluntary association, does not intend these guidelines to provide a basis for further litigation, or for sanctions or penalties. While some of the following guidelines are based on statutes or existing rules of professional conduct, others go beyond any requirement of current law. Lawyers are encouraged to apply the spirit of the guidelines, as appropriate, in circumstances that are not specifically addressed in any of the guidelines.

Nothing in the guidelines is intended to inhibit a lawyer's zealous representation of his or her client's interests. The guidelines are, however, based on the belief that zealous representation is compatible with professional and civil conduct.

The ABTL of San Diego encourages firms and individuals to adopt these guidelines as their own. As part of that commitment, firms are also encouraged to subscribe to the voluntary interfirm resolution process discussed below.

Guidelines

1. A lawyer must work to advance the lawful and legitimate interests of his or her client. This duty does not include an obligation to act abusively or discourteously. Zealous representation of the client's interests should be carried out in a professional manner.

2. A lawyer should not engage in derogatory or prohibited conduct on the basis of race, religion, gender, sexual orientation or other immutable characteristics of any person.

3. A lawyer should not behave in an offensive, derogatory or discourteous manner even when his or her client so desires. If necessary, a lawyer should advise the client that civility and courtesy are not signs of weakness.

4. The client's best interests are often served by alternatives to litigation. A lawyer should consider the possibility of settlement or alternative dispute resolution in every case and, when appropriate, bring such alternatives to the client's attention.

5. A lawyer should be punctual and prepared for all court appearances so that all matters may commence on the time and proceed efficiently. Lawyers should treat judges, counsel, parties, witnesses and court personnel in a civil and courteous manner, not only in court but in depositions, conferences and all other written and oral communications.

6. Where all alternative manner of service would not prejudice the client's legitimate interests, a lawyer should not use the timing and manner of service to embarrass or disadvantage the party or person on whom the papers are served.

7. A lawyer should consider opposing counsel's legitimate calendar conflicts when scheduling or postponing hearings, depositions, meeting or conferences, unless to do so would be contrary to the legitimate interests of his or her client. A lawyer should not arbitrarily or unreasonably refuse a reasonable request for an extension of time. In considering a request for an extension of time, a lawyer may appropriately take into account the interests of his or her client, whether there have been prior requests for extensions, the time required for the task, the nature of the adversary's scheduling difficulty, and whether the adversary will grant reciprocal reasonable requests.

8. Discovery is an important and appropriate litigation tool, and lawyers are expected to pursue such discovery as is appropriate in order to evaluate and establish the client's position in litigation. A lawyer should not, however, use discovery to harass opposing counsel or the opposing party or for the purpose of delaying the efficient resolution of a dispute. A lawyer should explore with opposing counsel alternatives to formal discovery that will achieve the same objective at lower cost.

(See "Guidelines" on page 11)

Is Your Client Prepared To Comply With the Data Security Breach Notification Laws?

By Alan M. Mansfield, Rosner & Mansfield LLP
Editor ABTL Report

It is now part of routine life that consumers receive a letter from a financial institution advising them that personal data in a third party's possession has been compromised and that they may need to take steps to protect themselves from identity theft. Or read in the news that a laptop or flash key with personal medical information or client data has been lost. Or for a company to learn, as the nationwide retailer T.J. Maxx recently revealed, that its customer data base with over 45 million names, credit card and/or driver's license information has been accessed from outside sources, and now the company must take immediate steps to remedy the situation.

This is not an isolated or theoretical issue for companies and consumers. According to www.attrition.org/dataloss and www.privacyrights.org/ar/ChronDataBreaches.htm, over 150 million consumer records have been compromised in close to 1,000 separate incidents since 2004. The U.S. Department of Justice reports that over 3.5 million consumers are the subject of identity theft *each year*, while the U.S. Federal Trade Commission places that figure closer to nine million individuals annually. If you have been one of those unfortunate victims, you know that the time and money necessary to remedy such a breach is sig-

Alan M. Mansfield

(See "Data Breach" on page 15)

Does The *Pioneer Electronics* Decision Work A Significant Change In the Privacy Law Arena?

By Richard Gluck, Esq., Fairbank & Vincent LLP

Thirty years ago the California Supreme Court held that businesses have a duty to notify their customers before disclosing their private information in litigation. See *Valley Bank of Nevada v. Superior Court*, 15 Cal. 3d 652, 658 (1975). Ever since then, plaintiffs and defendants in class actions have been fighting over how and when plaintiffs may obtain contact and other private information about those customers. The battle pits the plaintiffs' need to identify potential class members and witnesses against the customers' constitutionally protected privacy rights. The most recent skirmish left the plaintiffs' bar declaring victory, after the California Supreme Court upheld an order permitting discovery of customer contact information unless the customers affirmatively objected to such disclosure. See *Pioneer Electronics (USA), Inc. v. Superior Court*, 40 Cal.4th 360 (2007). But a closer look at this decision shows that those claims of victory may be overstated.

Richard Gluck

I. Background of *Pioneer*

Pioneer Electronics sells portable DVD players to consumers. Pioneer's DVD players apparently cannot

(See "Pioneer" on page 12)

Michael Bollman

Continued from page 1

calls themselves. Dick Murphy and I were lucky enough to receive many of both varieties of these calls for many years.

At Mike's recent Celebration of Life, attended by over 400 members of our legal community, long-time friend Bruce Beals recalled that if you mentioned to Mike you were planning a vacation, you could expect to receive from him in short order a stack of brochures on any destination you may have suggested. He was the consummate planner and master of follow-up because he cared more about his friends and family than himself. Any event for Mike was much less about the destination and much more about who was coming along with him. He had an endless supply of great tickets to ballgames and theatre and delighted in organizing elaborate plans for these outings with his friends. He would much rather do something for someone else than for himself.

Mike was born April 6, 1939, in Rock Island, Illinois. He graduated from high school there before attending Coe College in Cedar Rapids, Iowa, where he earned a Bachelor's Degree in English. After graduating from Coe, he attended the University of Iowa, where he earned a Master's Degree in Journalism. He then attended Chicago-Kent College of Law.

Mike was admitted to the Illinois Bar in 1965 and the California Bar in 1968. He moved to San Diego in 1968 where he became a partner at Smith, Bollman and Knoepp.

In 1972, the Junior Chamber of Commerce named Mike the Outstanding Young Man of San Diego. In 1985, he was appointed to the El Cajon Municipal Court, where he served as Presiding Judge in 1989 and was named Judge of the Year by the San Diego County Judge's Association. He was appointed to the Superior Court where he distinguished himself as a family law, civil independent calendar and settlement judge. He was an ABTL Board Member and long-time contributor to ABTL programs and this publication.

Mike was a devoted husband and father. His wife, Susan, their children, Carolyn and Thomas, and brother, Brian Bollman, survive him. He was a wonderful friend and respected colleague. Mike passed away on February 6, 2007. ▲

ESI

Continued from page 1

(revised August 3, 2004), page 5, these amendments have an impact on issues involving preservation, production, and privilege associated with ESI. Of these issues, preservation of ESI relevant to litigation is not covered extensively by the proposed new rules and by itself is the subject of extensive analysis and articles. As a result, this article focuses on the issues of production and privilege regarding ESI under the new Federal Rules.

I. Production of ESI Under the Proposed Rules

The new federal rules require early attention to ESI by the parties, define the practical universe of data within the scope of disclosure and discovery, and provide procedural guidance related to format and procedures under various devices related to ESI.

A. Early Attention to ESI

The concept of early attention to ESI is addressed in two ways in the new federal rules. First, Rule 16(b)(6) has been amended to reflect that the Court may include provisions for disclosure or discovery of electronically stored information, as well as the parties' agreement, if any, for protection against waiver of privilege, in the Rule 16(b) Scheduling Order. This ensures early attention by the Court.

Second, Rule 26(f) was amended to require parties discuss any issues relating to preserving discoverable ESI at the Rule 26(f) conference. The parties also need to develop a discovery plan that would cover any issues relating to disclosure or discovery of ESI, including the form or forms in which it should be produced and whether the parties have agreed to or require the Court to enter an order protecting their right to assert privilege after production of privileged information.

One issue that needs particular attention is the protocol for computer record searches. This is not only true in a general sense but also as it relates to any deleted information that might be occupying "unallocated space" awaiting to be overwritten. A court addressed this issue in *Antioch Co. v. Scrap-Book Borders, Inc.*, 210 F.R.D. 645 (D. Minn. 2002), which is a good reference point in this regard.

The Court in *Antioch* felt the parties could deal

(See "ESI" on page 7)

ESI

Continued from page 6

with the disclosure of current data that was requested. As to unallocated space, however, it had the computer forensic expert selected by the plaintiff review a "forensic copy" of defendant's data on a confidential basis. A list of key data in areas relevant to the case was then provided to the defendant and the Court. The defendant then used the filtered data to respond to the plaintiff's document requests.

In a recent case in the Southern District of California the Court took a different approach, requiring the joint experts to develop a search protocol for the "mirror image," and then proceed to jointly search and review any information recovered. The defendant's expert was allowed, to the extent possible, to identify privileged and non-relevant information within the unallocated disk space. A privilege log was cre-

(See "ESI" on page 8)

President's Column

Continued from page 2

"Ethics, Professionalism and Civility Guidelines for the ABTL of San Diego." I have requested that these guidelines be reprinted in this edition of the ABTL Report. I ask that each and every one of us review the guidelines for the purpose of re-dedicating ourselves to the principles contained in them. Not only is the practice of law decidedly more enjoyable and less stressful when the participants in a case act in a civil, ethical and professional manner, but I can assure you from my experience as both a lawyer and a judge that one's effectiveness as an advocate is immeasurably enhanced by conducting oneself honestly, civilly and professionally. So, as the title of a program on professionalism in which I participated two years ago aptly proclaimed, "Be a Zealous Advocate, Not a Zealot!" Thank you, and I look forward to seeing you at our upcoming programs. ▲

Continued from page 7

ated therefrom and provided to plaintiff. Only the remaining non-privileged relevant information in the unallocated disk space was made available to the plaintiff for review. The Court then dealt with issues with regard to privilege or excluded material thereafter. See, *Venture Catalyst, Inc. v. Tech Results, Inc.*, U.S. District Court for the Southern District of California, Civil No. 05cv0063 W (AJB), Docket No. 24.[1]

The amended rules also clearly contemplate the initial disclosure of ESI as part of the parties' obligations under Rule 26 by adding "electronically stored information" to Rule 26(a)(1)(B). Numerous courts had previously so held, even prior to these amendments. *Bills v. Kennecott Corp*, 108 F.R.D. 459 (D. Utah 1985); *Playboy Enterprises, Inc. v. Welles*, 60 F. Supp.2d 1050 (S.D. Cal. 1999); *Rowe Entertainment, Inc. v. The William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. 2002). Fed. R. Civ. P. 26(f)(3) places ESI on the agenda for the Rule 26(f) conference by adding, "any issues relating to disclosure or discovery of electronically stored information . . .". So even if you are not seeking your opponents' ESI, you may need to discuss disclosing ESI under Fed. R. Civ. P. 26(a).

B. Defining the Universe (ESI That is Not Reasonably Accessible).

In an attempt to define both the scope and the breadth of the discovery of ESI, and recognizing the difficulty in locating, retrieving and providing discovery of some electronically stored information, Rule 26(b)(2)(B) was amended to provide that "a party need not provide discovery of electronically stored information that the party identifies as not reasonably accessible because of undue burden or cost." This is commonly referred to as a "two tiered system." The burden of establishing "not reasonably accessible", and therefore being in the "second tier", is firmly on the party from whom the discovery is sought. *Id.* On a motion by the requesting party, the responding party must show that the information is not reasonably accessible. If that showing is made, the Court may order discovery of the information for good cause and may specify terms and conditions for such discovery. *Id.* These "terms and conditions" will likely involve consideration of cost shifting issues. No definition of "reasonably accessible" is set forth in the rule. This is because, as the Committee explains in the Note to subdivision (b)(2), it is simply "not . . . possible to define in a rule the different types of technical features that may effect the burdens and costs of accessing electronically stored information."

A party's duty to respond to this discovery is stated in the Committee Note to subdivision 26(b)(2) as "produce electronically stored information that is relevant, not privileged and reasonably accessible, subject to the (b)(2)(C) limitations that apply to all discovery." The Committee goes on to state that the responding party must "identify, by category or type, the sources containing potentially responsive information that it is neither searching nor producing. The identification should, to the extent possible, provide enough detail to enable the requesting party to evaluate the burdens and costs of providing the discovery and the likelihood of finding responsive information on the identified sources." *Id.*

As noted previously, the burden of establishing that the discovery is not "reasonably accessible" is on the responding party. In a discovery dispute where the appropriate showing is made, the burden shifts and the requesting party has the burden to show that it has a need for the discovery that outweighs the burdens and costs of locating, retrieving and producing the information. In trying to establish a focus on what is "reasonable," the balancing test under new Rule 26(b)(2)(C) is the likely source.

C. Interrogatories, Document Requests and Subpoenas.

Fed. R. Civ. P., Rule 33(d) was amended to include provisions regarding ESI, which would allow "a responding party to substitute access to documents or electronically stored information for an answer only where the burden of deriving the answer will be substantially the same for either party." See Committee Note to Rule 33(d). The rule already provides this option to produce business records, but now specifically addresses ESI. The rule still requires the party served with the interrogatory to "specify" the records, and the "specification shall be in sufficient detail to permit the interrogating party to locate and to identify as

(See "ESI" on page 9)

ESI

Continued from page 8

readily as can the party served, the records for which the answer may be ascertained." Fed. R. Civ. P. 33(d). The Committee Note to proposed Rule 33 characterizes this duty as follows: the party "must ensure that the interrogating party can locate and identify it."

Rule 33(d) contemplates affording the requesting party the opportunity to "examine, audit or inspect" as well as make compilations, abstracts or summaries of the identified data. As a result, and notably, when a party invokes Rule 33(d), they may "be required to provide direct access to its electronic information system, but only if it is necessary to afford the requesting party an adequate opportunity to derive or ascertain the answer to the interrogatory." *Id*. Faced with this issue of "direct access" a responding party may decide it is more prudent to provide the answer itself rather than utilize the provisions of Rule 33(d). A search of a party's active files should certainly be discouraged in any case. The issue of changed data, or lost data, as well as questions of privacy, are extreme. Utilizing a forensic copy of the enumerated files may be a good alternative to allow the "sampling" without the attendant risks.

Concerning requests for production of documents, Rule 34(a) also includes electronically stored information relative to a party's request to "inspect, copy, attest or sample . . . documents or electronically stored information."[2] The Committee Note to Rule 34 states a change in the treatment of the discovery of ESI, putting it on an "equal footing" with discovery of "paper documents." The same Committee Note states that "the change clarifies that Rule 34 applies to information that is fixed in a tangible form and to information that is stored in a medium from which it can be retrieved and examined." The Committee Note also provides some practical information for addressing Rule 34 discovery:

(1) The term "documents" should be understood to encompass, and the response should include, ESI information unless a clear distinction is drawn between ESI and other type of documents;

(See "ESI" on page 10)

ESI

Continued from page 9

(2) Rule 34 is intended to be broad enough to cover all current types of computer based information, and flexible enough to encompass future changes and developments; and

(3) The Rule's requirement that the producing party "translate" stored information into usable form does not contemplate translating from one human language to another.

Rule 34(a)(1), like Rule 33(d), also provides that a party may request an opportunity to test or sample material sought under the rule in addition to inspecting and copying it. This may be of particular value with ESI considering its nature and volume. The standard notions of burden and intrusiveness may be raised pursuant to Rules 26(b)(2) and 26(c) and in opposition to such a request. *See*, Committee Note to Rule 34(a).

Rule 34(b) now provides that the request may specify the form or forms in which ESI is to be produced. The responding party is entitled to object to the requested form in the response to the request. If no form is specified in the request, then the responding party must state the form or forms it intends to use when responding. Unless requested or ordered to agree, a responding party must produce any requested ESI in the form or forms in which it is ordinarily maintained, or in a form or forms that are reasonably usable. Finally, a party need only produce ESI in one form per Rule 34(b)(iii).

Rule 45 was also amended in conformity with changes to Rules 26 and 34, and reference to ESI is now specifically included throughout new Rule 45. For example: (1) the testing or sampling language from Rule 34(a) has been inserted into Rule 45(a)(1)(c); (2) the subpoena is allowed to specify the form of production, similar to proposed Rule 34(b), and where a subpoena does not specify the format, the responding party will be required to produce the information in the form or forms in which it is ordinarily maintained, or in a form or forms that are reasonably usable consistent with proposed Rule 34(b)(ii); (3) the "reasonably accessible" limits as to scope and breadth incorporated into Rule 26 (b)(2)(B) are repeated in Rule 45(d)(1)(D); and, (4) privilege will be dealt with under the same "status quo" concept (discussed below) set forth in Rule 26(b)(5). The same Rule 26(b)(5) provision is inserted into Rule 45(d)(2)(B).

II. Handling Privilege Under the Proposed Rules.

With close to a billion bytes of information in a computer storage system (including data, metadata, unallocated space awaiting to be overwritten), it is not always, if ever, feasible to fully search ESI for privilege. The Committee Note to Rule 26(b)(5) states that "the risk of waiver, and the time and effort required to avoid it, can increase substantially because of the volume of electronically stored information and the difficulty in ensuring that all information to be produced has in fact been reviewed."

Simply stated, the Rule as amended provides that if information is produced that is subject to a claim of privilege or a protection as trial preparation material: (1) the party making the claim may notify any party that received the information of the claim and its basis; (2) the party notified must promptly return, sequester, or destroy the specified information and any copies it has; (3) the receiving party is otherwise restricted from use or disclosure of the information until the claim of protection is resolved; and (4) the "receiving party" must take reasonable steps to retrieve any information that was disclosed prior to notification. Finally, the receiving party may promptly present the information to the Court under seal for a determination of the claim. The goal is to preserve the status quo until the Court can consider the questions of privilege and protection of work product.[3]

Notably, Rule 25(b)(5)(B) does not address whether the privilege or protection it has asserted after production was waived by the production. The issue of waiver is left to the Courts under the principles developed through case law. The impact of Rule 25(b)(5)(B) is to provide a procedure for presenting and addressing these issues, nothing more.

The Committee Note to Rule 26(b)(5) describes that the notice and claim for the basis of privilege must be as "specific" as possible. This is to allow the receiving party to decide whether to challenge the claim, and determine whether the claimed privilege or protection applies in the first place or is otherwise waived. Unless the notice is sufficiently detailed, the receiving party will be hampered in its attempt to decide its course of action.

There are a wide range of approaches

(See "ESI" on page 10)

ESI

Continued from page 10

employed by courts regarding waiver by inadvertent disclosure. "There is no consensus . . . as to the effect of inadvertent disclosure of confidential communications." *Alldread v. City of Grenada*, 988 F.2d 1425, 1434 (5th Cir. 1993). Courts deal with the issue in a variety of ways. These range from a strict liability approach such that any disclosure forfeits the privilege; a subjective intent approach, so that only a deliberate disclosure forfeits the privilege; and, a balancing test in which the Court considers all relevant circumstances. *United States ex rel. Bagley v. TRW*, Inc., 204 F.R.D. 170 (C.D. Cal. 2001).

Where courts use the "balancing" approach, a number of factors are considered in determining whether to excuse a waiver as "inadvertent." These include: (1) reasonableness of the precautions taken to prevent the disclosure in the first place; (2) the time that has passed since the disclosure; (3) the volume of discovery involved (which can be particularly extensive with ESI); (4) the amount of information disclosed; and, (5) and whether justice would be better served by relieving the party of its mistake. *Id.* at 177.

However, the time involved and the extent to which a party has relied upon the documents is extremely critical. Where a party in reliance on receipt of a document, and after a period of time, has relied upon the information in formulating or refining claims or defenses, or has used the information against the producing party, the privilege may indeed be lost. See *Bowles v. National Ass'n of Home Builders*, 2004 WL 2203831 (D.C. Cir 2004).

The intention of the Rules Committee was to create rules that will be flexible enough to embrace ever-changing technology. This wisdom should make these newly revised rules stable for many years to come. ▲

Editor's Note: This article was reprinted, with updates to reflect the current status of amendments, from Federal Lawyer, Vol. 53, No. 4 (May 2006).

1 This order is available on-line through the Court's PACER system at www.casd.uscourts.gov.

2 Changes to Rule 34(a) in 1970 made it clear that "records" included electronically prepared and stored information.

3 Withers, Ken, "We Have Moved The Two Tiers and Filled in The Safe Harbor," The Federal Lawyer, P. 50, Nov./Dec. 2005.

Guidelines

Continued from page 3

Lawyers should be willing to agree to mutual stipulations of genuinely undisputed facts.

9. Depositions are generally conducted by lawyers without direct judicial supervision and are frequently the most uncivil phase of litigation. A lawyer should take depositions only when actually needed to learn facts or preserve testimony, and should not engage in any conduct during a deposition that would not be appropriate in the presence of a judge.

10. Written discovery should be limited to seeking such information and documents that a lawyer reasonably believes are necessary for the prosecution or defense of an action. A lawyer responding to written discovery or complying with court rules requiring disclosure should not employ artificially restrictive interpretations to avoid disclosure of relevant and non-privileged information or documents.

11. A lawyer's submissions to the court should be professional in tone. A lawyer should at all times strive to be concise and to state accurately the law, the facts and the parties' positions. Briefs and pleadings should not be written in an unnecessarily inflammatory style.

12. A lawyer should avoid personal attacks on all court officers, including judges and opposing counsel, and should not comment adversely on the intelligence, integrity, motive or conduct of judges or opposing counsel, except in the rare circumstance when such matter is legitimately in issue. Even when the zealous representation of a client may necessitate allegations of improper conduct, a lawyer should review such allegations to ensure that they are justified and supported by the evidence. A lawyer should bear in mind that *ad hominem* comments frequently are unpersuasive, increase the level of personal antagonism, and tend to diminish public respect for lawyers and the courts.

13. A lawyer should not seek judicial sanctions against a party or opposing counsel without first conducting a reasonable investigation and unless the lawyer is convinced that sanctions would be fully justified.

14. Every law firm's reputation is affected by the professional conduct of its lawyers acting in the name of the firm. Law firms should include

(See "Guidelines" on page 12)

Pioneer

Continued from page 5

play all DVD formats, a "defect" about which Pioneer allegedly failed to inform consumers. One of those consumers brought suit against Pioneer on behalf of all customers who purchased the same model DVD player.

In response to discovery requests seeking the identity of any other customer who had complained about the DVD players, Pioneer produced redacted information showing that it had received roughly 700-800 complaints. Plaintiff moved to compel Pioneer to provide unredacted copies of the complaints and the names and contact information of each customer who had complained. Pioneer opposed the motion, arguing that the discovery violated its customers' privacy rights protected under the California Constitution, Cal. Const., art. I, § 1.

At the hearing on the motion, the trial court acknowledged plaintiff was seeking information protected by the Constitution's right to privacy. To protect that right, the trial court, relying on *Colonial Life & Accident Ins. Co. v. Superior Court*, 31 Cal. 3d 785, 787-790 (1982), ordered Pioneer to write and send letter (a *"Colonial Life"* letter) to each customer who had complained about the DVD players explaining that Pioneer had been asked to provide the customer's information to plaintiff's counsel and would do so unless the customer objected.

The parties then submitted competing *Colonial Life* letters. Pioneer submitted an "opt-in" letter that would inform customers that Pioneer would disclose the information only if the customers responded affirmatively that they did not object, while Plaintiff submitted an "opt-out" letter that would inform customers that the information would be disclosed unless the customers objected in writing. The trial court initially accepted Pioneer's version, finding that "[i]n order for the letter to have any meaning, it should require an affirmative response, as did the letter in the *Colonial Life* case." *Pioneer*, 40 Cal. 4th at 365. The trial court later reversed itself and accepted plaintiff's version, ordering Pioneer to send customers the opt-out letter. The trial court stayed its order to allow Pioneer to seek writ review, and the appellate court reversed.

While the appellate court agreed that the California Constitution's right to privacy covered the contact information for Pioneer's customers, it disagreed over what steps were needed to protect that right. The Court reasoned that a consumer cannot be deemed to have waived its privacy rights unless and until the consumer receives notice of the need to assert or waive its rights. The only practical way to ensure that the consumer had received such notice was to require the consumer to affirmatively consent to release of the information. Based on this reasoning, the appellate court vacated the trial court's order. The Supreme Court agreed to review the case, ultimately reversing the intermediate appellate court.

II. The Court's Analysis in *Pioneer*

The Supreme Court began its analysis of the

(See "Pioneer" on page 13)

Guidelines

Continued from page 11

the subject of professional and civil conduct in their programs for the training of new lawyers and legal education. Law firms should also identify a lawyer within the litigation practice group to whom questions regarding compliance with these guidelines (either by an attorney in the firm or by opposing counsel) may be addressed.

Dispute Resolution

The ABTL of San Diego encourages law firms subscribing to the principles of these guidelines to confirm their willingness to participate in a voluntary inter-firm dispute resolution process where opposing counsel whose firm has also subscribed to the principles of these guidelines believes that there has been a violation of the principles set forth in the guidelines or other applicable rules of professional conduct.

Participating firms would each designate an experienced member of the firm for this purpose. The designated lawyer would be available to receive, investigate and assist in the resolution of complaints of unprofessional or uncivil conduct. The ABTL of San Diego believes that the process would be facilitated if complaints were presented by a disinterested member of the complaining law firm. The goal of the process would be to resolve differences by inter-firm discussion, and the intervention of disinterested and responsible members of each firm, rather than through escalating abrasive behavior on each side and motions and counter-motions for sanctions. ▲

Pioneer

Continued from page 12

privacy issue by describing the test that courts must use in assessing invasion-of-privacy claims. Under that test, courts ask: (1) whether the claimant has a legally protected privacy interest, such as an interest in precluding dissemination or misuse of sensitive and confidential information, (2) whether the claimant possesses a reasonable expectation of privacy under the circumstances, and (3) whether the threatened invasion of that privacy interest is "serious," *i.e.*, whether its actual or potential impact would constitute an 'egregious' breach of social norms. 40 Cal. 4th at 370-371. If the answer to all of these questions is "yes", courts balance the threatened privacy invasion against any competing or countervailing interests, taking into account the need for the information and whether protective measures or safeguards can limit the privacy intrusion. *Id.* at 371.

Using this analytical framework, the Court concluded that the trial court had not abused its discretion in ordering Pioneer to produce the information absent objections from the complaining consumers. How the Court reached that conclusion provides a clue as to how the decision will shape future discovery battles in consumer litigation.

The Court first noted that complaining consumers have a reduced expectation that their contact information will be kept private. That is because consumers who voluntarily disclose their identifying information to manufacturers in the hopes of obtaining redress for defective products would not reasonably expect that their information would be withheld from a class action plaintiff seeking similar relief. *Id.* at 372. Indeed, "if anything, these complainants might reasonably expect, and even hope, that their names and addresses would be given to any such class action plaintiff." *Ibid*. While one can reasonably question the validity of that premise (does it really follow that a consumer who complains to a manufacturer about a product should expect that his name and contact information will be given to a lawyer she doesn't know and has never spoken to?), there is no question that this premise is central to the Court's decision.

The Court next determined that for many of the same reasons complaining consumers have a reduced expectation that their contact information will be kept private, the trial court could reasonably find that no serious invasion of privacy would occur if the information were released to the plaintiff in a consumer class action. The Court noted that the information sought was not particularly sensitive since it involved only disclosure of contact information already voluntarily disclosed to Pioneer. That consumers could choose to block production by returning the form sent to them further lessened the risk of a serious invasion of privacy.

Even though the Court's conclusions on these first two prongs were sufficient to uphold the trial court's "opt-out" order, the Court still weighed plaintiff's need for the information against any threatened harm caused by its disclosure. The Court determined that plaintiff's interest in the information outweighed the possibility that some of Pioneer's customers might fail to receive the notice and lose their opportunity to object to disclosure. The Court found it significant that the discovery rules expressly provide for discovery of the identity and location of persons having discoverable knowledge. See Cal. Cod. Civ. Proc. § 2017.010. The Court also noted that if plaintiff were allowed to contact customers who had complained about the DVD players, it might improve the chances of successfully prosecuting the action, which might well benefit those complaining customers. Thus, it made "little sense to make it more difficult for plaintiff to contact them by insisting they first affirmatively contact Pioneer as a condition to releasing the same contact information they already divulged long ago." *Pioneer*, 40 Cal. 4th at 374. Under all of these circumstances, the Court found there was nothing improper about ordering Pioneer to provide plaintiff with its customers' contact information after sending the customers an opt-out notice.

III. The Practical Implications of *Pioneer*

What are judges, practitioners and clients to make of this decision? Does it make it easier for class action and other plaintiffs to obtain private contact information about a corporate defendant's customers? Maybe. Is it the broad victory for plaintiffs that some have claimed? Probably not.

Had the Court decided that opt-out notice is always sufficient to protect consumers' privacy rights, the victory for plaintiffs might have been as great as some have claimed and others have feared. But the Court did not do so. Instead, the Court opted for a case-by-case inquiry. Thus, the case does little to change existing law.[1]

(See "Pioneer" on page 14)

Pioneer

Continued from page 13

In fact, the decision might be as noteworthy for what it does not do as for what it does. It does not hold that an "opt-out" *Colonial Life* letter is always sufficient to protect consumers. And it does not hold that an "opt-in" *Colonial Life* letter is never proper. Indeed, while *Pioneer* was under review, the Supreme Court refused to review or depublish another decision upholding an order providing for "opt-in" notice to consumers. See *Best Buy Stores v. Superior Court*, 137 Cal. App. 4th 772 (2006).

Since the *Pioneer* decision does not overrule or criticize the *Best Buy* decision, it is worth trying to decipher why opt-out notice was appropriate in one case and opt-in notice in the other. The answer appears to turn on whose information was being sought. In *Best Buy*, in which opt-in notice was ordered, a lawyer representing himself as plaintiff in a consumer class action sought contact information for Best Buy customers who had paid improper or illegal restocking fees for the admitted purpose of finding substitute class representatives. But unlike in *Pioneer*, the requested discovery was not limited to customers who had complained to Best Buy. If one is looking for a rule to take from *Pioneer*, it appears to be that opt-out notices are sufficient to protect the privacy rights of consumers who have complained about the product in question, at least in cases seeking class-wide relief for purchasers of the defective product.

Another question worth pondering is whether in the wake of the new standing requirements for consumer class actions under California's Unfair Competition Law, *Pioneer* gives enterprising plaintiff's lawyers a license to fish for class representatives. The answer seems to be "no" after another recent appellate decision that held a putative class representative who was never a member of the class he purports to represent may not use discovery to search for possible class representatives. See *First American Title Ins. Co. v. Superior Court*, 146 Cal. App. 4th 1564, 1578 (2007). On the other hand, a class representative who is a member of the class may discover customer contact information from the defendant for the purpose of finding additional or substitute class representatives. See *Best Buy*, 137 Cal. App. 4th at 779; *Budget Finance Plan v. Superior Court*, 34 Cal. App. 3d 794, 799-800 (1973). Since this rule pre-dates *Pioneer* and the *Pioneer* court cited *Budget Finance Plan* with approval, it would seem that any concern that *Pioneer* will open the discovery floodgates in consumer class actions is overblown.

What affect does the *Pioneer* decision have for discovery of complaining witnesses in non-class actions? What kind of notice is required before a plaintiff in a product-liability suit may discover the names and contact information of customers who have complained about the same product? While one cannot be certain, the rationale underlying Pioneer would appear to suggest that opt-in notice would be required. The *Pioneer* court concluded that opt-out notice was sufficient in that case because customers who had complained about the same product had a reduced expectation that their contact information would be kept private. And the principal reason that they had a reduced expectation of privacy was because they stood to benefit from successful prosecution of the lawsuit. See *Pioneer*, 40 Cal. 4th at 372. That rationale is missing completely in an individual action because the plaintiff is not seeking relief for the other customers, and those customers do not stand to benefit from successful prosecution of the action. While other factors could alter the outcome, it appears that opt-in notice normally would be required in individual actions to obtain information about other complaining consumers.

Thus, answering the original question of what to make of the *Pioneer* decision, the answer is that it depends on one's perspective. Practitioners who favor certainty in the law likely will be frustrated by the *Pioneer* Court's refusal to adopt a bright-line rule under which opt-out notice is either always acceptable or never acceptable. Lawyers who thrive on nuance, on the other hand, likely will appreciate the case-by-case inquiry that *Pioneer* requires.

In the end, the *Pioneer* decision's main contribution to the broader privacy debate is its confirmation of the analytical framework under which trial lawyers and judges are to litigate privacy questions. While the decision may not be the victory that either side had hoped for, it at least stakes out the rules of engagement for future battles. ▲

1 Given that the Supreme Court generally reviews a Court of Appeal decision only "when necessary to secure uniformity of decision or to settle an important question of law," Cal. Rule of Court 8.500(b)(1), neither of which seems applicable in *Pioneer*, one wonders why the Court agreed to review the case at all.

Continued from page 4

nificant. Studies have reported that the average identity theft victim spends between $400 and $880 and between 40 and over 300 hours to rectify problems caused by identity theft.

The corporate costs of remedying such a breach are also expensive. According to a recent study by the Ponemon Institute of Michigan, the average corporate cost of a data breach is $182 per compromised record, and the average company cost per data breach incident is $4.8 million – with insurance coverage for such losses available but highly variable. In the T.J. Maxx situation, for example, the company is now a defendant in at least seven federal and state class action lawsuits, the subject of over a dozen state Attorneys General informal investigations, and claims to have hired more than 50 security experts (and who knows how many lawyers) to investigate security breaches that went on for over a year, presumably undetected.

What started all these revelations? What do they mean? And, most significant, what can be done to prevent them? The short answer – data security breach notification laws, first adopted in California in 2003 and now adopted in a majority of states, require companies to make immediate and significant disclosures if data security breaches take place.

I. What Are Data Security Breach Notification Laws?

Many of us have heard about the privacy components of the Gramm-Leach-Bliley Act, HIPAA or the Sarbanes-Oxley Act. These federal laws protect different types of personal information from unauthorized access or use, as well as require disclosure of certain corporate privacy policies. Data security breach notification laws address the issue of what happens when the privacy protection measures adopted to protect such data have been compromised.

California adopted the first data security breach notification law, codified at Cal. Civ. Code Section 1798.80 *et seq.*, effective July 1, 2003. 33 other states have since adopted similar laws modeled after, but not the same as, the California law. Presently pending in Congress are several bills that would adopt a variant of the California model on a nationwide basis, including the Notification of Risk To Personal Data Act of 2007, S.239 (introduced January 10, 2007).

In general, these laws require a company notify law enforcement agencies and consumers if the company learns that personal consumer information has been compromised. Since California was the first to adopt these laws, this article highlights the California law.

First, what data are protected? Any personal, non-public information that has not been encrypted and includes a person's first name or initial and last name plus a wide variety of data, including their Social Security Number, driver's license number, or financial account number in combination with any password that would permit access to a financial account, is covered by the statute. Cal. Civ. Code Section 1798.82(e). According to the California Office of Privacy Protection, the vast majority of reported breaches involve Social Security Numbers.

Second, who is covered? Any entity that conducts business in California and owns, licenses or otherwise maintains computerized data about a customer or client located in California is subject to these statutory provisions. Civil Code Section 1798.81.5(e), which addresses a different issue about maintaining reasonable security procedures, provides a list of entities that are governed by other laws and thus may be exempt from some statutory requirements. Unlike other states, these California laws also cover government agencies.

Third, what must companies do if they become aware of a breach? Companies must notify any resident of California whose unencrypted personal data were, or are reasonably believed to have been, acquired by an unauthorized person that a security breach has taken place. Pursuant to Section 1798.82(g), this notification can be accomplished by written notice, electronic notice, or, if the cost of providing notice would exceed $250,000 or involve more than 500,000 persons, a combination of email notice, "conspicuous posting" of the notice on the Web site page and notification to major statewide media. The form of that notice is discussed *infra*.

(See "Data Breach" on page 16)

Data Breach

Continued from page 15

Fourth, when must companies undertake this notification effort? According to Section 1798.82(a), companies must accomplish this notification "in the most expedient time possible and without unreasonable delay". What does this mean? The California Office of Privacy Protection recommends such notification be accomplished within 10 business days after learning about the breach, depending on the sensitivity of the data. However, if a company believes the unauthorized access may be the result of a crime, this notification obligation may be delayed if a law enforcement agency first determines notification will impede a criminal investigation. Cal. Civ. Code Section 1798.82(c). Thus, a company should immediately (within a day or two) give notice of the relevant facts to appropriate law enforcement agencies so that such agencies can first ensure any notification will not compromise their investigation prior to the company implementing a notification program.

Because these data security breach notification laws differ from state to state, a multi-state business needs to immediately consider numerous factual and legal issues if a data breach occurs. Where was the data lost? Where are the clients or customers whose data were compromised located? If possible, where can the data breach be traced to? Answers to these questions are critically important to determine, because simply relying on the law of the state where the business is located may not be the answer.

Multiple laws could apply depending on the residence of the individuals whose data were compromised, triggering a potential conflicts analysis. This issue was recently recognized in *Kearney v. Salomon Smith Barney*, 39 Cal. 4th 95 (2006), where a conflict between Georgia and California law on a privacy issue was resolved in favor of applying California law due to California's significant interest in protecting the privacy of its residents. The Court permitted a class claim for injunctive relief, but not damages, to proceed. The Court found applied California law in part based on its conclusion that California "repeatedly has enacted new legislation in related areas in an effort to increase the protection of California consumers' privacy in the face of a perceived escalation in the impingement upon privacy interests caused by various business practices." *Id.* at 125.

While most of these laws may not directly conflict, some states have a safe harbor provision and some do not. Some have different time periods in which officials and consumers should be notified of a breach. Some apply to government agencies and some do not. Some require more information be contained in the notification letter. Thus, a company needs to quickly

(See "Data Breach" on page 17)

Continued from page 16

determine what state laws may apply in order to assess what its specific obligations may be. Because of the sensitivity of the data and the laws that come into play, this is not a question that can be resolved in weeks – this is a question that must be resolved within days after learning about the possible breach. The following links to other state laws are helpful to review these laws' similarities and differences: www.consumersunion.org/campaigns/Breach_laws_May05.pdf (complied by Consumers Union); www.ncsl.org/programs/lis/cip/priv/breach.htm (compiled by the National Conference of State Legislatures).

II. What Can Entities And Consumers Do To Protect Themselves?

Any entity that maintains personal consumer data in computerized format needs to undertake several important proactive measures before any breach event may occur: (1) understand what data they possess, (2) review the security of their data, and (3) adopt a data breach notification policy.

While the first step sounds simple, non-technical management within companies are sometimes surprised to learn what data they actually possess. Thus, an important threshold issue is to ensure that key management knows what information is collected that falls under the applicable security breach notification laws. Many companies, including large corporate retailers, do not have a good idea of what information they have collected from, or about, their customers. A company data audit is a good place to start.

As to the second issue, privacy officers marvel (or shiver) over how much data their companies retain. Some companies report having set a default mechanism for electronically stored data so that customer data is not deleted for 99 years! Data are maintained on active hard drives that may be downloaded on to laptops or flash keys. If that laptop or flash key is lost, stolen or misplaced (which has resulted in close to 50% of the data notification events), that may trigger the data security breach notification laws. Companies need to know and keep track of: 1) what data are maintained, 2) for how long and on what systems, 3) whether such data are segregated and/or encrypted, 4) what data can be downloaded to personal devices, 5) who can access or download such data and 6) how access to such data is monitored.

For some guidance on these data security protection issues, ISO 17799 entitled "Information Technology – Security Techniques – Code of Practice for Information Security Management" provides a nationally recognized data security reference standard. In addition, the FTC just recently issued a brochure entitled "Protecting Personal Information: A Guide for Business", located at www.ftc.gov/bcp/edu/pubs, which contain five key principles for companies to follow in developing a plan for securing personal information.

One of the best sources of information on how to comply with the data security breach notification laws (at least in California, and as a model for elsewhere) is available through the California Office of Privacy Protection. This Office has prepared and just recently revised a brochure available at www.privacy.ca.gov/recommendations/secbreach.pdf entitled "Recommended Practices on Notice of Security Breach Involving Personal Information". This brochure provides businesses and consumers with: 1) a summary of the California data security breach notification law, 2) preventative practices to adopt, 3) sample letters to send to consumers, and 4) what government agencies to contact. The latter are extremely important to consider, since many states (including California, see Cal. Civ. Code Section 1798.82(g)) have adopted a safe harbor provision for companies that have adopted their own security and notification procedures as part of a *pre*-data breach program that makes following those notification procedures *per se* compliance with that state's notification law.

If your company or client has not adopted these protections and a data breach occurs, the best advice you can give is to gather information quickly. Who lost the data or how was the data compromised? Was the data lost, stolen or hacked? Can you definitively trace what data were lost or accessed? Where are the customers or clients whose data were compromised located? What government agencies need to be immediately notified? Once you gather the answers to these questions, you can better assess and advise what laws

(See "Data Breach" on page 18)

Data Breach

Continued from page 17

may apply, what form the notification can take and how also to ensure compliance.

In California there is no case law yet on what constitutes compliance with these statutes, so this is an area for future case law development. This will include cutting edge issues such as: 1) whether failure to adopt such policies or follow the statutory requirements constitutes negligence *per se* or an unlawful business practice if required by statute, 2) conversely, if the safe harbor can be invoked does that create immunity from suit, 3) what type of tort or contract liability can flow to a company if a data breach occurs, and 4) what to do in the event a conflict of laws exist. These are important issues to consider and analyze in advising your clients.

If you receive one of those letters and it indicates your Social Security Number has been compromised, an important first step is to contact the three major credit reporting agencies (Experian, Transunion and Equifax) and ask to place a credit fraud alert on your credit report. You are entitled by law to one free annual credit report, so it is also a good idea to request a report to make sure no incidents have immediately arisen. You can request such a report through www.annualcreditreport.com. Sometimes banks will cancel and re-issue credit or debit cards if financial account information is disclosed, so consumers should also contact any relevant financial institutions. Finally, the California Office of Privacy Protection, the public interest group the Privacy Rights Clearinghouse, and the FTC all have available information on their websites listing steps consumers can take to protect themselves in the case of identity theft or compromised personal data due to a data security breach.

III. Conclusion

In the 21st Century even data that are not made available on the Internet can be compromised. In fact, most breaches are decidedly "low tech", the result of losing or misplacing a lap top computer, flash key or CD-ROM. How corporate entities protect and treat personal consumer data – and that goes for retailers, government agencies, and even law firms – is a critical component of their corporate data security practices. Ideally, entities will proactively manage, encrypt and/or delete unnecessry or outdated personal data they gather and retain. However, companies must have both an understanding and a plan about what to do if personal data in its possession are compromised. Having such policies in place not only makes good legal sense and can limit potential liability, but also is critical to avoid spending potentially millions of dollars and untold customer good will in the unfortunate event customer or client data are compromised. ▲

ASSOCIATION OF BUSINESS TRIAL LAWYERS SAN DIEGO

abtl

P.O. Box 16946
San Diego, CA 92176-6946

Editor: Alan M. Mansfield
(858) 348-1005

Editorial Board:
Erik Bliss, John T. Brooks,
Richard Gluck, Robert Gralewski,
and Shannon Petersen.

PRSRT STD
U.S. Postage
PAID
Permit #51
San Diego, CA